

<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>			1. CONTRACT ID CODE	PAGE OF PAGES <b>1</b>   <b>2</b>	
2. AMENDMENT/MODIFICATION NO. <b>PS1422</b>	3. EFFECTIVE DATE <b>See Block 16C</b>	4. REQUISITION/PURCHASE REQ. NO		5. PROJECT NO. <i>(If applicable)</i>	
6. ISSUED BY <b>U.S. General Services Administration FAS-ITC Office of Acquisition Operations 1800 F Street NW 4th Floor Washington DC 20405-0001</b>	CODE <b>QT2A1F</b>	7. ADMINISTERED BY (IF OTHER THAN ITEM 6) CODE			
8. NAME AND ADDRESS OF CONTRACTOR <i>(No., Street, County, State, and Zip Code)</i> <b>MCI Communication Services, Inc. DBA Verizon Business 22001 Loudon County Parkway Ashburn, VA. 20147 Attn: Katherine H. Conwell</b>			9A. AMENDMENT OF SOLICITATION NO.		
			9B. DATED <i>(SEE ITEM 11)</i>		
			10A. MODIFICATION OF CONTRACT/ORDER NO. <b>GS00T07NSD0038</b>		
CODE: <b>020751082</b> FACILITY CODE: <b>581P8</b>			10B. DATED <i>(SEE ITEM 13)</i> <b>May 31, 2007</b>		
<b>11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS</b>					

The above numbered, solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers  is extended  is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning \_\_\_\_\_ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers, FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA <i>(If Required)</i>	
<b>13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO., AS DESCRIBED IN ITEM 14</b>	
<input type="checkbox"/>	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: <i>(Specify Authority)</i> THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES <i>(such as changes in paying office, appropriation date, etc.)</i> SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).
<input checked="" type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: <b>FAR 43.103 (a) (3) Bilateral Modification by Mutual Agreement Between the Parties</b>
<input type="checkbox"/>	D. OTHER <i>(Specify type of modification and authority)</i>


E. IMPORTANT: Contractor  is NOT  is required to sign this document and return 1 copy to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

**SEE CONTINUATION SHEET**

❖ The total estimated dollar value of the contract is unchanged by this modification.

**Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore remains unchanged and in full force and effect.**

15A. NAME AND TITLE OF SIGNER <i>for Michael Maiorana, Sr. Vice President by Klara B Reilly, Director</i>		16A. NAME AND TITLE OF CONTRACTING OFFICER <i>Jong Lee, Contracting Officer</i>	
15B. CONTRACTOR/OFFEROR  	15C. DATE SIGNED  <b>27Feb2018</b>	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED  <b>02/27/2018</b>
<i>(Signature of person authorized to sign)</i>		<i>(Signature of Contracting Officer)</i>	

---

The purpose of this Modification is to incorporate the following:

1. To remove Sensitive Compartmented Information Facility (SCIF) requirement for MTIPS from the Network Contract in Section C.

The following sections affected by this change:

- a. Paragraph C.2.4.1.5.1.1 (1)d. - Function Definition - (page **C-69**)
- b. Figure C.2.4.1.5-3 - The TIC Portal Security Operation Center Architecture - (page **C-83**)
- c. Paragraph C.2.4.1.5.1.4.1 4 - TIC Portal Capabilities - ICD 705 Sensitive Compartmented Information Facility (SCIF) - (page **C-93**)
- d. Paragraph C.2.4.1.5.5.2.2 1.c. - MTIPS Global Response Loop - (page **C-110**)
- e. Table C.2.4.1.5-2 - MTIPS Security Domain Overview - (page **C-112**)

## Table of Contents

SECTIONS	PAGE
<b>SECTION C</b>	<b>C-1</b>
<b>C.1 Background</b>	<b>C-1</b>
C.1.1 Networx Enterprise Objectives	C-1
C.1.2 Scope	C-2
C.1.3 Mandatory Service Requirements	C-2
C.1.4 Optional Service	C-3
C.1.5 Authorized Users	C-3
C.1.6 Upgrades and Enhancements	C-3
C.1.7 Organization of this Statement of Work	C-4
<b>C.2 Technical Requirements</b>	<b>C-4</b>
C.2.1 General Requirements	C-4
C.2.2 Voice Services	C-18
C.2.3 Frame & Cell Switched Services	C-49
C.2.4 Internet Services	C-60
C.2.5 Dedicated Service	C-138
C.2.6 Combined Services	C-192
C.2.7 Virtual Private Network Services	C-197
C.2.8 Conferencing Services	C-265
C.2.9 Managed Networking Services	C-285
C.2.10 Security Services	C-290
C.2.11 Management & Applications Services	C-323
C.2.12 Management and Application Services	C-359
C.2.13 Access Services	C-365
C.2.14 Wireless Services	C-385
C.2.15 Reserved	C-407
C.2.16 Access Arrangements [As Applicable]	C-407
<b>C.3 Management and Operation</b>	<b>C-425</b>
C.3.1 General Information	C-425
C.3.2 Program Management	C-431
C.3.3 Service Management	C-453
C.3.4 Customer Service	C-485
C.3.5 Service Ordering	C-505
C.3.6 Billing	C-541
C.3.7 Training	C-608
C.3.8 Inventory Management	C-618
C.3.9 Operational Support Systems	C-628
<b>C.4 Transition</b>	<b>C-642</b>

C.4.1	Transition Process Definition	C-642
C.4.2	Transition Functional Requirements	C-646
C.4.3	Transition Data Requirements	C-653
C.4.4	Transition Report Requirement	C-659
<b>C.5</b>	<b>NATIONAL SECURITY AND EMERGENCY PREPAREDNESS (NS/EP)</b>	<b>C-670</b>
C.5.1	Introduction	C-670
C.5.2	NS/EP Technical Requirements	C-672
C.5.3	NS/EP Management Requirements	C-678
<b>C.6</b>	<b>SECTION 508 REQUIREMENTS</b>	<b>C-678</b>
C.6.1	Background	C-678
C.6.2	Voluntary Product Accessibility Template (VPAT)	C-679
C.6.3	Section 508 Applicability to Technical Requirements	C-679
C.6.4	Section 508 Provisions Applicable to Technical Requirements	C-679
<b>C.7</b>	<b>Technical Reports</b>	<b>C-681</b>
C.7.1	Frame Relay Service (FRS)	C-681
C.7.2	Asynchronous Transfer Mode Service (ATMS)	C-682
C.7.3	Dark Fiber Services (DFS)	C-682
C.7.4	Premises-Based IP VPN Services (PBIP-VPNS)	C-683
C.7.5	Network-Based IP VPN Services (NBIP-VPNS)	C-683
C.7.6	Managed Tiered Security Services (MTSS)	C-683
C.7.7	Layer 2 VPN Services (L2VPNS)	C-684
C.7.8	Incident Response Services (INRS)	C-684
C.7.9	Call Center/Customer Contact Center Services (CCS)	C-685
C.7.10	Storage Services (SS)	C-685
C.7.11	TeleWorking Solutions (TWS)	C-685
C.7.12	Cellular/Personal Communications Service (CPCS)	C-686
C.7.13	Multimode/Wireless LAN Service (MWLANS)	C-686
C.7.14	Unified Messaging Service (UMS)	C-686
C.7.15	Land Mobile Radio Service (LMR)	C-687
C.7.16	National Security and Emergency Preparedness (NS/EP) Functional Requirements Implementation Plan (FRIP)	C-687

List of Figures

<b>Figures</b>	<b>Page</b>
FIGURE C.2-1A NETWORK SERVICE TYPES AND SERVICES FOR MANDATORY IP-BASED SERVICES SET	C-6
FIGURE C.2-2 STRUCTURE OF SERVICE SPECIFICATIONS	C-8
FIGURE C.2-3 END POINTS OF THE CONTRACTOR'S RESPONSIBILITY FOR PERFORMANCE MANAGEMENT	C-14
FIGURE C.2.4.1.1.4-1 EXAMPLES OF IPS ACCESS ALTERNATIVES	C-62
FIGURE C.2.4.1.5-1 NETWORK MTIPS NOTIONAL ARCHITECTURE	C-68
FIGURE C.2.4.1.5-2 MTIPS CONTEXT ARCHITECTURE	C-69
FIGURE C.2.4.1.5-3 THE TIC PORTAL SECURITY OPERATION CENTER ARCHITECTURE	C-83
FIGURE C.2.5.3.1.4-1 POINT-TO-POINT DARK FIBER CONNECTION	C-163
FIGURE C.2.5.3.1.4-2 ROUTE DIVERSE DARK FIBER RING CONNECTION WITH SINGLE DROPS	C-164
FIGURE C.2.5.3.1.4-3 ROUTE DIVERSE DARK FIBER RING CONNECTION WITH DUAL DROPS	C-164
FIGURE C.2.5.3.1.4-4 DARK FIBER CONNECTIONS USING STAR CONFIGURATION	C-165
FIGURE C.2.5.4.1.1.4-1. OCONUS AND NON-DOMESTIC WAVELENGTH SERVICES	C-173
FIGURE C.2.5.4.1.1.4-2 – CONUS WAVELENGTH SERVICE	C-174
FIGURE C.2.5.4.1.2.1-1 – GEOGRAPHICALLY DIVERSE WAVELENGTHS ENDING AT THE SAME SDP	C-179
FIGURE C.2.12.1.1.3-1 - TWS APPLICATION FOR A "WORK AT HOME" TELEWORKER	C-361

List of Tables

<b>Tables</b>	<b>Page</b>
TABLE C.2.4.1.5-1 SUBSCRIBING AGENCY & CONTRACTOR ROLES FOR MTIPS SECURITY OPERATIONS	C-110
TABLE C.2.4.1.5-2 MTIPS SECURITY DOMAIN OVERVIEW	C-112
TABLE C.2.14.6.4-1 MINIMUM DEDICATED ACCESS ARRANGEMENTS	C-408

## Section C

### C.1 Background

The Federal Technology Service (FTS) provides Government users with up-to-date, cost-effective, and easy to use telecommunications and information technology services. The Networkx Enterprise acquisition provides authorized users with the full range of telecommunications products, services and solutions necessary to support their missions.

The FTS Program will continue to adapt to the changing commercial marketplace. It is explicitly recognized that:

- a. The telecommunications industry is rapidly changing. Merger activity, technology innovations, and regulatory issues have created a fluid and dynamic environment of change.
- b. Multiple contracts will be required to most effectively meet Government requirements and manage market driven risks. The General Services Administration (GSA) will compete, award and administer these contracts for the benefit of its user Agencies.
- c. The Government will encourage competition through multiple contracts of the same or overlapping scope, available to a wide range of service providers.
- d. Acquisitions will be initiated and contracts awarded in the best interest of the Government. All contracts will be available to all users as authorized by law or regulation.

#### C.1.1 Networkx Enterprise Objectives

This contract is for telecommunications services and solutions and is referred to as Networkx Enterprise. Its term includes a 48 month base period plus three (3) 24 month options. The Government intends to make multiple awards to contractors chosen under full and open competition to meet its Networkx Program goals as stated in Attachment J.1. Networkx Enterprise contracts are intended to meet the program goals for:

- Highly Competitive Prices
- High-Quality Service
- Alternative Sources
- Operations Support
- Transition Assistance and Support
- Performance-Based Contracts

The Government recognizes that the marketplace of telecommunications suppliers has changed significantly since the award of the FTS2001 contracts, and that further change is likely through the life of the Networkx program. This may include loss of suppliers,

further consolidation among suppliers, and/or the emergence of new technologies and market leaders. The Government intends to minimize the risks to the Government posed by these potential changes and also to ensure the benefits of competition throughout the term of the Networx Program. A separate acquisition known as Networx Universal will be used in conjunction with Networx Enterprise to address these risks, and specifically its goals of Service Continuity and Full Service Vendors, in a comprehensive manner.

Within the FTS Networx Program, Agencies will generally have the right to select the acquisition which meets their requirements, to buy from multiple contracts, and to change contractors and services within the FTS Networx Program when appropriate to meet requirements, subject to the limitations necessary to meet Minimum Revenue Guarantees.

### **C.1.2 Scope**

The scope of each Networx Enterprise contract will include services and solutions necessary for the Government to satisfy its telecommunications and networking requirements for the life of the contracts, with the exception of IPTelS and VoIPTS. These services will be considered for withdrawal on the contract under new terms and conditions of Section C.2.1.1 Organization of Networx Services, where the Verizon commercial footprint changes. In addition to the specific statement for work requirements set forth in Section C, the scope of this contract includes, at the discretion of the Government, technological enhancements, service improvements, customer-specific applications and extensions, ancillary equipment and professional services necessary to complete solutions. The scope also includes all new and/or emerging telecommunications services offerings. In particular, the scope of each Networx contract will include all local, regional, national and international telecommunications services, features, functions, software enhancements, network-based applications and associated offerings that will be generally available as a part of the contractor's commercial offerings, as well as offerings available in the commercial marketplace, during the term of these contracts, plus network-based solutions and services for which there may not be commercial offerings.

### **C.1.3 Mandatory Service Requirements**

Networx Enterprise requires each contractor to deliver and price a mandatory set of services. These mandatory service requirements are summarized below:

- A set of mandatory IP services with an associated mandatory geographic profile representing locations with access at speeds greater than or equal to T3 and one or more FTS2001 data services. Contractors will also be required to offer the services and prices where the contractor provides them commercially.

OR

- A set of wireless services with service provided in 90% of metropolitan statistical areas (MSAs) and 90% of rural statistical areas (RSAs)

Mandatory service requirements for Networkx Enterprise are specified in Attachment J.2, Geographic Coverage, and are included in the Traffic Model.

In addition, the contractor shall also provide service to the Government where it offers service commercially, as specified in Attachment J.2. After contract award, the contractor shall update its service coverage by contract modification to remain current with its commercial coverage.

After contract award, when requested by the Government, the contractor shall also provide service to any location (e.g., due to office construction, relocation and/or expansion) not served in its initial contract or covered by a subsequent contract modification. When the Government makes such a request, the contractor shall provide a timely proposal reflecting all necessary changes to the contract for negotiation with and acceptance by the Government (see Attachment J.4, Guidelines for Modifications to Networkx Program Contracts).

#### **C.1.4 Optional Service**

Most of the services in Networkx Enterprise are optional to offer. Optional services are specified in Figure C.2.1a and Figure C.2.1b. When offering optional services, the contractor shall provide service geographic coverage, for each service, where that service is offered commercially by the contractor. After contract award, the contractor shall update its optional service coverage by contract modification to remain current with its commercial coverage.

Optional services will be awarded on a service by service basis in accordance with the procedures contained in Section M. Optional service awards will be made at the time of contract award. After contract award notification, any optional service not awarded to an contractor will remain in scope but will not be considered for addition to the contractor's awarded contract for 24 months after contract award notification. After the 24 month period expires, and when in the Government's best interests, the Government will consider proposals by the contractor to incorporate any non awarded service specified in Section C.2. into its contract by contract modification.

#### **C.1.5 Authorized Users**

This contract is for the use of all Federal Agencies, authorized Federal contractors, Agency-sponsored universities and laboratories, other organizations as defined in Section H.2, and, when authorized by law or regulation, state, local, and tribal governments.

#### **C.1.6 Upgrades and Enhancements**

The Government recognizes that telecommunications technologies and services are rapidly evolving and advancing. The Government wishes Networkx services and solutions to remain up-to-date with commercial equivalents. Accordingly, the Government anticipates that services and solutions available under this contract will be increased, enhanced, and upgraded as these improvements become available to commercial customers.



In particular, the contractor shall provide upgrades to its commercial support systems, (including but not limited to systems for billing and invoicing, service ordering and tracking, trouble and complaint handling, and management and administrative reporting) at no additional cost to the Government as these upgrades become available to commercial customers at no or minimal costs.

### **C.1.7 Organization of this Statement of Work**

Section C.2 summarizes the technical requirements addressed by this contract. Section C.2.1 describes the general requirements and the format for the specification of the individual service types and services, which are contained in Sections C.2.2 through C.2.14. Section C.3 specifies the management and operations requirements that must be met by all Networx Enterprise contractors, including requirements for program management, service management, service ordering, billing, customer service, inventory management, operational support systems, and training. Section C.4 contains requirements for management of transition from another GSA-administered contract to Networx Enterprise, Section C.5 specifies the Government's requirements for National Security/Emergency Preparedness (NS/EP) that have been established in accordance with Executive Order 12472. Section C.6 specifies the Government's requirements for Section 508 compliance that have been established to ensure access to information and services by Government employees and citizens with disabilities. Section C.7 specifies technical reports that must be provided by the Networx contractor.

## **C.2 Technical Requirements**

### **C.2.1 General Requirements**

The contractor shall provide:

- (a) **Communications Services.** These services will be used to satisfy Agency requirements for the secure transport of communications (e.g. voice, video, and data) and to provide required supporting services (e.g, management and applications).
- (b) **Management and Operations Services.** (Refer to Section C.3) These services will be used to effectively manage and control telecommunications resources, reduce network management and operations costs, and administer the contract.

#### **C.2.1.1 Organization of Networx Services**

Networx communications services are grouped into "Service Types." Service Types describe services that are similar and are grouped to simplify specification, offering and evaluation processes.

There are six (6) Service Types as follows:

- (1) **Telecommunications Services Type.** This Service Type delivers telecommunications services. This Service Type is further categorized as follows:

- (a) **Communications Transport Services Category.** These include services that are basic transport level services.
- (b) **IP-Based Services Category.** These include services that are based on Internet Protocol
- (c) **Optical Services Category.** These include services that are based on optical fiber
- (2) **Management and Application Services Type.** These include services that address the Agency's need for management and application services that are directly associated with, and add value to, the delivery of telecommunications services and solutions
- (3) **Security Services Type.** This Service Type includes services that provide additional security solutions and management
- (4) **Special Services Type.** This Service Type includes services that are based on satellite and land mobile radio transmission systems
- (5) **Wireless Services Type.** This Service Type includes services that are based on wireless transmission systems
- (6) **Access Services Type.** This Service Type includes services that can be used to connect to Agency designated networks

There are 50 services specified in this acquisition which are organized by appropriate Service Type. Additionally, Network Enterprise services are classified as Mandatory and Optional.

A Network service provider must offer either (a) a mandatory set of services which meet minimum government requirements for managed, secure IP networks ; or, (b) a mandatory wireless service, Cellular Personal Communications Service. Figure C.2-1a and Figure C.2-1b present the organizational structure for the six Service Types, the 50 individual services, and identifies which services are mandatory to offer and which are optional to offer.

**NETWORKX ENTERPRISE**  
**Mandatory and Optional IP-Based Services Set**  
**9 Mandatory Services**  
**41 Optional Services**  
**50 Total Services organized into 6 Types of Services**

<p><b>(1) Telecommunications Services Type</b></p> <ul style="list-style-type: none"> <li>• <b>Communications Transport Services Category</b> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Voice</li> <li>- Circuit Switched Data</li> <li>- Toll-Free</li> <li>- Combined</li> <li>- Private Line</li> <li>- Frame Relay</li> <li>- Asynchronous Transfer Mode</li> <li>- Ethernet</li> </ul> </li> </ul> </li> <li>• <b>IP-Based Services Category</b> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- Network-Based IP VPN</li> <li>- Voice over IP Transport</li> <li>- Internet Protocol</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Premises-Based IP VPN</li> <li>- Content Delivery Network</li> <li>- Converged IP</li> <li>- IP Telephony</li> <li>- IP Video Transport</li> <li>- Layer 2 VPN</li> </ul> </li> </ul> </li> <li>• <b>Optical Services Category</b> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Synchronous Optical Network</li> <li>- Optical Wavelength</li> <li>- Dark Fiber</li> </ul> </li> </ul> </li> </ul>	<p><b>(2) Management &amp; Applications Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- Managed Network</li> <li>- Customer Specific Design and Engineering</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Video Teleconferencing</li> <li>- Audio Conferencing</li> <li>- Teleworking Service</li> <li>- Call Center/Customer Contact Center</li> <li>- Web Conferencing</li> <li>- Dedicated Hosting</li> <li>- Collocated Hosting</li> <li>- Storage</li> <li>- Unified Messaging</li> <li>- Collaboration Support</li> <li>- Internet Facsimile</li> </ul> </li> </ul> <p><b>(3) Security Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- Managed Firewall</li> <li>- Intrusion Detection and Prevention</li> <li>- Managed Tiered Security</li> <li>- Anti-Virus Management</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Managed E-Authentication</li> <li>- Vulnerability Scanning</li> <li>- Incident Response</li> <li>- Secure Managed Email</li> </ul> </li> </ul>	<p><b>(4) Special Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Land Mobile Radio</li> </ul> </li> </ul> <p><b>(5) Wireless Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Cellular/PCS</li> <li>- Multimode Wireless</li> <li>- Cellular Digital Packet Data</li> <li>- Paging</li> </ul> </li> </ul> <p><b>(6) Access Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Wireline Access</li> <li>- Broadband Access</li> <li>- Wireless Access</li> <li>- Satellite Access</li> </ul> </li> </ul>
---	--	--

**Figure C.2-1a Networkx Service Types and Services for Mandatory IP-Based Services Set**

**NETWORK ENTERPRISE**  
**Mandatory and Optional Wireless Services Set**  
**1 Mandatory Service**  
**49 Optional Services**  
**50 Total Services organized into 6 Types of Services**

<p><b>(1) Telecommunications Services Type</b></p> <ul style="list-style-type: none"> <li>▪ <b>Communications Transport Services Category</b> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Voice</li> <li>- Circuit Switched Data</li> <li>- Toll-Free</li> <li>- Combined</li> <li>- Private Line</li> <li>- Frame Relay</li> <li>- Asynchronous Transfer Mode</li> <li>- Ethernet</li> </ul> </li> </ul> </li> <li>▪ <b>IP-Based Services Category</b> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Network-Based IP VPN</li> <li>- Voice over IP Transport</li> <li>- Internet Protocol</li> <li>- Premises-Based IP VPN</li> <li>- Content Delivery Network</li> <li>- Converged IP</li> <li>- IP Telephony</li> <li>- IP Video Transport</li> <li>- Layer 2 VPN</li> </ul> </li> </ul> </li> <li>▪ <b>Optical Services Category</b> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Synchronous Optical Network</li> <li>- Optical Wavelength</li> <li>- Dark Fiber</li> </ul> </li> </ul> </li> </ul>	<p><b>(2) Management &amp; Applications Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Managed Network</li> <li>- Customer Specific Design and Engineering</li> <li>- Video Teleconferencing</li> <li>- Audio Conferencing</li> <li>- Teleworking Service</li> <li>- Call Center/ Customer Contact Center</li> <li>- Web Conferencing</li> <li>- Dedicated Hosting</li> <li>- Collocated Hosting</li> <li>- Storage</li> <li>- Unified Messaging</li> <li>- Collaboration Support</li> <li>- Internet Facsimile</li> </ul> </li> </ul> <p><b>(3) Security Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Managed Firewall</li> <li>- Intrusion Detection and Prevention</li> <li>- Managed Tiered Security</li> <li>- Anti-Virus Management</li> <li>- Managed E-Authentication</li> <li>- Vulnerability Scanning</li> <li>- Incident Response</li> <li>- Secure Managed Email</li> </ul> </li> </ul>	<p><b>(4) Special Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Land Mobile Radio</li> </ul> </li> </ul> <p><b>(5) Wireless Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- Cellular/PCS</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Multimode Wireless</li> <li>- Cellular Digital Packet Data</li> <li>- Paging</li> </ul> </li> </ul> <p><b>(6) Access Services Type</b></p> <ul style="list-style-type: none"> <li>• <u>Mandatory</u> <ul style="list-style-type: none"> <li>- None</li> </ul> </li> <li>• <u>Optional</u> <ul style="list-style-type: none"> <li>- Wireline Access</li> <li>- Broadband Access</li> <li>- Wireless Access</li> <li>- Satellite Access</li> </ul> </li> </ul>
---	---	--

**Figure C.2-1b Network Service Types and Services for Mandatory Wireless Services set**

The 50 services are specified in Sections C.2.2 through C.2.14.

A single service specification structure is used for every service. This common structure is intended to facilitate clarity of specification and consistency of contractor responses. This structure also conforms with performance based contracting guidelines. Figure C.2-2 illustrates this structure.

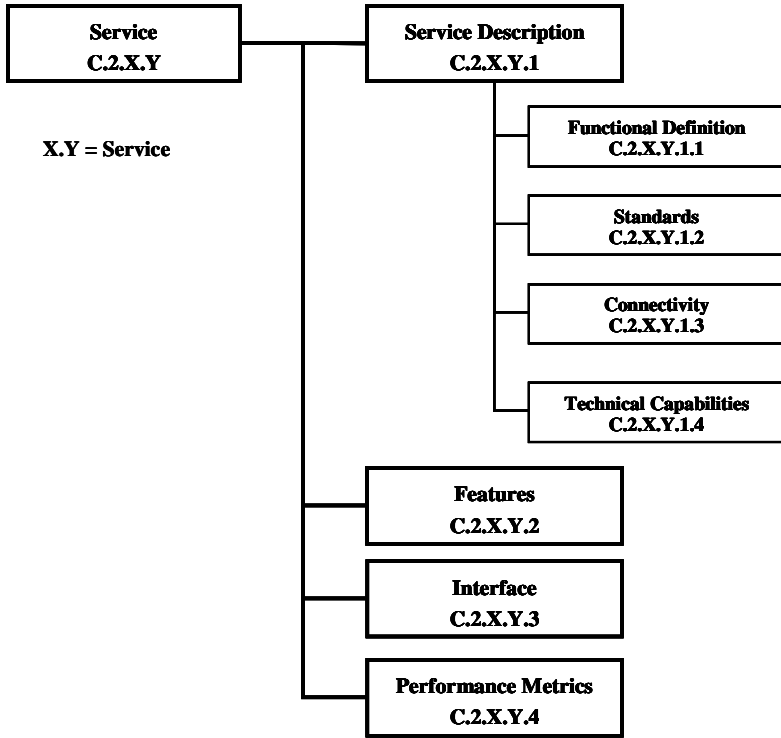


Figure C.2-2 Structure of Service Specifications

Each service is described in functional terms and in terms of the industry standards to be met, the connectivity to be provided (e.g., to Government Furnished Property (GFP), Public Switched Network (PSN), and other Network Universal and Network Enterprise contractor networks), and associated technical capabilities required. Service features, interfaces, and performance metrics are presented in tabular form. Contractors shall provide all services awarded for the duration of the Network Enterprise contract, except for IPTeS and VoIPtS, which now have special terms and conditions for the duration of the Verizon Extension contract period of performance. This includes services awarded at contract inception and those added during the life of the contract by modification. If the contractor determines that any of these services can no longer be supported due to obsolescence, the contractor shall notify the Contracting Officer in writing of plans to withdraw the service at least eighteen (18) months prior to the proposed date of the withdrawal. Contractors at that time must propose to the Government an acceptable plan to ensure service continuity. The GSA contracting officer must approve any withdrawal of service offerings through a contract modification. If the contractor determines that IPTeS and VoIPtS can no longer be supported due to changes in the commercial footprint, the contractor shall notify the Contracting Officer in writing of plans to withdraw the service in areas affected by a change in commercial footprint, at least eighteen (18) months prior to the proposed date of the withdrawal. Contractors at that time must propose to the Government an acceptable plan to ensure service continuity. The GSA Contracting officer must approve any withdrawal of service offerings through a contract modification.

Section C.2 summarizes the technical requirements addressed by this contract. Section C.2.1 describes the general requirements and the format for the specification of the individual service types and services, which are contained in Sections C.2.2 through C.2.14. Section C.3 specifies the management and operations requirements that must be met by all Network Enterprise contractors, including requirements for program management, service management, service ordering, billing, customer service, inventory management, operational support systems, and training. Section C.4 contains requirements for management of transition from another GSA-administered contract to Network Enterprise, Section C.5 specifies the Government's requirements for National Security/Emergency Preparedness (NS/EP) that have been established in accordance with Executive Order 12472. Section C.6 specifies the Government's requirements for Section 508 compliance that have been established to ensure access to information and services by Government employees and citizens with disabilities. Section C.7 specifies technical reports that must be provided by the Network contractor.

#### **C.2.1.1.1 Relationship of Service Descriptions to Pricing Tables**

The Service Specifications in Sections C.2.2 through C.2.15 have corresponding pricing tables in Section B.2. A detailed mapping of Service Specifications to pricing tables is contained in Table B.1.2-1. Separate pricing tables are provided in Section B.3 for the access arrangements as specified in Section C.2.16. Pricing for the Service Enabling Devices (SEDs) used in the delivery of the services specified in this section is contained in Section B.4. Pricing of miscellaneous items associated with these services, such as moves and changes, is contained in Section B.6.

### **C.2.1.2 Service Coverage**

The Network contractor shall provide services for both domestic and non-domestic locations. Domestic locations are defined in Section J.11. All other locations are defined as non-domestic for the purposes of this contract.

### **C.2.1.3 Service Delivery Point**

The interface point at which a service is delivered by the contractor to the Government or its designated agent. The SDP is the interface point for the physical or logical delivery of a service, the point at which performance parameters are measured to determine compliance with the contract, and the point used by the contractor to identify the pricing for services rendered.

SDPs may be located on or off Agency premises. Possible SDP locations include but are not limited to:

- a) Network side of a Private Branch Exchange (PBX), Central Office, Centrex system, or other communications system or network.
- b) User side of contractor-provided access facilities (e.g., gateway router).
- c) Standard carrier/user demarcation point.
- d) Minimum Point of Penetration (MPOP) [FCC defined demarcation point].
- e) Desktop (e.g., telephone set, personal computer [PC]). contractor's POP.
- f) Wireless phones and satellite earth stations.

Services may or may not have a physical SDP, depending on the characteristics of the individual services.

#### **C.2.1.3.1 Premises Wiring/Cabling**

Premises wiring/cabling may be required within a building and/or between buildings in a campus or military base environment to reach the SDP. If existing wiring/cabling is to be used, the contractor shall verify that all such wiring/cabling meets the technical standards for the services being provided (e.g., U.S. cabling and safety standards and guidelines as published by American National Standards Institute (ANSI) Electronic Industries Association/Telecommunications Industries Association (EIA/TIA) 568/569/606/TSB-36/TSB-40, ANSI/National Fire Protection Association (NFPA)-70, EIA-T568A, Telcordia GR-409, and ISO/IEC 11801). However, for non-domestic locations, the contractor shall follow country-specific applicable wiring/cabling standards and guidelines. If the existing or installed wiring/cabling does not meet technical standards at initial service delivery, the contractor shall identify the standards to the user. This verification and identification shall be at no additional cost to the Government.

The contractor shall be responsible for isolating and identifying to the user any service problem caused during or after acceptance of the service by the existing or installed wiring/cabling so that user can rectify the wiring/cabling problem. However, the

contractor will not be responsible for rectification of problems associated with existing premises wiring/cabling, except for wiring/cabling installed by the contractor.

If installation of new wiring/cabling is required for initial service delivery and when provided with appropriate authority by the Agency, the contractor shall order wiring/cabling from the Agency's designated provider. In addition, the contractor shall also coordinate installation, trouble reporting, and trouble rectification of wiring/cabling with the entity selected by the user for inside wiring for the acceptance of the service delivery.

When requested by the Agency, the contractor shall provide premises wiring/cabling from the standard commercial demarcation to the designated SDP location. The contractor shall provide a warranty period of at least 30 calendar days for the premises wiring/cabling after service acceptance.

#### **C.2.1.4 On-Net and Off-Net Locations**

The contractor shall provide services to on-net and off-net locations as described in the individual service specifications presented in Section C.2. Unless otherwise specified, on-net and off-net locations are as defined in Attachment J.11.

#### **C.2.1.5 Access**

Access is the means for providing connection for on-net locations between an SDP and the backbone-network POP. There are two ways of providing an access connection using:

1. Access Arrangements
2. Access Services

Access Arrangements are a component of an ordered Telecommunications Service to facilitate proper service delivery and can not be ordered as a stand alone access service. When a Telecommunications Service is ordered on Networx Enterprise, the service shall be delivered by the contractor either at 1) an SDP located at the customer's premise or 2) the contractor's POP (with access provided by the Government via separate means). In this contract, Access Arrangements provides the convention to specify and price the originating and/or terminating access component required to connect the SDP to the contractor's POP when that access component is required to deliver a Telecommunications Service. Since Access Arrangements are a component of an ordered Telecommunications Service which contains service delivery metrics, there are no separate Performance metrics specified for Access Arrangements. Access Arrangements are specified in Section C.2.16

Access Services (See Section C.2.13) provide connections between SDPs and the Agency-designated network POPs. Like any other services (e.g., Internet Protocol Service), Access Services (e.g., Wireline Access Service) also provide performance metrics. Access services can be used for connecting to any Government designated-network, including other Networx contractor's network.



### C.2.1.6 Performance

#### C.2.1.6.1 Standardized Performance Metrics

All Network services, except for Dark Fiber Service (DFS), have specified a standard set of common metrics or Key Performance Indicators (KPIs) to measure and report their performance. This standard set of KPIs measures the primary dimensions an Agency needs in order to evaluate service effectiveness. The underlying KPI computations are service specific or context sensitive (as defined within each service) to reflect the broad range of service offerings and the Network focus on delivery of end to end services. The eight standard KPIs used for services as specified within this contract are defined in Section C.2.1.6.1.1 below.

##### C.2.1.6.1.1 Standard Key Performance Indicators

No.	Key Performance Indicator	Abbreviation
1	Availability (Service)	Av (S)
2	Time to Restore	TTR
3	Grade of Service(Service)	GOS(S)
4	Bit Error Rate	BER
5	Latency(Service)	Latency(S)
6	Jitter	Jitter
7	Event Notification	EN
8	Response Time	RT

For certain services, when required by Agency customers, two service levels are specified. *Routine* service levels apply for most Government applications. *Critical* service levels are defined for Agency applications requiring higher levels of availability, performance, or restoral criteria. The parameters specified in the service descriptions shall apply to all domestic (both CONUS and OCONUS) services. Performance parameters for non-domestic services are specified in Section C.2.1.9. In addition, the performance provided shall always be at a level not less than what is generally available commercially at no additional cost to the Government. Thus, if the available commercial performance parameter is more demanding than the minimum acceptable level specified in this contract, the available commercial performance parameter shall prevail.

#### C.2.1.6.2 Special Performance Requirements for Telecommunications, Special and Wireless Services

All technical performance requirements for Telecommunications, Special, and Wireless services are specified on an SDP-to-SDP and/or POP-to-POP basis. The contractor shall meet the specified performance levels regardless of traffic congestion in the contractor's commercial or other private networks. The end points of the contractor's responsibility for performance will vary based on whether access arrangements are being provided by the contractor or by the Agency. There are three possible scenarios for service delivery as shown in Figure C.2-3. The SDPs at both ends of a circuit may be located on user premises, as shown in Figure C.2-3 (a), or the SDP at one or both ends may be located at the contractor's POP, as shown in Figure C.2-3 (b) and (c). The

contractor must deliver service which meets the service specified performance requirements in all three cases.

Unless otherwise authorized by the Government, the delivery point (usually the SDP) at which the performance levels are measured (for KPI/AQL or SLA purposes) for a service is the network side of the User to Network Interface.

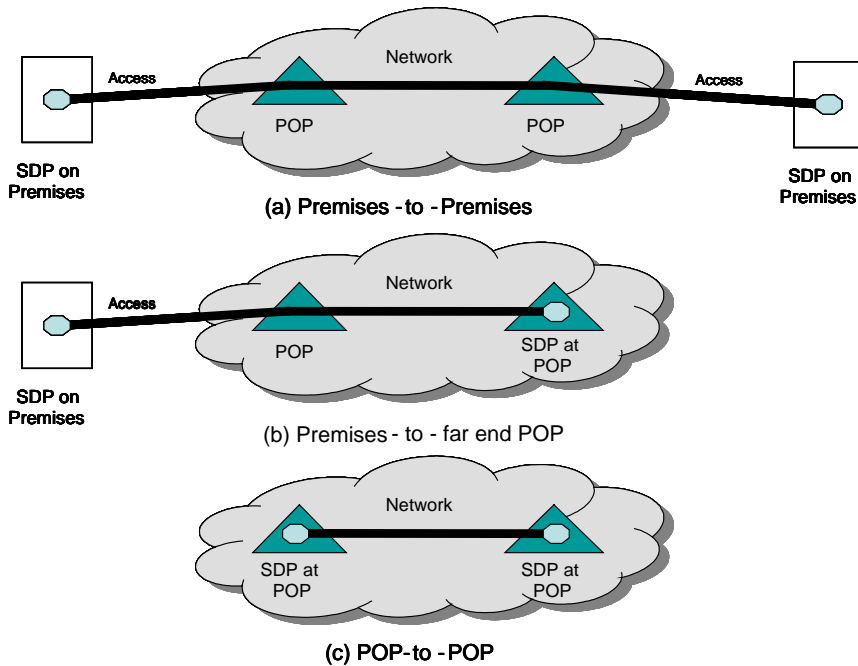
When an agency orders a service in which the technical performance requirements are specified on an SDP-to-SDP basis<sup>1</sup> and where the contractor requires the use of SEDs to meet the requirements and/or requires access to, or use of, the agency's customer-premises equipment or software to meet the requirements, the ordering agency may (1) elect to not order such SEDs and/or (2) elect to not permit contractor access to, or any use of, the agency's customer-premises equipment or software for such purposes.

In these situation(s) and unless otherwise agreed to by the contractor and the user agency, the contractor, when directed by the user agency or by GSA, shall monitor, measure, and report the performance of the service for KPI/AQL and for SLA purposes either (1) on an SDP-to-SDP basis, by defining the SDP for performance metric measurement purposes for affected location(s) as being located at the connecting POP(s) of the location(s), or (2) on a POP-to-POP basis. If directed to use the latter method, the contractor shall comply with the following:

- (1) For all IP-based network services, the applicable POP-to-POP performance requirements to be used shall be those defined in Section C.2.4.1 (IPS).
- (2) For emulated FRS and ATMS, the contractor shall monitor, measure, and report the frame or cell-based performance metrics (for FRS see Table C.2.3.1.4.1; for ATMS see Table C.2.3.2.4.1) on the customer side of the provider edge equipment at the POP or as otherwise agreed to by the contractor and the user agency.
- (3) For all other services, the service-specific SDP-to-SDP performance metrics shall be applied on a POP-to-POP basis unless a stipulated POP-to-POP performance metric already applies for the associated service(s).

---

<sup>1</sup> Including performance requirements specified on an end-to-end and/or agency premises-to-agency premises performance requirement basis.



**Figure C.2-3 End Points of the Contractor's Responsibility for Performance Management**

#### C.2.1.7 Service Enabling Devices (SEDs)

A Service Enabling Device (SED) is a unit of, or separately priced component within, contractor-provided and owned equipment used to meet the interface requirements for an individual service. In addition, it can be used to implement access aggregation and integration to provide a lower service delivery cost to the Government. A SED may also be a unit of, or separately priced component within, contractor-provided and owned equipment and/or software used to enable the requirements associated with the Management and Applications Services and Security Services. A SED shall only be offered as needed to provide delivery of a service that is acquired under this contract. Section B.4 provides details for SEDs.

#### C.2.1.8 Conformity to Standards

Throughout Section C, references are made to standards (including interim standards, Internet Engineering Task Force [IETF] Requests for Comments [RFCs], or defacto standards) as they existed at the time of contract award. If a standard is defined by a specific version and/or date, then that specific version of the standard shall be implemented. Otherwise, compliance with the latest versions of these standards is

expected. American National Standards shall supersede international standards for services to be provided to on-net users located in the U.S. Where multiple standards are cited, the order of precedence shall be industry forum specification (e.g., ATM Forum [ATMF]), followed by ANSI, followed by Telcordia, followed by ITU-TSS, unless otherwise specified.

#### **C.2.1.9 Non-Domestic Services**

The contractor shall supply services globally. Global coverage includes delivery of service from domestic SDPs to non-domestic SDPs, from non-domestic SDPs to domestic SDPs, and from non-domestic SDPs to non-domestic SDPs. The following requirements for numbering plan, features, performance, interfaces, security, and management and operations considerations that are applicable to the non-domestic services shall supersede the corresponding requirements specified for the domestic services:

(a) **Numbering Plan.** The numbering plan for non-domestic locations shall conform to country specific numbering plans.

(b) **Features.** All features identified as mandatory in each service description shall be provided to non-domestic SDPs when they become commercially available in the areas involved.

(c) **Dial-In.** The contractor shall support country-specific non-domestic PSTN numbers and/or toll free numbers, if commercially available, for dial-in access of services.

(d) **Performance.** The Key Performance Indicators (i.e., KPI) in the performance metrics for each service between non-domestic SDPs or between domestic and non-domestic SDPs shall be compliant with the best commercial values or practices for those parameters within the foreign (non-domestic) country(ies) and/or jurisdiction(s) hosting the non-domestic SDPs.

(e) **Interfaces.** When a service is delivered to an SDP at a non-domestic location, the User-to-Network Interfaces (UNI), i.e., interface type, payload data rate, protocol type, standard for the SDP shall comply with the country-specific interface standards when delivering service to the country-specific Government equipment. However, if the Government equipment conforms to a North American standard, then the UNI standard at the SDP shall comply with the North American standard where permitted by local law and regulations.

#### **C.2.1.10 Interoperability**

The contractor shall support interoperability for given service offerings so that a user of a service from one Network contractor shall be able to communicate with users of services from other Network contractors with performance equivalent to that commercially available. GSA recognizes that different levels of interoperability (i.e., partial or full) exist commercially, particularly in the area of data networking.

Interoperability shall be made available for any service that is currently commercially offered by the contractor and is interoperable with other Networkx contractors' service. The contractor shall notify GSA of the details of the level of interoperability available for the service. In addition, the contractor shall make available any future service interoperability at no additional cost to GSA when the contractor offers the interoperability for its regularly provided service commercially.

Since near full interoperability is provided via the Public Switched Telephone Network (PSTN) for switched services, the contractor shall support interoperability between Voice Services, Circuit Switched Data Service, Combined Services, and Wireless Services [Optional]. The contractor shall support interoperability of its Internet Protocol Services with the public Internet, and with Government IP networks. The contractor must also support connectivity and interoperability for remote and mobile users as specified in the individual service descriptions.

#### **C.2.1.11 Security Requirements for Networkx**

##### **C.2.1.11.1 Contractor Infrastructure**

Communications services under this contract will carry non-sensitive programmatic and administrative traffic, Sensitive But Unclassified (SBU) traffic, and higher levels of sensitive and/or classified traffic that has been encrypted by Agency users. Therefore, the contractor is required to provide basic security for all network services, as well as the network management systems and information systems and databases used to support those network services. Such security shall include protecting all network services, information, contractor infrastructure and information processing resources against threats, attacks, or failures of systems.

##### **C.2.1.11.2 Security Guidance**

Security shall comply with requirements as outlined in Section C.3.3.2 "Security Management," and Office of Management and Budget (OMB) Circular A-130. In addition, the contractor shall comply with the FCC "Network Reliability and Interoperability Council (NRIC), Focus Group 1A" Physical Security Recommendations

(specifically VI-IA-05 through VI-1A-10), ANSI T1.276-2003<sup>2</sup> and Telcordia security standards. In case of a conflict, the order of precedence is OMB Circular A-130, followed by NRIC Recommendations (VI-IA-05 through VI-1A-10), followed by ANSI T1.276-2003, followed by Telcordia security standards.

Additional mandatory policy guidance for managing the Network security infrastructure is found in:

- (a) E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
- (b) National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 199 – Standards for Security Categorization of Federal Information and Information Systems
- (c) NIST FIPS PUB 140 – 2, Security Requirements for Cryptographic Modules
- (d) Public Law 104-191, Health Insurance Portability & Accountability Act (HIPPA) of 1996

National Security and Emergency Preparedness (NS/EP) directives as contained in Sections C.5 and C.2.1.12.

#### **C.2.1.11.3 Agency Specific Protection**

Additional Agency specific security requirements will be defined by the specific Agency after contract award. Examples of such requirements are (a) DoD Systems; Defense Information Assurance Certification and Accreditation Process (DIACAP) – DoDI 8510.01. (b) National Security Systems; National Information Assurance Certification and Accreditation Process (NIACAP) – NTISSI-1000.

#### **C.2.1.12 Compliance with National Policy Directives**

The concept of a national telecommunications infrastructure is recognized in national policy statements and directives issued under the authority of the Executive Office of the President, Congress, the Department of Homeland Security (including the National Communications System) and other entities of the Federal Government. This telecommunications infrastructure is required to support the critical needs of the government under conditions of stress that range from crises and natural disasters (e.g., flood, earthquake) through declared conditions of National Security and Emergency Preparedness (NS/EP). Public safety and the economic well being of the nation also depend upon the availability of reliable and responsive telecommunications

---

<sup>2</sup> ANSI T1.276-2003 (*OAM&P Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*) was initially developed by the National Telecommunications Advisory Committee (NSTAC) and later refined and approved by Alliance for Telecommunications Industry Solutions (ATIS), an accredited body of the American National Standards Institute (ANSI).

services. Networx is a key component of the U.S. national telecommunications infrastructure.

GSA expects to effectively provide assurance for government users that services and other service elements (technical and management and operations related) acquired through Networx will be in compliance with national policy throughout the life of the contracts. The Networx contractor shall ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure. Specific national policy requirements include, but are not limited to:

- a. NS/EP requirements include a wide range of Executive Orders, Presidential Directives as promulgated by the Executive Office of the President, the Director of Homeland Security, the National Communications System and other government entities. Specific NS/EP requirements are presented in Section C.5
- b. Section 508, 1998 amendment to the Rehabilitation Act requires Agencies to make their information technology accessible to persons with disabilities. Specific section 508 requirements are presented in Section C.6. The Networx contractor shall ensure that services delivered support Federal Agencies as required to comply with Section 508, 1998 amendment to the Rehabilitation Act.
- c. OMB Memorandum M-05-22 directs that Agencies must transition from IPv4 Agency infrastructures to IPv6 Agency infrastructures (network backbones) by a predetermined date. The Networx contractor shall ensure that services delivered support Federal Agencies as required to comply with OMB IPv6 directives.
- d. Starting on October 1, 2014 (Federal Government fiscal year 2015) all Internet Protocol (IP)-Based services and Service Enabling Devices (SEDs) procured via the Networx acquisition program which make use of IP-Based Services or provide support for IP-Based Services must comply with the following standards and policies and directives to the greatest extent that they are applicable to the IP-Based service or Service Enabling Device, with the following allowable exceptions;
  1. If the procuring department/Agency's Chief Information Officer determine the need for and provides an explicit written waiver: (For example; the procuring Agency CIO provides an explicit written waiver if the agency requests SEDs that do not have commercially available IPv6 functionality).
  2. If the IP-Based service does not sit on the agencies' network but is instead provided on the Contractor's network, or is not provided on the public Internet.

IP-Based Service is defined in Networx Section C.2.1.1, figure C.2-1 to include the following; Premises-Based IP VPN, Network-Based IP VPN, Voice Over IP Transport, Content Delivery Network, Converged IP, IP Telephony, Internet Protocol, IP Video Transport, and Layer 2 VPN Service.

Standards and policies and directives;

- Federal Acquisition Regulation (FAR) requires acquisitions to adhere to U.S. National Institute of Standards and Technology (NIST) Special Publication 500-267, A Profile for IPv6 in the U.S. Government
- Federal Acquisition Regulation (FAR) requires acquisitions to adhere to declarations of conformance as defined in the USGv6 Test Program associated with U.S. National Institute of Standards and Technology (NIST) Special Publication 500-267, A Profile for IPv6 in the U.S. Government (reference NIST Special Publication (SP) 500-273, USGv6 Test Methods: General Description and Validation)
- The September 28, 2010 memorandum from the U.S. Chief Information Officer with subject: "Transition to IPv6"
- Office of Management and Budget Memorandum M-05-22, dated August 2, 2005 with subject: "Transition Planning for Internet Protocol Version 6 (IPv6)"
- Federal Chief Information Officers Council Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government

Increasingly, telecommunications policy and the national telecommunications infrastructure are being impacted by the convergence of telecommunications and information technology. Thus, policy directives in the areas of Electronic Government ("E-Gov"), Enterprise Architecture development, and Information Assurance, for example, may also have implications for telecommunications infrastructure. Additional policy requirements may be identified to the contractor. If contract modifications are required to meet new government-specific requirements, the contractor shall submit to the Administrative Contracting Officer (ACO) a technical approach and schedule for proposing these modifications within 30 calendar days after notification of the requirements.

## **C.2.2 Voice Services**

### **C.2.2.1 Voice Services (VS)**

The Federal Government has a large community of voice users throughout the U.S. public sector and also conducts a considerable amount of business with U.S. citizens, private sector firms, and foreign entities.

#### **C.2.2.1.1 Service Description**



**C.2.2.1.1.1 Functional Definition**

Voice Services support voice calls whether initiated from on-net locations or from off-net locations after verification of authorization code, to be connected to all on-net and off-net locations by direct station-to-station dialing.

**C.2.2.1.1.2 Standards**

Voice Services shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. ANSI T1.101
2. ANSI ISDN
3. ANSI SS7 standards
4. Telcordia Notes on the Networks, Issue 4, October 2000
5. All applicable Telcordia, ANSI, and ITU Standards
6. ITU-T E.164 as interpreted by the Industry Number Committee of ATIS
7. The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards when offered commercially.

**C.2.2.1.1.3 Connectivity**

Voice Services shall connect to and interoperate with:

1. Government specified terminations (such as single-line telephones, Secure Telephone Unit (STU) III, multiline key telephone systems, conference-room audio equipment, PBX, Centrex, T1 MUX, modem, FAX, and video teleconferencing system)
2. Public Switched Telephone Network (PSTN), including both wireline and wireless networks, in domestic and non-domestic locations
3. All other Network Universal and Network Enterprise VS Contractors' networks.
4. Inmarsat (terminal types A, B, M, Mini-M, and Aeronautical) for calls terminating to Inmarsat.

**C.2.2.1.1.4 Technical Capabilities**

The following Voice Services capabilities are mandatory unless marked optional:

1. Uniform numbering plan:
  - a. Unique directory number for all on-net Government locations, including support of existing FTS2001 numbers
  - b. PSTN (including both wireline and wireless networks) numbers and any future changes to PSTN numbers
  - c. Non-commercial Agency specific private 700 numbers [Optional]
    - i. Transparency and interconnectivity between the contractor's network and other networks (see Section C.2.2.1.1.3, Connectivity).

The contractor shall provide gateways between the networks as needed.

ii. Originating and terminating on-net calls. Incoming off-net calls from the PSTN shall be blocked unless an Agency specific request for the service gateway has been received and implemented.

d. Contractor's network-specific private numbers, including access to contractor's operators, trouble reporting, or other special applications.

2. Network Intercept. Network intercept to a recorded announcement shall be provided as an inherent network capability when a call cannot be completed. At a minimum, such announcements shall be provided for the following conditions:

- a. Number disconnected (disconnected number shall not be reassigned for at least 90 days for those situations where the contractor controls number assignment)
- b. Time out during dialing
- c. Network congestion
- d. Denial of access to off-net and non-US calls
- e. Denial of access to features

3. User-to-User Signaling Via ISDN D-Channel [Optional]. The contractor shall support user-to-user signaling, in accordance with ITU-TSS Q.931 standards, via the ISDN D-channel during a call.

4. Voice quality at least equal to 64 kbps PCM (standard: ITU G.711) Features  
The following Voice Services features in Section C.2.2.1.2.1 below are mandatory unless marked optional:

**C.2.2.1.1.5 Voice Services Features**

ID Number	Name of Feature	Description
1	Agency-Recorded Message Announcements (Optional)	<ol style="list-style-type: none"> <li>1. Authorized Government personnel shall be able to record message announcements within the network after authentication of user-ID and password/token.</li> <li>2. The recording shall be assigned an on-net number and shall be accessible from on-net and off-net stations.</li> <li>3. The contractor shall provide the capability of a three-minute message announcement length.</li> <li>4. The length of each message provided by the Government will be determined on a case-by-case basis and will continue to three minutes in length (or longer if the contractor capability exists and is provided at no additional cost to the Government).</li> <li>5. A call to the announcement must be answered within five rings and barge-in access to the announcement shall be permitted.</li> <li>6. The contractor shall provide a system-wide capability for storing a minimum of 500 recorded messages.</li> <li>7. The contractor shall enable a minimum of 250 callers concurrently to access an announcement.</li> </ol>
2	Authorization	The contractor shall provide authorization codes. The authorization code

ID Number	Name of Feature	Description
	Codes/ Calling Cards	<p>shall support the following functionalities:</p> <ol style="list-style-type: none"> <li>1. Caller identification and class-of-service (COS) for users to include call screening (see User's Call Screening feature) and service performance levels (see Performance Metrics for routine and critical users). At a minimum, 128 classes of service shall be available to each user, station, or trunk.</li> <li>2. Same authorization code for originating on-net, off-net, and audio conference calls.</li> <li>3. Use authorization code if originating station identification cannot be made by other means for billing and COS purposes.</li> <li>4. Use authorization code when override capabilities are desired.</li> <li>5. The COS derived from an authorization code shall take precedence over that derived from any other means.</li> <li>6. When an authorization code is used for the service, it shall be verified without involving an operator before a call is connected.</li> <li>7. The Government will specify the following:               <ol style="list-style-type: none"> <li>a. Actual requirements for calling party identification (e.g., ANI suppression).</li> <li>b. COS assignment.</li> <li>c. Types of calling cards:                   <ol style="list-style-type: none"> <li>1. Post-paid calling cards.                       <ol style="list-style-type: none"> <li>1. Charges accumulate as the card is used and billing is based upon monthly charges.</li> <li>2. Limit on the amount of dollars billable either in total or in a billing period.</li> </ol> </li> <li>2. Pre-paid calling cards.                       <ol style="list-style-type: none"> <li>1. Fixed dollar amount in various increments, e.g., \$10.00, \$50.00, and \$100.00, etc.</li> <li>2. Rechargeable dollar amount where amount can be renewed or increased when the initial amount balance is low or depleted</li> </ol> </li> </ol> </li> <li>d. Expiration date for pre-paid calling cards.</li> <li>e. Use for audio conferencing service (ACS) only.</li> <li>f. Agency specific logo or no printing of FTS logo on the card.</li> <li>g. Suppression of call detail records (CDRs).</li> <li>h. Immediate cancellation of the card if reported stolen or lost by a user without incurring further charges on the card.</li> </ol> </li> </ol> <p>The format of the authorization code shall be determined by the contractor and shall support/provide the following capabilities:</p> <ol style="list-style-type: none"> <li>1. Credit card-sized authorization code card(s), also called Calling Cards, unless otherwise directed by the Government.</li> <li>2. Durable plastic composition and imprinted with authorization code, user's name, and organization. Magnetic strip (swipe) coding [optional]</li> <li>3. User instructions shall be issued, as directed by the Government, at no additional cost.</li> <li>4. Safeguards as follows:               <ol style="list-style-type: none"> <li>a. Potential fraud and theft regarding issuance, distribution, and activation of authorization codes.</li> <li>b. Delivery of Personal Identification Numbers (PINs)</li> </ol> </li> </ol>

ID Number	Name of Feature	Description
		<p>independent from delivery of the calling cards.</p> <p>c. Exclusion of the last 4 digits of authorization codes, i.e., PINs, in billing records.</p> <p>5. If sufficient space is available, inclusion of the Federal Relay Service's "TDD/800-877-8339" number on the back of the calling card.</p> <p>6. contractor-defined dialing sequence that alerts the network when an authorization code is about to be entered so that processing of calls not requiring this feature are not delayed.</p> <p>7. Temporary override of a COS restriction assigned to a caller's station. This will allow an individual user to place a call at a higher network COS for the duration of the call by entering a valid authorization code. This capability shall have the following functionalities.</p> <p>a. Absence of excessive delays caused by waiting for all digits to be dialed before recognizing the call as one that involves an override.</p> <p>b. Inclusion of all CDR relevant data charged to the authorization code rather than to the originating station.</p> <p>8. Allowance of authorized users to gain access, after validation of authorization codes, to on-net VS and features from off-net locations by dialing certain contractor-provided toll free and message unit-free (to the callers) commercial directory numbers. This capability shall have following functionalities.</p> <p>a. Numbers may be a local number, a Foreign Exchange number, an NANP number, or some other service type, e.g., toll free service, for which toll free and message unit-free service has been arranged for predesignated regions.</p> <p>b. Toll free and message unit-free commercial directory numbers shall be printed on the back of the calling card.</p> <p>c. Region boundaries shall be defined by the contractor.</p> <p>d. Users shall be able to select, by service order, the regions of the country from which access is to be allowed and the service type that provides the most economical service for a given application.</p> <p>9. A multiple call feature that shall allow the user to dial a code (e.g., the "pound" key [#]) after a call in order to make multiple calls without re-dialing the access and card number.</p> <p>10. Direct operator access to provide assistance with dialing or for providing information.</p> <p>11. An error correction feature that enables cardholders to correct a dialing mistake by pressing a key, e.g., the "star" key (*) and re-enter the correct number.</p> <p>12. A speed dialing option that allows cardholders to use abbreviated dial codes for frequently dialed numbers.</p> <p>13. Availability of all administrative tools or management reports made available by the contractor with equivalent commercial calling card offerings.</p> <p>14. Allow users to enter an authorization code by voice [optional]. The contractor may require a unique dialing sequence for this functionality.</p>
3	Caller	The contractor shall provide the calling number to the terminating station

ID Number	Name of Feature	Description
	Identification (ID)	for each incoming call.
4	Call Screening for users (Optional)	<p>Call screening consists of a set of features that determine a call's eligibility to be completed as dialed based upon COS information associated with the user, the station, or the trunk group. The following call screening features shall be supported:</p> <p>1. <u>Class of Service (COS) and Restrictions.</u> The contractor shall provide a minimum of 128 classes of service for each user, station, or trunk.</p> <p>COS shall be determined from the ANI, authorization code, traveling classmark, or trunk group. The COS derived from an authorization code shall take precedence over that derived from other means. Classes of service shall identify but not be limited to access and feature restrictions as follows:</p> <p>(i) Access restrictions shall include but not be limited to access to toll free and 900 calls, access to off-net calling, access to other Government networks, access to non-US calling, and access to other than specified NPA/NXXs.</p> <p>(ii) Feature restrictions shall allow or restrict access to network features by users or groups of users.</p> <p>2. <u>Time of Day.</u> Time of day, day of week, and day of year restrictions shall be possible and executable on a per station, per location, and per authorization code (overriding the COS of the calling station) basis. As an example, this type of restriction can be used to prevent unauthorized use of the service after normal business hours. (Optional)</p>

ID Number	Name of Feature	Description
		<p>3. <u>Traveling Classmark</u>. The contractor shall enable acceptance of traveling classmarks from all locations served by PBXs and Centrexes that are able to provide these classmarks including calls extended by operators. Traveling classmarks (TCOS) shall conform to the TCOS format (i.e., called number + TCOS). User calling characteristics and limitations may be determined from the traveling classmark. (Optional)</p> <p>4. <u>Code Block</u>. The contractor shall screen and prevent ineligible users, stations, and trunks with certain class-of-service access restrictions from calling specified area codes, exchange codes, and countries. Blocked calls shall be intercepted to appropriate network recorded announcements.</p>
5	Customized Network Announcement Intercept Scripts [optional].	The contractor shall implement customized network intercept announcement scripts as requested by the Government. The contractor shall record the customized network announcements after obtaining Government approval of scripts.
6	Internal Agency Accounting Code (Optional)	<p>For calls involving an Networkx Calling Card or originating station with a special COS, the following capabilities shall be provided:</p> <ol style="list-style-type: none"> <li>1. Entry of additional (up to a maximum of eight) digits to identify internal Agency accounting codes for the call, i.e., these accounting codes will be transferred to the CDR with no further processing.</li> <li>2. CDRs shall reflect all relevant data on the call to include internal Agency accounting code digits.</li> <li>3. Calls shall be charged to the authorization code rather than to the originating station.</li> </ol>
7	Off-Net Information Calls	A user shall be able to call off-net directory assistance by dialing NPA-555-1212 or any other off-net directory assistance number. NPA also includes service access codes, e.g., 800, for this feature.
8	Operator Services	<p>Operators shall provide support services in English and Spanish and shall provide services in any other languages as requested by an Agency. This service shall be made available 24x7. Users shall not receive a busy tone when calling for operator services. Calls to operators shall be answered within five rings 90 percent of the time. The following services shall be provided by operators:</p> <ol style="list-style-type: none"> <li>1. Operators shall be available to assist users, including TDD/TTY users, encountering dialing difficulties while using the contractor's services. The operator shall remain on the line until the call has been connected.</li> <li>2. Operators shall provide callers with locator service numbers for all Agencies serviced by the Networkx contracts. Locator service numbers are Agency numbers from which callers can receive further information that enables them to complete the call. These numbers will be provided to the contractor by the Government and will be updated periodically. The contractor shall maintain its locator database for the Government.</li> </ol>

ID Number	Name of Feature	Description
		3. Operators shall be able to complete calls from authorized users from off-net and on-net locations. Operators shall be able to verify authorization codes given verbally by callers accessing the network and, upon confirmation, shall be able to complete the call
		4. A user shall be able to call an operator by dialing a special number to report and deactivate a stolen or lost authorization code or calling card, to obtain a credit adjustment for an interrupted call or a completed call to a wrong number, or for unsatisfactory transmission.
9	Support for Government travel cards (Optional)	The Government provides certain individuals with credit cards, i.e., travel cards, for use while traveling on official Government business. The contractor shall perform following functions: <ol style="list-style-type: none"> <li>1. If requested by the Government, coordinate directly with Government travel card contractor(s) to enable the travel card to make Network calls.</li> <li>2. If requested by the Government, provide Government travel card contractor(s) all necessary information so that this information can be included on the back side of the travel card.</li> <li>3. Bill any calls made with the aid of the travel card using the procedures specified in Section C.3.</li> </ol>
10	Suppression of Calling Number Delivery	Based on the COS of the originating station or Network Calling Card, the contractor shall inhibit the delivery of the calling number, i.e., ANI, by setting the Privacy Indicator at the originating end and honoring it at the terminating end. In addition, it shall be possible to block calling number delivery on a call by call basis by dialing a contractor provided code.

### C.2.2.1.2 Interfaces

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.2.1.3.1, are mandatory unless marked optional:

#### C.2.2.1.2.1 Voice Services Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Analog Line: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line - Loop Signaling
2	Analog Line: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line - Loop Signaling
3	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk - Loop Signaling (loop and ground start)
4	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk - Wink Start Signaling
5	Analog Trunk: Four-Wire (Std: Telcordia	4 kHz Bandwidth	Trunk - E&M Signaling

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
	SR-TSV-002275)		
6	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
7	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
8	Digital: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
9 (Non-US)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
10	Optical: SONET OC-1 (Std: ANSI T1.105 and 106) (Optional)	49.536 Mbps	SS7
11	Electrical: SONET STS-1 (Std: ANSI T1.105 and 106) (Optional)	49.536 Mbps	SS7
12 (Non-US)	Digital: E3 Channelized (Std: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
13	Digital Line: ISDN BRI S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 Kbps (2x64 Kbps)	ITU-TSS Q.931

### C.2.2.1.3 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Voice Services in Section C.2.2.1.4.1, are mandatory unless marked optional:

#### C.2.2.1.3.1 Voice Services Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Availability (SDP-to-SDP)	Routine	99.5%	≥ 99.5%	
	Critical (Optional)	99.95%	≥ 99.95%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
Grade of	Routine	0.07 (SDP-to-SDP)	≤ 0.07	See Note 3



Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Service (Call Blockage)		0.01 (POP-to-POP)	≤ 0.01	
	Critical (Optional)	0.01 (SDP-to-SDP & POP-to-POP)	≤ 0.01	

## Notes:

1. Voice Service availability is calculated as a percentage of the total reporting interval time that the voice service is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

[Note that this KPI is waived for calls made with calling card.]

2. Refer to Section C.3.3.1.2.4 for definition and how to measure.
3. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements (e.g., "All trunks busy" condition). For example, 0.01 indicates that 1 percent of the calls not being completed (1 out of 100 calls).

### C.2.2.2 Circuit Switched Data Service (CSDS)

As data and multimedia applications expand within the Government, requirements for digital connectivity on a dial-up basis will continue to increase. The Government currently has a large community of CSDS users, particularly in the area of on-demand video conferencing applications.

#### C.2.2.2.1 Service Description

##### C.2.2.2.1.1 Functional Definition

CSDS provides a synchronous, full duplex, totally digital, circuit-switched service at DS0 data rate; and optionally at higher data rates up to DS1, including integral multiples of DS0 data rates (i.e., NxDS0, where N = 1 to 24), to on-net and off-net locations.

##### C.2.2.2.1.2 Standards

Circuit Switched Data Service shall comply with the following standards, as applicable: After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. ANSI X3.189
2. ITU E.721
3. Applicable Telcordia and ANSI standards for digital transmission, including SONET
4. ITU-TSS and EIA standards for DTE interfaces

### C.2.2.2.1.3 Connectivity

Circuit Switched Data Service shall connect to and interoperate with:

1. Agency specified terminations such as Digital PBX, Intelligent MUX, Group 4 FAX, Video codec, and Workstation/PC.
2. PSTN (where available).
3. All other Network Universal and Network Enterprise CSDS Contractors' networks. [Optional]

### C.2.2.2.1.4 Technical Capabilities

The following Circuit Switched Data Service capabilities are mandatory unless marked optional:

1. Uniform numbering plan:
  - a. Unique directory number for all on-net Government locations.
  - b. Same uniform numbering plan as proposed for Voice Services and which shall be integrated with the Voice Services plan (refer to Section C.2.2.1.1, Service Description).
2. Authorization Codes for CSDS. Authorization codes for CSDS shall be the same as specified for Voice Services (see Section C.2.2.1.2.1-2, Features Authorization Codes).
3. For calls terminating to off-net locations, the bandwidth requested by the originating on-net location shall be limited to the bandwidth limitations in the PSTN between the contractor's network and the called location.
4. Calling capability that does not require scheduling.
5. Provision of network-derived clocking to the DTE or PBX/Multiplexer (MUX) at the SDP.
6. Following call establishment, all bit sequences transmitted by the DTE shall be transported as data/bit transparent and shall maintain data/bit sequence integrity.
7. Categories of dialable information-payload bandwidth are as follows:
  - a. **DS0 Category.** The dialable bandwidth shall be DS0 (i.e., 56 Kbps and 64 Kbps) data rate.
  - b. **DS1 Category.** The dialable bandwidth shall be DS1 (i.e., 1.536 Mbps) data rate. [Optional]
  - c. **Multirate DS0 Category.** The dialable bandwidth shall be NxDS0, where N= 1 to 24. [Optional]
8. For the Multirate DS0 category, the contractor shall provide the following [Optional] :
  - a. Appropriate dialing sequence for initiating calls with different bandwidths. [Optional]

- b. Transport of all bit sequences transmitted by the DTE as data/bit transparent after establishment of the dialing sequence. [Optional]

The following categories of dialable information-payload bandwidth are optional:

1. **Multirate DS1 Category.** The dialable bandwidth range shall be available from DS1 to N times DS1 data rates, where N varies from 2 to 27.
2. **DS3 Category.** The dialable bandwidth shall be DS3 (i.e., 43.008 Mbps) data rate.
3. **SONET Level-I (i.e., OC-1) Category.** The dialable information-payload bandwidth shall be SONET OC-1 (i.e., 49.536 Mbps) data rate.
4. **SONET Level-II (i.e., Multirate OC-1) Category.** The dialable information-payload bandwidth range shall be available from SONET OC-1 to N times OC-1 data rates, where N varies from two to three.
5. **SONET Level-III (i.e., Multirate OC-3c) Category.** The dialable information-payload bandwidth range shall be available from SONET OC-3c to N times OC-3c data rates (concatenated), where N varies from two to four. SONET OC-3c shall support information-payload data-rate of 148.608 Mbps.

#### C.2.2.2.2 Features

The following Circuit Switched Data Service features in Section C.2.2.2.1 are mandatory unless marked optional:

##### C.2.2.2.1 Circuit Switched Data Service Features

ID Number	Name of Feature	Description
1	Dial-In	Where available commercially, the contractor shall support toll free numbers, in addition to 10-digit PSN numbers, for dial-in access from off-net locations (i.e., PSN) via ISDN access arrangement. Access to CSDS shall only be provided after verification of the authorization code entered by the user.
2	User-to-User Signaling Via ISDN D-Channel [Optional]	User-to-user signaling via ISDN D-channel during a call shall be supported in accordance with ANSI T1 and ITU-TSS standards for ISDN and SS7.

#### C.2.2.2.3 Interfaces

The following User-to-Network-Interfaces (UNIs) at the SDP, as defined in the Section C.2.2.2.3.1, are mandatory unless marked optional:

##### C.2.2.2.3.1 Circuit Switched Data Service Interfaces

UNI Type	Interface Type and Standards	Payload Data Rate	Signaling Type
1	ITU-TSS V.35	56/64 Kbps; and optionally up to 1.536 Mbps	RS366A (dialing)

UNI Type	Interface Type and Standards	Payload Data Rate	Signaling Type
2	EIA RS-449	56/64 Kbps; and optionally up to 1.536 Mbps	RS366A (dialing)
3	EIA RS-530	56/64 Kbps; and optionally up to 1.536 Mbps	RS366A (dialing)
4	ISDN PRI (Multirate) (T Reference Point) (Standard: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
5	T1 (with ESF) (Std: SR-TSV-002275, and ANSI T1.102/107/403)	Up to 1.536 Mbps	SS7
<b>The Following optional interfaces are in the scope of the contract</b>			
6	T3 (Standard: Telcordia Pub GR-499-CORE)	Up to 43.008 Mbps	SS7
7	E1 (Standard: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
8	E3 (Standard: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
9	SONET OC-1 (Standard: ANSI T1.105 and 106)	Up to 49.536 Mbps	SS7
10	Electrical: SONET STS-1 (Standard: ANSI T1.105 and 106)	Up to 49.536 Mbps	SS7
11	SONET OC-3 (Standard: ANSI T1.105 and 106)	Up to 148.608 Mbps	SS7
12	SONET OC-12 (Standard: ANSI T1.105 and 106)	Up to 594.432 Mbps	SS7
13	ISDN BRI (Multirate) (S and T Reference Point) (Standard: ANSI T1.607 and 610)	Up to 128 Kbps	ITU-TSS Q.931

#### C.2.2.2.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of Key Performance Indicators (KPIs) for Circuit Switched Data Service in Section C.2.2.2.4.1, are mandatory unless marked optional:

#### C.2.2.2.4.1 Circuit Switched Data Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Availability (SDP-to-SDP)	Routine	99.5%	> 99.5%	
	Critical (Optional)	99.95%	≥ 99.95%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
Grade of Service (Call Blockage)	Routine	0.07 (SDP-to-SDP)	≤ 0.07	See Note 3
		0.01 (POP-to-POP)	≤ 0.01	
	Critical (Optional)	0.01 (SDP-to-SDP & POP-to-POP)	≤ 0.01	

Notes:

1. CSDS availability is calculated as a percentage of the total reporting interval time that the CSDS is operationally available to the Agency. Availability is computed

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

by the standard formula: . [Note that this KPI is waived for calls made with calling card.]

2. Refer to Section C.3.3.1.2.4 for definition and how to measure.
3. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements (e.g., "All trunks busy" condition). For example, 0.01 indicates that 1 percent of the calls not being completed (1 out of 100 calls).

#### C.2.2.3 Toll Free Service (TFS)

Agencies can utilize inbound Toll Free Service (TFS) as a convenient means of accessibility for different callers including citizens, non citizens, and Agency personnel. TFS includes a set of advanced service features and related voice applications to meet Agency needs for delivering services to their callers.

##### C.2.2.3.1 Service Description

###### C.2.2.3.1.1 Functional Description

Toll Free Service provides basic inbound toll free calling and offers advanced feature and call routing capabilities. TFS includes intelligent call routing and network based Interactive Voice Response (IVR) capabilities to enable Agencies to effectively manage inbound calls.

**C.2.2.3.1.2 Standards**

Toll Free Service shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. ITU-T standard E.164 as interpreted by the Industry Number Committee of the Alliance for Telecommunications Industry Solutions (ATIS). The contractor shall support the following numbering schemes:
  - a. For domestic (CONUS and OCONUS) service, numbering shall be consistent with 800, 888, 877, 866, and other toll free non geographic codes available from the SMS/800 database managed by Telcordia.
  - b. For non-domestic service, numbering shall be consistent with requirements or practices in the country in which the call originates.
2. ITU-T P.800 series of standards for telephone transmission quality.
3. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

**C.2.2.3.1.3 Connectivity**

Toll Free Service shall connect to and interoperate with the Public Switched Telephone Network (PSTN) including both wireline and wireless.

Toll Free Service utilizes underlying Voice Service (VS) for connectivity as delineated in Section C.2.2.1 (VS). TFS shall be offered for both dedicated and switched terminating access arrangements.

**C.2.2.3.1.4 Technical Capabilities**

The following Toll Free Service capabilities are mandatory unless marked optional:

1. The contractor shall act as the responsible organization or "Resp Org" for assignment and maintenance of toll free numbers if requested by the subscribing Agency.
2. The contractor shall support toll free number portability.
3. The contractor shall accommodate any presently assigned Agency toll free numbers and assign Agency requested "vanity" toll free numbers (e.g., 1-800-CALL GSA), if available, for TFS.
4. When requested by a subscribing Agency, the contractor shall provide Universal International Toll Free Number service (also known as Universal International Free Phone Number - UIFN). This shall enable the Agency to request a single, unique toll free number that is the same throughout the world (Where available commercially from participating countries). [Optional]

5. The contractor shall provide the capability for a single toll free number to terminate at multiple locations (SDP's) and multiple toll free numbers to terminate at a single location (SDP).
6. As a default measure, the contractor shall provide a busy signal or recorded announcement for all calls encountering network congestion and/or terminating egress congestion. The choice of providing a busy signal or recorded announcement shall be determined subscribing Agency.
7. The contractor shall provide a network intercept to recorded announcements as an inherent network capability when a call cannot be completed. At a minimum, such generic announcements shall be provided for the following conditions:
  - a. Time out during dialing.
  - b. Denial of access to features, and other related conditions.
  - c. Denial of access to non-domestic or restricted calls.
8. The contractor shall provide the capability for customized network intercept recorded announcements. The contractor shall offer options for the custom announcement to be (a) recorded by the contractor or (b) remotely by the subscribing Agency.
9. The contractor shall, at a minimum, provide the capability to have all announcements recorded in English and Spanish languages. Other languages shall be optional.
10. The contractor shall provide a referral message to callers of a disconnected toll free number. Upon a submission of a TFS disconnect order; the Agency shall have the option for a referral telephone number to be provided in an announcement message to callers of the disconnected toll free number.
11. The contractor shall provide Dialed Number Identification Service (DNIS). DNIS will enable multiple toll free numbers to be routed and uniquely identified on a shared trunk group. The contractor shall transmit DNIS digits, upon Agency request, prior to the delivery of a TFS call to uniquely identify the dialed toll free number. The DNIS digit length shall range from 3 to a maximum of 10 digits.
12. The contractor shall identify and provide the calling parties Automatic Number Identification (ANI) to assist Agencies with identifying malicious or emergency calls.

#### **C.2.2.3.2 Features**

The following Toll Free Service features in Section C.2.2.3.2.1 and Section C.2.2.3.2.2 below are mandatory unless marked optional.

The features in Section C.2.2.3.2.1 shall be capable of being used independently of each other or in any combination except where noted by the contractor. The combination of features associated with routing functions unique with each toll free number shall constitute a "Call Routing Plan". Call Routing Plans shall be subject to control by the subscribing Agency via the Routing Control feature described in this section.

#### C.2.2.3.2.1 Toll Free Service Features

ID Number	Name of Feature	Description
1	Agency based routing database (also known as Host Connect)	<p>The contractor shall provide the ability to route TFS calls or provide information based upon a query(s) of information provided by a database located at the subscribing Agency premise. The query(s) could be to single, redundant, or multiple databases, depending upon Agency specifications and the complexity of the application.</p> <p>The contractor shall implement and provide the appropriate interface and connectivity for the contractor's IVR application to successfully query and access a subscribing Agency's database(s). The IVR caller shall have the capability to retrieve, review, and modify information located on the Agency database based upon subscribing Agency needs. The Agency database(s) can be a (1) mainframe (e.g. IBM Systems 360/370/390/3090) or (2) server based relational database.</p> <p>If the database does not respond to the network query within 250 milliseconds, an Agency-defined default routing plan shall be used.</p>
2	Alternate Routing (also known as "Cascade" routing)	The contractor shall allow TFS calls to be re-routed on a pre-determined plan based upon availability of trunks (busy) at the terminating location, a maximum number of calls allowed in progress, or a pre-defined ring-no-answer condition. If none of the alternate terminations are able to receive the call, then the call shall be terminated to a (1) predefined announcement, or to a (2) busy signal, at the subscribing Agencies option.
3	ANI	Automatic Number Identification (ANI). The contractor shall allow transmission of the TFS caller's real time ANI information (full 10 digit number or non-domestic equivalent) to the subscribing Agency.
4	ANI Based Routing	The contractor shall enable TFS calls to be routed based upon the originating ANI of the caller. Default routing defined by the subscribing Agency shall be used if ANI is not available.
5	Announced Connect	The contractor shall provide a customized message to the called party, before the TFS caller is connected, and provides the called party with information about the caller (e.g. ANI, account number etc.). This feature is commonly referred to as a "whisper".
6	Announcements	The contractor shall provide TFS network based announcements with both generic and customized recordings. For customized recordings, the Agency shall have the option to record the custom announcement script or have the contractor record the script. At a minimum, the announcements should be available in



ID Number	Name of Feature	Description
		both (1) English and (2) Spanish. At an Agency's request, the contractor shall provide the option for a forced disconnect after the announcement recording is played.
7	Call Prompter	<p>The contractor shall allow TFS callers to be provided with informational messages and be routed according to information entered via DTMF signal or via speech. The contractor's call prompter shall provide, at a minimum, the following capabilities:</p> <ol style="list-style-type: none"> <li>1. Select pre-recorded announcement messages with the capability for announcements. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in English and other languages after obtaining subscribing Agency script approval.</li> <li>2. The contractor shall provide the ability to transfer out ("menu routing") during an announcement to an Agency-specified predefined termination and an option to return back an announcement/menu without needing to redial.</li> <li>3. The contractor shall support multi-tiered prompting (menus) such that another series of options can be provided to the caller after making the initial menu selection. Provide routing to an Agency designed default location if no caller input is entered.</li> <li>4. Leave caller information via DTMF signal or speech (e.g., names, addresses, account information, phone numbers) for transcription or reporting purposes. For speech transcription, the contractor shall provide: a) transmission of the recorded voice files and DTMF data for each transaction to the Agency and b) [Optional] Provide a report of caller responses that transcribes the caller provided information for the subscribing Agency based upon a subscribing Agency's needs and transmits it to the Agency. The contractor shall provide transcription reports from English and Spanish speaking callers.</li> </ol>
		<ol style="list-style-type: none"> <li>5. The contractor shall provide a capability that allows callers to hear and verify their names and addresses in an Agency-provided name and address database after the caller has entered their telephone number via DTMF, or based on the caller's ANI.</li> <li>6. The contractor shall provide a means for the subscribing Agency to retrieve caller-entered DTMF or speech messages.</li> <li>7. Upon Agency request, the contractor shall offer the option for</li> </ol>

ID Number	Name of Feature	Description
		<p>a forced disconnect after an announcement recording is played.</p> <p>8. The contractor shall provide features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats.</p>
8	Call Redirection	<p>The contractor shall enable TFS calls to be efficiently transferred by the contractor's network, no matter which platform the call is being re-directed from, from the called party/agent to another toll free number or any PSTN number by utilizing, at the Agency's discretion, any one of the three following modes of network level call transfer:</p> <ol style="list-style-type: none"> <li>1. Blind transfer (unsupervised).</li> <li>2. Verification by the agent and then transfer (supervised).</li> <li>3. Three-way conference and then transfer.</li> </ol> <p>The contractor shall ensure that there is no double billing for toll free calls which have been transferred using call redirection. This includes calls being redirected within the contractors' network from one operating platform to another operating platform.</p> <p>In addition, the contractor shall offer the ability to put the caller on hold and provide abbreviated dialing codes. The contractor shall state the amount of abbreviated-dial codes available for use with this feature. The contractor shall provide two options for music on hold during the call redirection – either contractor provided or from an Agency provided source.</p>
9	Computer Telephony Integration (CTI)	<p>The contractor shall provide CTI messaging capability that enables transfer of caller information and Agency-specified data between the TFS contractor and Agency-specified systems simultaneously with the associated inbound toll free call. This feature can be used to support a diverse set of applications such as screen pop/splash, intelligent call routing, enhanced reporting, third party call control, and multi-channel call blending solutions.</p> <p>A discovery meeting shall be required to gather requirements for an Agency's specific application. The output of the discovery meeting shall be a deliverable. At a minimum the contractor's deliverable shall include the following: '</p> <ol style="list-style-type: none"> <li>1. Scope of Work</li> <li>2. Proposed solution</li> <li>3. Roles and responsibilities</li> <li>4. Project plan and schedule</li> <li>5. Deliverables</li> <li>6. Cost estimate</li> <li>7. Project risk assessment</li> </ol> <p>The contractor shall provide the deliverable within five business days upon completion of the discovery meeting.</p>
10	Custom Call Records	<p>This feature shall be used in conjunction with the TFS Interactive Voice Response and Call Prompter features. The contractor shall provide individual call detail data records which include, at a minimum, the following data:</p>

ID Number	Name of Feature	Description
		<ol style="list-style-type: none"> <li>1. Date and time of TFS call</li> <li>2. Call duration</li> <li>3. Specific details regarding the call attempt (e.g., Menu options selected in an IVR or Call Prompter application)</li> <li>4. Call entered digits</li> <li>5. Call Disposition (busy, complete, no answer, blocked)</li> <li>6. Caller information (ANI - if available or DNIS)</li> <li>7. Toll free number dialed</li> <li>8. Flexible custom fields according to Agency needs</li> </ol> <p>The contractor shall provide a detailed description of each call detail record field including definitions of the data elements prior to activation of the feature. The format of the call record data shall be such that it can be easily imported into Agency databases or applications. The call records and a summary report should be available electronically on a daily, weekly or monthly basis as requested by the subscribing Agency.</p>
11	Day of Week Routing	The contractor shall enable TFS calls to be routed to different terminations or applications based upon the day of week.
12	Day of Year Routing (Holiday Routing)	The contractor shall enable TFS calls to be routed to different terminations or applications based upon the day of the year. A minimum of ten dates should be eligible during a twelve month period for day of year routing.
13	In Route Announcements	This feature shall allow TFS callers to hear an announcement during call setup without affecting the final termination/route of the call. At a minimum, announcements shall be available in either (1) English or (2) Spanish.
14	Interactive Voice Response (IVR)	<p>The contractor shall provide an automated application that provides TFS callers with information based upon input from either (a) DTMF key entries or (b) natural speech recognition. The contractor shall provide the minimum required capabilities listed below:</p> <ol style="list-style-type: none"> <li>1. Select pre-recorded announcement messages with the capability for announcements and offer the ability for a caller to opt out during an announcement to a predefined termination and an option to return back an announcement without needing to redial. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in English and other languages.</li> </ol>
		<ol style="list-style-type: none"> <li>2. Leave caller information via DTMF signal or speech (e.g., name, address, account information, etc.). For transcription of caller information, the contractor shall provide: a) transmission of the recorded voice files and DTMF data for each transaction to the Agency and b) [Optional] a report of caller responses that transcribes the caller provided information for the subscribing Agency based upon a subscribing Agency's needs and transmits it to the Agency. The contractor shall provide transcription reports from English and Spanish speaking callers</li> </ol>

ID Number	Name of Feature	Description
		<p>3. The contractor shall provide a means for the subscribing Agency to retrieve caller-entered DTMF or speech messages.</p> <p>4. The contractor shall query a database that delivers Agency-provided information to the caller. The database may be located at the subscribing Agency or, at the subscribing Agency's discretion, located at a contractor location and updated by the subscribing Agency. Provide a default routing or message (Agency option) if the database is unavailable.</p> <p>5. The contractor shall provide a capability to allow callers to hear and verify their names and addresses in an Agency-provided name, address, and zip code database after the caller has entered their telephone number via DTMF, or based on the caller's ANI. (Text to Speech).</p> <p>6. The contractor shall support speech recognition as a valid caller input. The contractor shall support at a minimum, all spoken numeric digits as well as "yes" and "no." English and Spanish language callers shall be supported. The contractor shall be able to accept and process, at a minimum, 95% of the above speech responses. Speech responses which are not accepted shall be routed to default location designated by the subscribing Agency.</p> <p>7. The contractor shall provide the capability to perform surveys (via DTMF or speech) to IVR callers. The surveys can be provided to all or a random percentage of callers according to Agency needs. Survey results shall be provided electronically to the subscribing Agency.</p> <p>8. The contractor shall provide a facsimile "fax back" capability (e.g. Fax Catalog application) that shall permit callers to retrieve Agency specific documents or forms. The contractor shall fax back the request documents within one hour of the initial call and retry a minimum of 13 attempts over a six hour interval in order to complete the request. Fax transmittal shall include an option for a cover sheet (standard or customized).</p> <p>9. At the Agency's option, the caller's IVR selection(s) information shall be transferred to the Agency.</p> <p>10. The contractor's IVR capacity must be configured such that the application answers a call within 3 ring cycles for 99 % of the</p>
		<p>offered call volume (measured on an hourly basis) during the busy hour.</p>

ID Number	Name of Feature	Description
		<p>11. The contractor shall provide features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats. These electronic form lines need not be voice feature enabled.</p> <p>12 The contractor shall provide summary reporting that at a minimum provides information on the caller, average call duration, caller opt out (transfer), and disposition of the calls within the IVR application on a daily, weekly, and monthly basis.</p>
15	Make Busy Arrangement	<p>The contractor shall permit the Agency to deactivate one or more TFS dedicated access trunks within a trunk group, Upon deactivation, the trunk(s) shall appear in a busy state. The capability to activate and deactivate the status of the trunks shall be controlled either via software available to the subscribing Agency or at the Agency's option by notifying the contractor. At a minimum, the request shall be executed by the contractor within one hour of request.</p>
16	Network Call Distributor	<p>The contractor shall provide advanced, intelligent call routing capabilities based upon real time status of each call center's operating conditions, agent skills, and/or Agency specified business rules. The contractor shall poll all of the subscribing Agency's PBX/ACD's regular intervals for real-time ACD operating status information to update a call routing processor which shall use call routing logic/algorithms that have been predefined by the Agency, to determine the best location or resource to deliver the inbound call.</p> <p>The call routing processor containing the call routing logic/algorithms shall be able to use, in the subscribing Agency's defined combinations, all real-time operating status information collected from the Agency's PBX/ACD's.</p> <p>The ACD-provided information shall be polled and shall include at a minimum:</p> <ol style="list-style-type: none"> <li>1. Number of incoming trunks</li> <li>2. Number of incoming trunks available to receive a call</li> <li>3. Number of calls in queue or queue size</li> <li>4. Average delay in queue</li> <li>5. Number of answering agents logged on</li> <li>6. Number of answering agents unavailable to answer a call</li> <li>7. Number of answering agents available to answer a call</li> <li>8. Number of answering agents available to answer a call by skill</li> <li>9. Longest available answering agent</li> <li>10. Average speed of answer</li> </ol>

ID Number	Name of Feature	Description
		<p>11. Average call handling time (includes agent talk time, after-call wrap-up time and call hold time)</p> <p>12. Number of calls abandoned</p> <p>13. Average time to abandonment</p> <p>The type of network information that shall also be available to the call routing processor for utilization by the call routing logic/algorithms shall include:</p> <ol style="list-style-type: none"> <li>1. The dialed toll-free number</li> <li>2. The caller's originating 10 digit number</li> <li>3. The caller's entered digits.</li> </ol> <p>Call routing logic/algorithms that shall be accommodated shall include at a minimum:</p> <ol style="list-style-type: none"> <li>1. Routing to the best available answering agent by skill group</li> <li>2. Routing based upon expected wait times</li> <li>3. Routing based upon least cost.</li> </ol> <p>The contractor shall document the maximum hourly call processing rate and grade of service available without any degradation in performance (e.g. can process 100,000 calls per hour).</p> <p>The contractor shall permit the call routing processor up to 250 milliseconds from receipt of a call query to respond to the destination (or next node). In the event that the 250 milliseconds is exceeded, the contractor shall route the call using a default routing plan previously defined by the subscribing Agency.</p> <p>The contractor shall provide, via a graphical user interface, all software and hardware necessary for subscriber Agency access to the call routing processor to permit Agency definition of the call routing logic/algorithms.</p> <p>The subscribing Agency will be responsible for providing telecommunications connections to the contractor's system.</p> <p>The Network Call Distributor feature shall be offered as a managed service with the following options:</p> <ol style="list-style-type: none"> <li>1. <u>Contractor-provided and contractor-based:</u> The contractor shall provide all necessary components required for the provision of this feature and they shall be housed within the contractor's network. (Default).</li> <li>2. <u>Contractor-provided and Agency-based:</u> The contractor shall provide all necessary components required for the provision of this</li> </ol>

ID Number	Name of Feature	Description
		<p>feature and they shall be housed at the subscribing Agency's designated location (Where applicable).</p> <p>3. <u>Agency-provided and contractor-based: [Optional]</u> All the necessary components required to the provision of this feature (including ACD) will be provided by the Agency or Agency specified contractor. The Agency equipment shall be housed and managed by the contractor. (Where applicable).</p> <p>4. The contractor shall provide any additional reporting or monitoring options that are available from the contractor's equivalent commercial service offering at no additional charge.</p>
17	Network Queuing [Optional]	The contractor shall enable TFS callers to remain, in a network queue, if resources are unavailable at the subscribing Agency. This is a feature that shall allow a caller to be held in queue in the contractor's network until a subscribing Agency's terminating SDP(s) become(s) available to receive the call. Upon entering the queue, the caller shall hear an initial announcement and shall then hear a reassurance announcement at a predetermined interval thereafter. The subscribing Agency shall be able to define the time for calls that can be held in queue before being sent to a terminating announcement. The contractor shall be responsible for recording announcements after subscribing Agency script approval.
18	NPA/NXX Routing	The contractor shall enable TFS calls to be routed to different terminations based upon the calling party's originating NPA or NPA/NXX or country code. Where NPA/NXX is not available, calls shall be routed to an Agency-defined default location.
19	Office Locator Database Service	The contractor shall enable a TFS caller to query a database that delivers Agency-provided information (e.g., specific information about the nearest Agency office is provided when a caller enters a Zip code; this information can include Name, Address, City, State, Zip code (NACSZ)). This feature can be used in conjunction with other features such as a call prompter, IVR application, or host connect for informational and call routing applications.
20	Operator Connect Bridging	The contractor shall enable TFS callers to access a contractor-provided operator for assistance. This feature can be used as a default termination in conjunction with other feature options such as Call Prompter and Interactive Voice Response.
21	Percentage Call Allocation	The contractor shall enable TFS calls to be allocated on a percentage basis and terminate at multiple locations. The Agency-specified percentage distribution can range from 0% to 100% in a minimum of 1% increments.
22	Real Time Reporting	The contractor shall provide Agencies with the ability to monitor and report on summary and detail data relating to the status of TFS calls on a near real-time basis (e.g., minimum required refresh rate of 30 seconds and at other contractor proposed intervals). The TFS reports and monitoring data shall be

ID Number	Name of Feature	Description
		<p>available electronically within 5 minutes of the request. The contractor shall provide all components necessary to present this information in a graphical and tabular format to the subscribing Agency and allow it to be exported to external applications (e.g., spreadsheet or database). The user will be responsible for providing connections to the contractor's real time monitoring system. A secure web based-interface is preferred.</p> <p>At a minimum, the contractor shall provide the following:</p> <ol style="list-style-type: none"> <li>1. The number of TFS calls from each area code who have dialed a given toll free number and average call duration.</li> <li>2. The total number of calls directed to a subscribing Agency's terminating SDP.</li> <li>3. The total number of calls directed to a subscribing Agency's terminating SDP(s) that could and could not be completed.</li> <li>4. The percentage of trunks busy at a users terminating SDP.</li> <li>5. Any standard real time reports or data available to commercial users.</li> </ol> <p>The contractor shall make available any reports available from its corresponding commercial service offering.</p>
23	Routing Control	<p>The contractor shall allow subscribing Agencies to perform real time and scheduled TFS call routing changes from their location or via the contractor's customer service center. This feature shall permit authorized users to review, create, validate, change, or execute call routing plans (or sets) from the subscribing Agency's premises or via request to the contractor's customer service center. Activation of a routing plan shall be executed within a period not to exceed five minutes of the request.</p> <ol style="list-style-type: none"> <li>1. The contractor shall provide adequate security procedures that will prevent unauthorized access to this feature.</li> <li>2. The contractor shall provide audit trail information to track the identity, time, and plan changes executed by a subscriber.</li> <li>3. The contractor shall provide any components necessary to enable the user to utilize this feature.</li> <li>4. Users may provide their own terminal equipment when it meets contractor-provided specifications.</li> </ol>
24	Service Assurance Routing	<p>The contractor shall route TFS calls to an announcement or a predefined alternate termination within five minutes of the Agency request if an emergency situation or service disruption occurs. The contractor shall complete routing requests to other types of terminations within thirty minutes of the request.</p>
25	Speech Recognition	<p>The contractor shall provide network based natural speech recognition applications with the ability to recognize spoken vocabulary, digits, zip codes, credit card numbers, account numbers, alpha numeric numbers, etc. At a minimum, the contractor shall offer capabilities in both (a) English and (b)</p>



ID Number	Name of Feature	Description
		Spanish.
26	Tailored Call Coverage	The contractor shall enable restriction of TFS calls originating from specific areas (country, state), telephone numbers (NPA, NPA/NXX, or ANI), or call type (Payphones). The originating caller should hear a standard announcement informing them of the restriction.
27	Time of Day Routing	The contractor shall enable routing of TFS calls to different terminations or applications based upon the time-of-day. At a minimum, at least 48 time-of-day intervals shall be offered.

#### C.2.2.3.2.2 Toll Free Service Features - Reports

The contractor shall provide TFS reports that provide the subscribing Agency with information about the status of calls placed to each toll free number and/or termination. The contractor shall provide this information on an (1) hourly, (2) daily, (3) weekly, (4) monthly, and (5) quarterly basis. Reports shall contain information summarized in 30 and 60 minute increments. Multiple report formats that further summarize the information by time zone or subscribing Agency region shall be made available where applicable. The reports shall be archived and available for a minimum of 90 days. Reports shall be made available by electronic means such as a Web site, or via e-mail or other contractor-proposed applications and have the capability to export data, in a standard file format, to Agency applications (e.g., spreadsheets, databases) for analysis. The reports shall be made available electronically within 30 minutes of the submitted request. The contractor shall also provide Agencies with documentation containing a description of the report, definition of the report fields, and instructions on how the Agency can effectively use the report(s) to manage TFS.

All time indicators within the report shall default to Eastern Time with presentation of hours using either a 24 hour clock or a 12 hour clock with an AM/PM indicator. There shall also be an option to provide the reports indicating the time zone of the TFS terminating location.

Each report shall contain standard information including:

1. Title of Report.
2. Date of Report.
3. Period covered by the Report.
4. Name of subscribing Agency.
5. Toll free number(s) included in the Report.

Listed in Section C.2.2.3.2.3 below are the minimum reporting requirements. They are mandatory unless marked as optional. The contractor shall also provide any historical or real time reports that are commercially available with their TFS reporting packages.

### C.2.2.3.2.3 Toll Free Service Features – Reports

ID Number	Name of Feature	Description
28	Call Status Report – <u>Toll Free Service</u>	<p>For any given toll free number, the contractor shall, at a minimum, provide the following information within the reports:</p> <ol style="list-style-type: none"> <li>1. The number of calls from each area code and/or State that dialed the toll free number. A minimum of three views shall be available:               <ol style="list-style-type: none"> <li>a. calls originated by area code</li> <li>b. calls originated by State</li> <li>c. sorted by State and area code</li> </ol> </li> <li>2. The number of calls and the percentage of all calls that encounter a busy signal or that are blocked:               <ol style="list-style-type: none"> <li>a. Within the contractor's TFS network</li> <li>b. At the user's (Agency's) terminating access location</li> </ol> </li> <li>3. The number of calls offered to the user TFS trunk group</li> <li>4. The number of calls received at each user's terminating access</li> <li>5. The number of received calls at each user's terminating access that resulted in successful answerback supervision</li> <li>6. The average duration of calls answered at each user's terminating access</li> <li>7. The average duration of all calls answered for a given toll free number at all terminations serving the toll free number.</li> </ol>
29	Call Status Report – <u>Alternate Routing</u>	<p>For any given toll free number utilizing Alternate Routing, the contractor shall, at a minimum, provide the following information within the reports:</p> <ol style="list-style-type: none"> <li>1. The total number of calls offered to the initial termination</li> <li>2. The number of calls that were re-routed to alternate SDP(s) or toll free service trunk group(s).</li> </ol>
30	Call Status Report – <u>Announcement</u>	<p>For any given toll free number utilizing Terminating Announcement or In-Route Announcements, the contractor shall, at a minimum, provide the following information within the reports:</p> <ol style="list-style-type: none"> <li>1. The number of calls offered to the announcement</li> <li>2. The number of calls blocked at the announcement</li> <li>3. The number of calls completed in the announcement</li> <li>4. The average duration of calls to each announcement</li> </ol>

ID Number	Name of Feature	Description
		5. The number of abandoned calls for In-Route announcements.
31	Call Status Report – <u>Call Prompter</u>	<p>For any given toll free number utilizing Call Prompter Access, the contractor shall, at a minimum, provide the following information within the reports:</p> <ol style="list-style-type: none"> <li>1.The number of calls offered to the call prompter</li> <li>2.The number of calls to the call prompter that were abandoned without making a selection</li> <li>3.The average duration of all calls while in the call prompter</li> <li>4. The number and percentage of calls selecting each option within the call prompter application.</li> </ol>
32	Call Status Report - <u>IVR</u>	<p>For any given toll free number utilizing IVR, the contractor shall, at a minimum, provide the following information within the reports by application:</p> <ol style="list-style-type: none"> <li>1.The total number of calls offered to the IVR and average call duration</li> <li>2.The number of calls completed (i.e., successfully accessed) to the IVR</li> <li>3.The number and percentage of calls completed to the IVR but abandoned within the application</li> <li>4. The number and percentage of calls selecting each option</li> <li>5. The average duration of calls selecting each option</li> <li>6. For faxback applications, the fax delivery status and usage</li> <li>7. For survey applications, summary and detail information on call survey responses</li> <li>8. For transcription applications, summary and detail information regarding transcription usage.</li> </ol>
33	Caller Information Report	<p>The contractor shall provide a report that identifies the ANI information of all callers to a specified toll free number. Note: Agencies recognize that ANI, although available in most cases, is not always provided. In those instances where ANI is not available, the NPA or NPA-NXX (as available) of the caller shall be provided. Zeroes shall be substituted in place of any missing digits.</p> <p>For any given toll free number, the contractor shall, at a minimum, provide the following information regarding each call:</p>

ID Number	Name of Feature	Description
		<ol style="list-style-type: none"> <li>1.Date of call</li> <li>2.Time of call (expressed using either a 24 hour clock or a 12 hour clock with an AM/PM indicator, Eastern Standard Time)</li> <li>3.ANI of caller (if available)</li> <li>4.Dialed 10 digit number</li> <li>5.Duration of call</li> <li>6.Disposition of call (i.e., using an alpha or numeric code) to include, at a minimum, the following information:               <ol style="list-style-type: none"> <li>a. Call blocked within contractor's network</li> <li>b. Call blocked at user's terminating access</li> <li>c. Call completed to user's terminating access</li> <li>d. Other (not included in categories a – c above)</li> </ol> </li> </ol>
34	Caller Profile Report	<p>The contractor shall provide the following caller information.</p> <ol style="list-style-type: none"> <li>1. Lost Callers. The number of TFS callers who never called back after an incomplete attempt during the reporting period.</li> <li>2. Average Number of Attempts Per Caller. The grand total number of call attempts divided by the number of first call attempts during the reporting period.</li> <li>3. Average Number of Contacts Per Caller. The number of attempts generated from each telephone number on average during this reporting period. This is calculated by dividing the total number of first call attempts by the total number of unique telephone numbers from which the calls were made.</li> <li>4. 50 Percent of Successful Attempts. Represents the number of attempts to access the network for 50 % of the callers who completed during the requested measurement interval.</li> <li>5. 75 Percent of Successful Attempts. Represents the number of attempts it took to access the network for 75 % of the callers who completed during the requested interval.</li> </ol>
35	Call Redirection Report [Optional]	<p>The contractor shall provide a summary report on the call redirection activity by toll free number and abbreviated dial code (if applicable). At a minimum, the report should identify the following:</p> <ol style="list-style-type: none"> <li>1. Number of transfer attempts</li> <li>2. Number of completed transfers</li> </ol>

ID Number	Name of Feature	Description
		3. Number of incomplete transfers 4. Number of blocked transfers 5. Type of call redirection (blind, supervised, or 3 way) 6. Terminating number for redirection

### C.2.2.3.3 Interfaces

#### C.2.2.3.3.1 Network Interfaces

The existing User-to-Network Interfaces (UNIs) at the SDP, as defined in the Section C.2.2.3.3.2, are mandatory unless indicated otherwise:

#### C.2.2.3.3.2 Toll Free Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Analog Line: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line - Loop Signaling
2	Analog Line: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line - Loop Signaling
3	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk - Loop Signaling (loop and ground start)
4	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk - E&M Signaling, Wink start signaling
5	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
6	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
7	Digital: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
8 (Non-Domestic)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
9 (Optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7
10 (Non-Domestic)	Digital: E3 Channelized (Std: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
[Optional]			
11	Digital Line: ISDN BRI S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 Kbps (2x64 Kbps)	ITU-TSS Q.931

#### C.2.2.3.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI's) for Toll Free Services in Section C.2.2.3.4.1 are mandatory.

##### C.2.2.3.4.1 Toll Free Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Av(POP-to-terminating SDP)	Routine	99.5%	≥ 99.5%	
	Critical (Optional)	99.95%	≥ 99.95%	
Grade of Service (Call Blockage)	Routine	0.07	≤ 0.07	See Note 2
	Critical (Optional)	0.01	≤ 0.01	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Av(POP-to-POP) and Av (POP-to-terminating SDP) are measured and calculated as a percentage of the total reporting interval time that TFS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity within the contractor's TFS. For example, 0.01 indicates that 1 percent of the calls not being completed successfully (1 out of 100 calls).
3. See Section C.3.3.1.2.4 for definitions and measurement guidelines.

### **C.2.3 Frame & Cell Switched Services**

#### **C.2.3.1 Frame Relay Service (FRS)**

FRS provides reliable, high speed connectivity between user locations at contracted service levels. The service's flexibility and reliability make it an attractive alternative to private line networks.

##### **C.2.3.1.1 Service Description**

###### **C.2.3.1.1.1 Functional Definition**

FRS provides connection-oriented, data transmission at data rates up to DS3. The Government will purchase bandwidth by specifying the Committed Information Rate (CIR), which is the user's guaranteed minimum transmission rate for a Permanent Virtual Circuit (PVC). FRS enables bursting above the CIR up to the capacity of the access circuits.

###### **C.2.3.1.1.2 Standards**

FRS shall comply with the following standards, as applicable, and when commercially available. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards

1. ANSI T1.606/614/617/618
2. ITU TSS I, Q, and X series recommendations for the provision of FRS and the North American adaptations of these recommendations as defined by the T1 Committee of the Alliance for Telecommunications Industry Solutions (ATIS) (formerly the Exchange Carrier Standards Association [ECSA])
3. Frame Relay Forum implementation agreements to include:
  - a. FRF.1.2 — PVC User-to-Network (UNI)
  - b. FRF.2.2 — Frame Relay Network-to-Network Interfaces (NNI)
  - c. FRF.3.2 — Frame Relay Multiprotocol Encapsulation
  - d. FRF.4.1 — SVC User-to-Network Interface (UNI)
  - e. FRF.5 — Frame Relay/ATM PVC Network Interworking
  - f. FRF.6.1 — Frame Relay Service Customer Network Management (MIB)
  - g. FRF.7 — Frame Relay PVC Multicast Service and Protocol Description
  - h. FRF.8.1 — Frame Relay/ATM PVC Service Interworking
  - i. FRF.9 — Data Compression over Frame Relay

- j. FRF.10.1 — Frame Relay Network-to-Network Interface SVC
  - k. FRF.11.1 — Voice over Frame Relay
  - l. FRF.12 — Frame Relay Fragmentation
  - m. FRF.13 — Service Level Definitions
  - n. FRF.14 — Physical Layer Interface
  - o. FRF.15 — End-to-End Multilink Frame Relay
  - p. FRF.16.1 — Multilink Frame Relay UNI/NNI
  - q. FRF.17 — Frame Relay Privacy
  - r. FRF.18 — Network-to-Network FR/ATM SVC Service Interworking
  - s. FRF.19 — Frame Relay Operations, Administration and Maintenance
  - t. FRF.20 — Frame Relay IP Header Compression
4. Internet Engineering Task Force (IETF) RFCs
  5. North American ISDN Users' Forum (NIUF)
  6. MPLS/Frame Relay Alliance as standards become commercially available
  7. Additionally, all new versions, amendments, and modifications made to the above listed documents and standards, as they become commercially available.

#### **C.2.3.1.1.3 Connectivity**

FRS shall connect Government and Government specified locations at service delivery points (SDPs) via customer's routers, layer 2/3 switches, multiplexing/switching devices, computers, and other frame relay access devices (FRADs).

#### **C.2.3.1.1.4 Technical Capabilities**

The following FRS capabilities are mandatory unless marked optional:

1. The contractor shall support provisioning over PVCs between SDPs.
2. The contractor shall support a maximum frame size of 4096 bytes.
3. The contractor shall support variable length frames.
4. The contractor shall support provisioning of:
  - a. Single point-to-point virtual connection.
  - b. [Optional] Multiple point-to-point virtual connection.
5. The contractor shall support multiple CIR options from 0 to DS3. The contractor shall:
  - a. Support PVCs that can utilize the full capacity of the access circuit.
  - b. [Optional] Accommodate multiple PVCs with CIR values, which when totaled can add up to the full bandwidth of the access circuit.
6. Reserved.



### C.2.3.1.2 Features

The FRS features in Section C.2.3.1.2.1 are mandatory unless marked optional.

#### C.2.3.1.2.1 FRS Features

ID Number	Name of Feature	Description
1	Class of Service (CoS)	<p>The contractor shall support CoS.</p> <p>CoS provides traffic differentiation by treating packets differently based on packet importance.</p> <ol style="list-style-type: none"> <li>1. Variable Frame Rate-real time (VFRrt) – highest queuing, lowest latency.</li> <li>2. Variable Frame Rate-non real time (VFRnrt) – standard delivery, minimal loss and delay.</li> <li>3. Unspecified Frame Relay (UFR) – basic service, lowest queuing.</li> </ol>
2	Disaster Recovery PVCs	The contractor shall provide pre-established PVCs to an alternate location upon notification by the Agency.
3	Frame-to-Internet Gateway	The contractor shall provide frame-to-Internet gateway services that allows users to put FR traffic and Internet connections on the same access circuit.
4	Interworking services	<p>The contractor shall provide interworking services to enable the customer's FRS to transparently access customer locations that use the following:</p> <ol style="list-style-type: none"> <li>1. The contractor's ATMS (the contractor's FRS/ATMS interworking shall support both ATM VBRnrt and ATM CBR (if provided).</li> <li>2. The contractor's IP services networks, e.g., network-based IP VPN services as described in Section C.2.7.3.</li> </ol>
5 (Optional)	IP-enabled FR	<p>The contractor shall support IP-enabled FR.</p> <p>The customer's interface to the network is IP over FR PVC. The PVC is terminated at service provider's edge switch/router. The contractor then routes the customer's IP traffic over its backbone network and the customer is provided any-to-any connectivity as needed.</p> <p>If the contractor's backbone is MPLS based, IP-enabled FRS with CoS support shall be provided.</p> <p>IP-enabled FR services allow end-users to retain the Frame Relay UNI in the access network and also serve as a migratory step toward IP. IP-enabled services also allow the provision of a full mesh network without each site having to establish separate PVCs to every other site.</p>

ID Number	Name of Feature	Description
6 (Optional)	Multilink Frame Relay	The contractor shall support Multilink Frame Relay (MFR).  MFR uses inverse multiplexing techniques to enable the bundling of several physical DS1 (or E1) lines into a single logical connection. With MFR, end-users (and service providers) can use existing network equipment and infrastructure to support more flexible access services at higher rates. [MFR is similar to Inverse Multiplexing for ATM (IMA).]
7 (Optional)	Switched digital access to FRS	The contractor shall support access via dial-up or ISDN will be at 64 Kbps, 128 Kbps, 256 Kbps, or 384 Kbps (Optional) in case of outages.
8 (Optional)	Voice over Frame Relay	The contractor shall support Voice over Frame Relay (VoFR).  VoFR service is enabled by the use of Frame Relay communications devices such as routers or FRADs configured with voice modules. In general, VoFR implementations utilize CIR/DE to prioritize voice over data traffic across Virtual Circuits.

### C.2.3.1.3 Interfaces

The following User-to-Network-Interfaces (UNI) at the SDP, as defined in Section C.2.3.1.3.1 are mandatory unless marked optional.

#### C.2.3.1.3.1 Frame Relay Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling or Protocol Type (See Note 3)
1	ITU-TSS V.35	Up to 1.536 Mbps	Frame Relay
2	ITU-TSS V.35	Fractional T1	Frame Relay
3 [Optional]	ITU-TSS V.35	Up to 1.536 Mbps	Asynchronous ASCII
4 [Optional]	ITU-TSS V.35	Up to 1.536 Mbps	IBM BSC
5 [Optional]	ITU-TSS V.35	Up to 1.536 Mbps	IBM SNA/SDLC
6 [Optional]	ITU-TSS V.35	Up to 1.536 Mbps	UNISYS Poll/Select
7	ITU-TSS V.35	Up to 1.536 Mbps	IPv4 and IPv6 (See Note 3)
8	All 802.3 cable and connector types	Up to 1.536 Mbps (See Note 1)	IEEE 802.3 IP/IPX
9	All 802.5 cable and connector types	Up to 1.536 Mbps (See Note 1)	IEEE 802.5 IP/IPX
10	EIA RS-232	Up to 56 Kbps	Asynchronous ASCII
11	EIA RS-232	Up to 56 Kbps	IBM BSC
12	EIA RS-232	Up to 56 Kbps	IBM SNA/SDLC
13	EIA RS-232	Up to 56 Kbps	UNISYS Poll/Select
14	EIA RS-232	Up to 56 Kbps	IPv4 and IPv6 (See Note 3)
15	EIA RS-422	Up to 1.536 Mbps	Frame Relay
16	EIA RS-422	Fractional T1	Frame Relay
17	EIA RS-422	Up to 1.536 Mbps	Asynchronous ASCII

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling or Protocol Type (See Note 3)
18	EIA RS-422	Up to 1.536 Mbps	IBM BSC
19	EIA RS-422	Up to 1.536 Mbps	IBM SNA/SDLC
20	EIA RS-422	Up to 1.536 Mbps	UNISYS Poll/Select
21	EIA RS-422	Up to 1.536 Mbps	IPv4 and IPv6 (See Note 3)
22	EIA RS-449	Up to 1.536 Mbps	Frame Relay
23	EIA RS-449	Fractional T1	Frame Relay
24 [Optional]	EIA RS-449	Up to 1.536 Mbps	Asynchronous ASCII
25 [Optional]	EIA RS-449	Up to 1.536 Mbps	IBM BSC
26 [Optional]	EIA RS-449	Up to 1.536 Mbps	IBM SNA/SDLC
27 [Optional]	EIA RS-449	Up to 1.536 Mbps	UNISYS Poll/Select
28	EIA RS-449	Up to 1.536 Mbps	IPv4 and IPv6 (See Note 3)
29	EIA RS-530	Up to 1.536 Mbps	Frame Relay
30	EIA RS-530	Fractional T1	Frame Relay
31	EIA RS-530	Up to 1.536 Mbps	Asynchronous ASCII
32	EIA RS-530	Up to 1.536 Mbps	IBM BSC
33	EIA RS-530	Up to 1.536 Mbps	IBM SNA/SDLC
34	EIA RS-530	Up to 1.536 Mbps	UNISYS Poll/Select
35	EIA RS-530	Up to 1.536 Mbps	IPv4 and IPv6 (See Note 3)
36 [Optional]	ISDN PRI (Multirate)	Up to 1.472 Mbps	Frame Relay
37 [Optional]	ISDN PRI (Multirate)	Up to 1.472 Mbps	IBM BSC
38 [Optional]	ISDN PRI (Multirate)	Up to 1.472 Mbps	IBM SNA/SDLC
39 [Optional]	ISDN PRI (Multirate)	Up to 1.472 Mbps	UNISYS Poll/Select
40 [Optional]	ISDN PRI (Multirate)	Up to 1.472 Mbps	IPv4 and IPv6 (See Note 3)
41	T3	Up to 43.008 Mbps	Frame Relay
42	Fractional T3	Up to 43.008 Mbps	Frame Relay
43	T3	Up to 43.008 Mbps	IPv4 and IPv6 (See Note 3)
44	High Speed Serial Interface (HSSI)	Up to STS-1 (49.536 Mbps)	Frame Relay
45	All IEEE 802.3 cable and connector types	Up to 43.008 Mbps (See Note 1)	IEEE 802.x (x=3,5) IPv6/IPX/SNA/IPv4
46	E3 (non-domestic)	Up to 30.72 Mbps	Frame Relay
47	E3 (non-domestic)	Up to 30.72 Mbps	IPv4 and IPv6 (See Note 3)
48 [Optional]	ISDN BRI (Multirate)	Up to 128 Kbps	Frame Relay
49 [Optional]	ISDN BRI (Multirate)	Up to 128 Kbps	Asynchronous ASCII
50 [Optional]	ISDN BRI (Multirate)	Up to 128 Kbps	IBM BSC
51 [Optional]	ISDN BRI (Multirate)	Up to 128 Kbps	IBM SNA/SDLC
52 [Optional]	ISDN BRI (Multirate)	Up to 128 Kbps	UNISYS Poll/Select
53 [Optional]	ISDN BRI (Multirate)	Up to 128 Kbps	IPv4 and IPv6 (See Note 3)
54	All IEEE 802.3 cable and connector types (non-domestic)	Up to 30.72 Mbps (See Note 1)	IEEE 802.x (x=3,5) IPv6/IPX/SNA/IPv4

## Notes:

1. Output data rate of a contractor-provided router connecting to a LAN.

2. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.
3. IPv6 shall be supported when offered commercially by the contractor.

**C.2.3.1.4 Performance Metrics**

The performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for FRS in Section C.2.3.1.4.1 below are mandatory unless indicated otherwise. All KPI measurements shall be SDP-to-SDP.

**C.2.3.1.4.1 Performance Metrics for Frame Relay Service**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
<b>GOS(Data Delivery Rate) (DDR)</b>	Routine	99.90%	≥ 99.90%	See Note 1
	Critical (Optional)	99.99%	≥ 99.99%	
<b>Latency (CONUS)</b>	Routine	120 ms	≤ 120 ms	See Note 2
	Critical (Optional)	90 ms	≤ 90 ms	
<b>Av(PVC)</b>	Routine	99.925%	≥ 99.925%	See Note 3
<b>Time to Restore</b>	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. The GOS(DDR) or throughput is based upon the total number of octets accepted by the network as a percentage of total octets successfully delivered by the network on a calendar monthly basis with associated CIR > 0. Relevant standard: FRF.13.
2. Latency is the end-to-end round trip delay experienced across the Network network. It reflects the transit time across a vendor’s frame relay network and is defined as “The amount of latency for octets to be carried through a frame relay network.”
3. PVC availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the PVC is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(PVC) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100.$$

4. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

### **C.2.3.2 Asynchronous Transfer Mode Service (ATMS)**

ATMS provides high-speed, reliable, and secure transport for data, video, and voice applications. ATMS may be delivered as Native ATM or as Emulated ATM, but not both.

#### **C.2.3.2.1 Service Description**

##### **C.2.3.2.1.1 Functional Definition**

ATMS provides a connection-oriented, transmission service with scalable port speeds of DS-1, DS-3, OC-3, and OC-12. In addition, ATMS provides E-1 and E-3 port speeds for terminations outside the United States.

##### **C.2.3.2.1.2 Standards**

ATMS shall comply with the following standards, as applicable, and when commercially available. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards.

1. ANSI T1
2. ITU TSS Recommendations
3. MFA Forum, formed to consolidate ATM Forum, Frame Relay Forum (FRF) and MPLS Forum, Implementation Agreements and Standards
4. Internet Engineering Task Force (IETF)
5. Reserved
6. Digital Subscriber Line (DSL) Forum Technical Reports for ATM
7. All new versions, amendments, and modifications made to the above listed documents and standards as they become commercially available.

##### **C.2.3.2.1.3 Connectivity**

ATMS shall connect customer locations via Agency routers, ATM edge switches, multiplexing/switching devices, PBX, or host computers.

##### **C.2.3.2.1.4 Technical Capabilities**

The following ATMS capabilities are mandatory unless marked optional

1. The contractor shall support ATMS [Native or Emulated] over PVCs and/or SVCs between SDPs. (SVCs are optional). Permanent Virtual Connections (PVCs) may be transported over ATM native networks or converged networks.

2. The contractor shall support Quality of Service (QoS) and/or Class of Service (CoS) levels on a per PVC/SVC basis, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage:
  - a. Constant bit rate (CBR) or its emulated equivalent to support jitter and latency sensitive applications. Constant Bit Rate is a mandatory requirement if the contractor provides native ATM service. Constant Bit Rate is an optional requirement if the contractor provides an emulated ATMS equivalent. The CBR performance metrics in Section C.2.3.2.4.1 are a mandatory requirement for native ATMS and emulated ATMS (if CBR is provided by the contractor).
  - b. Variable bit rate non-real-time (VBRnrt) or its emulated equivalent to support high priority business applications
  - c. Variable bit rate real-time (VBRrt) or its emulated equivalent to support medium priority business applications
  - d. [Optional] Available bit rate (ABR) or its emulated equivalent low priority business applications
  - e. Unspecified bit rate (UBR) or its emulated equivalent low business applications.
3. The contractor shall support bandwidth on demand via scalable Class of Service (CoS) to facilitate dynamic bandwidth management.
4. The contractor shall support provisioning as a point-to-point virtual connection. When migrating to or delivering over converged solutions, the provisioning of the PVC/SVC shall keep original traffic profiles or their equivalents.
5. The contractor shall support local access/Local loops.
6. The contractor's ATM edge switches or Provider Edge Routers (or other ATM access devices) shall be accessible by the Agency's network management systems via SNMP, or equivalent functionality, via a User Interface, for querying status, performance statistics, equipment configuration, and fault detection by the Agency's network management staff.
7. The contractor shall support multiple PVC/SVC speeds from 64 Kbps up to and including OC-12, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage.
8. The contractor shall support
  - a. Symmetrical PVCs
  - b. [Optional] Asymmetrical PVCs (which allows end users to specify varying bandwidths in each direction).
9. The contractor shall provide Virtual Path/Virtual Channel (VP/VC) addressing support. The contractor shall support the two-layered hierarchical addressing scheme for ATM PVCs. A virtual path is the highest order logical address and refers to a given group of channels on a link. A virtual channel is the lowest order logical address in ATM. The contractor shall enable the Agency to specify VPs and VCs as needed. When providing emulated ATM, address resolution/translation shall be supported if required by the subscribing Agency.

### C.2.3.2.2 Features

The ATMS features delineated in Section C.2.3.2.1 are mandatory unless marked optional otherwise.

#### C.2.3.2.2.1 ATMS Features

ID Number	Name of Feature	Description
1 [Optional]	Circuit Emulation Services	The contractor shall provide: <ol style="list-style-type: none"> <li>1. Circuit emulation services (CES) to enable TDM traffic to be terminated and efficiently transported via the ATM network to other sites before being converted back to TDM. When using CES, the ATM network shall provide a transparent transport mechanism for G.703/G.704 facilities. Voice and other voice-band traffic are encoded on standard TDM networks using PCM, ADPCM, or other encoding and compression mechanisms. (Refer to af-vtoa-0078.000)</li> <li>2. Dynamic Bandwidth Circuit Emulation (DBCES), which is a variation of CES. DBCES transmits only when there is an active voice call and does not send a constant bit stream of cells. (Refer to af-vtoa-0085.000)</li> </ol>
2	Disaster Recovery PVCs	The contractor shall provide pre-established PVCs to an alternate location upon notification by the Agency.
3	Port Diversity	The contractor shall enable the Agency to specify the following: <ol style="list-style-type: none"> <li>1. ATM Switch or Provider Edge Diversity. The contractor shall provide up to three mutually exclusive groups of ports that will not coexist on a single ATM Switch or Provider Edge Router. The ports may be provisioned using Automatic Protection Switching (APS) arrangements.</li> <li>2. Reserved.</li> </ol>
4	Interworking Services	The contractor shall provide interworking services for the Agency's ATMS to transparently access Agency locations that use the following: <ol style="list-style-type: none"> <li>1. The contractor's FRS.</li> <li>2. The contractor's IP services networks, e.g., network-based IP VPN services as described in Section C.2.7.3.</li> </ol>
5	Inverse Multiplexing for ATM (IMA)	The contractor shall connect from the SDP to the contractor's POP using IMA. IMA entails inverse multiplexing and demultiplexing of ATM cells in a cyclical fashion among links (nxDS1/E1) to form a higher bandwidth logical link whose rate is approximately the sum of the link rates. This is referred to as an IMA group. (Refer to af-phy-0086.001)
6	IP-enabled ATM	The contractor shall support IP-enabled ATM.  The Agency's interface to the network is IP over ATM PVC. PVCs are terminated at contractor's edge

ID Number	Name of Feature	Description
		switches. The contractor's backbone network carries the traffic. The Agency is provided any-to-any connectivity as needed.  The contractor shall provide CoS traffic differentiation, which treats packets differently based on customer-assigned importance markings, i.e., specific priorities and designated queues within the service provider's network.
7 (Optional)	Point-to-Multipoint PVCs	The contractor shall support Point-to-Multipoint PVCs.  Point-to-Multipoint PVCs enable end users to send one transmission to multiple locations simultaneously. Bandwidth requirements at the host are equal to the one transmission, not the aggregate total.

### C.2.3.2.3 Interfaces

The User-to-Network-Interfaces (UNI) at the SDP, as defined in Section C.2.3.2.3.1 are mandatory unless marked optional.

#### C.2.3.2.3.1 Asynchronous Transfer Mode Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth <sup>3</sup>	Signaling or Protocol Type <sup>4</sup>
1	ITU-TSS V.35	Up to 1.536 Mbps	AAL Type 5
2	EIA RS-449	Up to 1.536 Mbps	AAL Type 5
3	EIA RS-530	Up to 1.536 Mbps	AAL Type 5
4 (Optional)	DS1	Up to 1.536 Mbps	AAL Type 1
5 (Optional)	DS1	Up to 1.536 Mbps	AAL Type 5
6 (Optional)	DS3	Up to 43.008 Mbps	AAL Type 1
7	DS3	Up to 43.008 Mbps	AAL Type 5
8 (Optional)	DS1	Up to 1.536 Mbps	Native Mode
9	DS3	Up to 43.008 Mbps	Native Mode
10 (Optional)	ITU-TSS V.35	Up to 1.536 Mbps	AAL Type 3/4
11 (Optional)	EIA RS-449	Up to 1.536 Mbps	AAL Type 3/4
12 (Optional)	EIA RS-530	Up to 1.536 Mbps	AAL Type 3/4
13 (Optional)	DS1	Up to 1.536 Mbps	AAL Type 3/4
14 (Optional)	DS3	Up to 43.008 Mbps	AAL Type 3/4
15 (Optional)	SONET OC-3c	Up to 148.608 Mbps	AAL Type 3/4
16 (Optional)	SONET OC-12c	Up to 594.432 Mbps	AAL Type 3/4
17 (Optional)	SONET OC-48c	Up to 2.378 Gbps	AAL Type 5
18 (Optional)	SONET OC-48c	Up to 2.378 Gbps	AAL Type 3/4
19 (Optional)	E1 (Non Domestic)	Up to 1.92 Mbps	AAL Type 3/4

<sup>3</sup> Payload data rates include cell overhead.

<sup>4</sup> When AAL Type is specified, the Contractor shall provide the ATM adaptation function. For native mode, the user traffic type will be AAL Type 1 or AAL Type 5.



UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth <sup>3</sup>	Signaling or Protocol Type <sup>4</sup>
20 (Optional)	E3 (Non Domestic)	Up to 30.72 Mbps	AAL Type 3/4
21	COAX	Up to 43.008 Mbps	Native Mode
22 (Optional)	OC-3c	Up to 148.608 Mbps	Native Mode
23 (Optional)	High Speed Serial Interface (HSSI)	Up to 43.008 Mbps	HSSI
24 (Optional)	HSSI	From 2xDS1, in multiples of DS1, up to and including 8xDS1	HSSI

Note:

- Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

#### C.2.3.2.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of key performance indicators (KPIs) for ATMS in Section C.2.3.2.4.1 are mandatory unless indicated otherwise. All KPI measurements shall be SDP-to-SDP. The CBR performance metrics in Section C.2.3.2.4.1 are a mandatory requirement for native ATMS. The CBR performance metrics in Section C.2.3.2.4.1 are only mandatory for emulated ATMS if CBR is provided by the contractor.

##### C.2.3.2.4.1 Performance Metrics for Asynchronous Transfer Mode Service

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(PVC)	Routine	99.925%	≥ 99.925%	See Note 1
GOS(Max Cell Transfer Delay) (CONUS)	CBR	50 ms	≤ 50 ms	See Note 2
	VBRrt	55 ms	≤ 55 ms	
	VBRnrt	60 ms	≤ 60 ms	
GOS(Max Cell Loss Ratio)	CBR	1.00E-09	≤ 1.00E-09	See Note 3
	VBRnrt	1.00E-06	≤ 1.00E-06	
	VBRrt	1.00E-07	≤ 1.00E-07	
GOS(Max Cell Delay Variation)	CBR	1 ms	≤ 1 ms	See Note 4
	VBRrt	1.5 ms	≤ 1.5 ms	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	

Notes:

- PVC availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the PVC is operationally available to the Agency.

Availability is computed by the standard formula:

$$Av(PVC) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100.$$

2. GOS maximum cell transfer delay) is the end-to-end one-way delay experienced across the Network network. It reflects the transit time across a contractor's ATM network for a specific CoS and is defined as the amount of latency for data to be carried through an ATM network.
3. Network devices, such as switches and routers, sometimes must retain data cells in buffered queues when a link gets congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost.
4. GOS cell delay variation is a measure of the variance of cell transfer delay. High variation implies larger buffering for delay-sensitive traffic such as voice and video.
5. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

## **C.2.4 Internet Services**

### **C.2.4.1 Internet Protocol Service (IPS)**

The Government uses IPS to support a wide range of connectivity requirements that enable Government users to access the Internet, Government-wide intranets, and extranets. IPS will use the TCP/IP protocol suite to interconnect customer premise equipment (CPE) with other Government networks and the public Internet Service Provider (ISP) networks.

Verizon's Independent and Embedded Analog and ISDN Dial-up Services referenced under the Technical capabilities, Features, and Interfaces sections of C.2.4.1 were previously offered under Networkx, but are now discontinued effective 07/31/2013, in accordance with Networkx Contract Section C.2.1.1.

#### **C.2.4.1.1 Service Description**

##### **C.2.4.1.1.1 Functional Description**

IPS provides transport of Internet Protocol (IP) packets.

##### **C.2.4.1.1.2 Standards**

IPS shall comply with the following standards, as applicable, and when commercially available. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards.

1. Internet Engineering Task Force (IETF) RFCs
2. ANSI T1
3. ITU TSS Recommendations

4. ATM Forum
5. Frame Relay Forum implementations agreements
6. North American ISDN Users Forum (NIUF)
7. IEEE
  - a. 802.1Q
  - b. 802.1P
  - c. 802.3AD
8. Metro Ethernet Forum (MEF).
9. IETF RFCs for IPv6 when offered commercially by the contractor
10. All new versions, amendments, and modifications to the above documents and standards as they become commercially available.

#### **C.2.4.1.1.3 Connectivity**

IPS shall connect:

1. Government locations, including mobile and remote users, (i.e., SDP devices such as customer routers, switches, and firewalls) to the Internet.
2. A wide range of equipment (such as notebook PCs, PDAs, etc.) via appropriate combinations of Network services to the Internet.
3. Government locations to other networks, including other Network contractor's networks.

#### **C.2.4.1.1.4 Technical Capabilities**

The following IPS capabilities are mandatory unless indicated otherwise:

1. The contractor shall provide IPS ports at the peak data rates specified by the customer.
2. If access is required, the contractor shall support appropriate access services (such as dial-up VS analog data service, dial-up ISDN, DSL, cable high speed access, FRS, PLS, satellite, or ATMS) to connect customers' SDPs to the contractor's IPS service office(s). Figure C.2.4.1.1.4-1 Figure C.2.4.1.1.4-1 illustrates some examples of access alternatives.
3. The contractor's network shall have:
  - a. Established public peering arrangements from the contractor's network to the Internet.

- b. Private peering arrangements established from the contractor's network with redundant links to connect to its private peering partners.
  - c. Support for the Government assigned and InterNIC registered IP addresses and domain names.
  - d. Primary and Secondary Domain Name Service (DNS) to provide an authoritative name server for the customer.
4. The contractor shall provide support for the border gateway protocol (BGP) for Network customers with registered Autonomous System (AS) numbers.

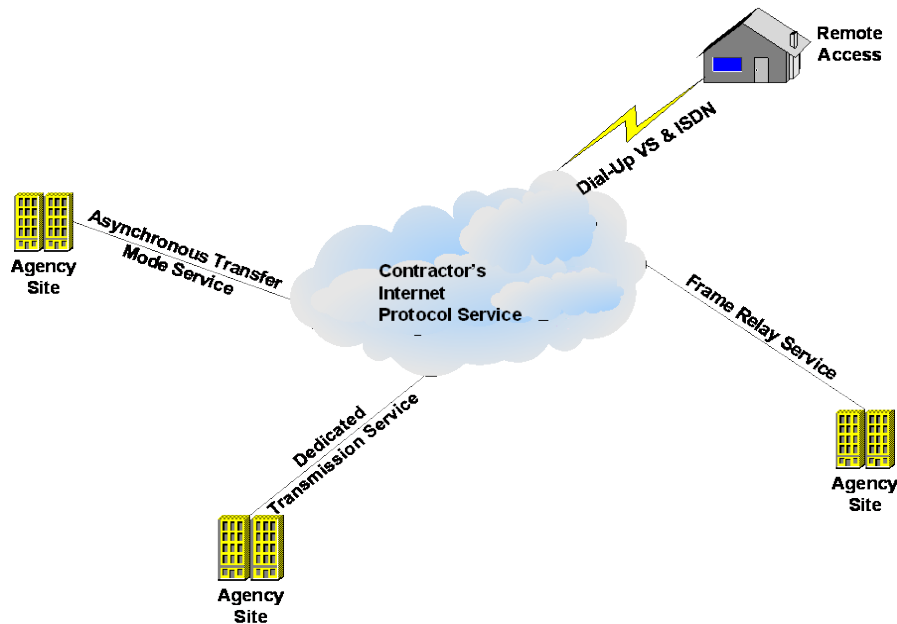


Figure C.2.4.1.1.4-1 Examples of IPS Access Alternatives

#### C.2.4.1.2 Features

The IPS features delineated in Section C.2.4.1.2.1 are mandatory unless indicated otherwise.

##### C.2.4.1.2.1 IPS Feature Set

ID Number	Name of Feature	Description
1	Dialup backup of dedicated ports	The contractor shall provide separate transmission using, as a minimum, the following accesses: <ol style="list-style-type: none"> <li>1. VS at a rate of 56 Kbps</li> <li>2. ISDN BRI at a peak data rate of 64 Kbps (Optional)</li> <li>3. ISDN BRI at a peak data rate of 128 Kbps (Optional)</li> </ol>
2 [Optional]	Web Based Directory Services	The contractor shall provide a web based directory service with the following capabilities: <ol style="list-style-type: none"> <li>1. Web interface</li> <li>2. No area code necessary</li> <li>3. Reverse number searches</li> <li>4. Reverse street searches</li> <li>5. Freedom to roam</li> <li>6. Reporting available</li> </ol>
		Feature replaces standard, telephone-connected directory assistance by providing Agencies with a convenient, self-service way to find national listings. The directory service will provide the following capabilities.

### C.2.4.1.3 Interfaces

#### C.2.4.1.3.1 Network Interfaces

The user-to-network-interfaces (UNI) at the SDP, as defined in Section C.2.4.1.3.2 below, for the provisioning of IPS are mandatory, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage.

#### C.2.4.1.3.2 User-to-Network Interfaces for IPS

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Asynchronous Transfer Mode Service	<ol style="list-style-type: none"> <li>1. T1</li> <li>2. T3</li> <li>3. OC-3c (Optional)</li> <li>4. OC-12c (Optional)</li> </ol>	IPv4/v6 over ATMS
2	Cable High Speed Access	320 Kbps up to 10 Mbps	Point-to-Point Protocol, IPv4/v6
3	Circuit Switched Data Service	<ol style="list-style-type: none"> <li>1. ISDN at 64 Kbps</li> <li>2. ISDN at 128 Kbps</li> <li>3. ISDN dial backup at 64 Kbps</li> <li>4. ISDN dial backup at</li> </ol>	Point-to-Point Protocol, IPv4/v6

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
		128 Kbps	
4	Ethernet Interface	<ol style="list-style-type: none"> <li>1. 1 Mbps up to 1 GbE (Gigabit Ethernet)</li> <li>2. 10 GbE (Optional)</li> </ol>	IPv4/v6 over Ethernet
5	Frame Relay Service	<ol style="list-style-type: none"> <li>1. 56 Kbps with 32 Kbps CIR</li> <li>2. Fractional T1               <ol style="list-style-type: none"> <li>(a) 128 Kbps with 64 Kbps CIR</li> <li>(b) 256 Kbps with 128 Kbps CIR</li> <li>(c) 384 Kbps with 128 Kbps CIR</li> <li>(d) 512 Kbps with 256 Kbps CIR</li> <li>(e) 768 Kbps with 384 Kbps CIR</li> </ol> </li> </ol>	IPv4/v6 over FRS
		<ol style="list-style-type: none"> <li>3. T1               <ol style="list-style-type: none"> <li>(a) 1.536 Mbps with 768 Kbps CIR</li> <li>(b) 1.536 Mbps with 1024 Kbps CIR</li> </ol> </li> <li>4. Fractional T3               <ol style="list-style-type: none"> <li>(a) 3 Mbps</li> <li>(b) 6 Mbps</li> <li>(c) 12 Mbps</li> <li>(d) 24 Mbps</li> <li>(e) 45 Mbps</li> </ol> </li> <li>5. T3</li> </ol>	

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
6	IP over SONET Service	<ol style="list-style-type: none"> <li>1. OC-3c (Optional)</li> <li>2. OC-12c (Optional)</li> <li>3. OC-48c (Optional)</li> <li>4. OC-192c (Optional)</li> </ol>	IP/PPP over SONET
7	Private Line Service	<ol style="list-style-type: none"> <li>1. DS0</li> <li>2. Fractional T1</li> <li>3. T1</li> <li>4. Fractional T3</li> <li>5. T3</li> <li>6. OC-3c (Optional)</li> <li>7. OC-12c (Optional)</li> <li>8. OC-48c (Optional)</li> <li>9. OC-192c (Optional)</li> </ol>	IPv4/v6 over PLS
8	Voice Service	Analog dialup at 56 Kbps	Point-to-Point Protocol, IPv4/v6
9	DSL Service	xDSL access at 1.5 to 6 Mbps downlink, and 384 Kbps to 1.5 Mbps uplink	Point-to-Point Protocol, IPv4/v6
10 (Optional)	Multimode/Wireless LAN Service	See Section C.2.14.3.3.1 MWLANS User-to-Network Interfaces	
11 (Optional)	Wireless Access	See Section C.2.16.2.3.3.1 Wireless Access Arrangement Interfaces	
12 (Optional)	Satellite Access	See Section C.2.16.2.4.3.1 Satellite Access Arrangement Interfaces	

Notes:

1. IPv6 shall be supported when offered commercially by the contractor.
2. Reserved
3. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

**C.2.4.1.4 Performance**

The performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for IPS in Section C.2.4.1.4.1 below are mandatory unless marked optional.

**C.2.4.1.4.1 Performance Metrics for IPS**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(Port)	Routine	99.95%	≥ 99.95%	See Note 1
	Critical (Optional)	99.995%	≥ 99.995%	
Latency (CONUS)	Routine	60 ms	≤ 60 ms	See Note 2
	Critical (Optional)	50 ms	≤ 50 ms	
GOS(Data Delivery Rate)	Routine	99.95%	≥ 99.95%	See Note 3
	Critical (Optional)	99.995%	≥ 99.995%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(Port) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

. For *critical user type*, the contractor would provide essentially 100% uptime for customer's Internet connection with high availability equipment, redundancy, automatic restoration, and reconfiguration.

2. Latency is the backbone delay experienced across the Networx network. It is the average time for IP packets to travel over the Networx core network. The Backbone Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. The Internet Control Message Protocol (ICMP) test can be used to calculate packet delivery and latency. The ICMP test consists of sending, every five minutes, a series of five test packets between Networx core service aggregation points (i.e., POPs). The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. Relevant standards: RFC 1242 and RFC 2285.
3. Network devices, such as switches and routers, sometimes have to hold data packets in buffered queues when a link is congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost. The loss can be measured with the ICMP test. Relevant standards: RFC 1242 and RFC 2285.
4. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.4.1.5 Managed Trusted Internet Protocol Service (MTIPS)**

The Managed Trusted Internet Protocol Service (MTIPS) allows Agencies to physically and logically connect to the public Internet or other external connections, as required by the Agency, in full compliance with the Office of Management and Budget's (OMB) Trusted Internet Connections (TIC) initiative (M-08-05), announced in November 2007.



MTIPS facilitates the reduction of the number of Internet connections in Government networks and provides standard security services to all Government users.

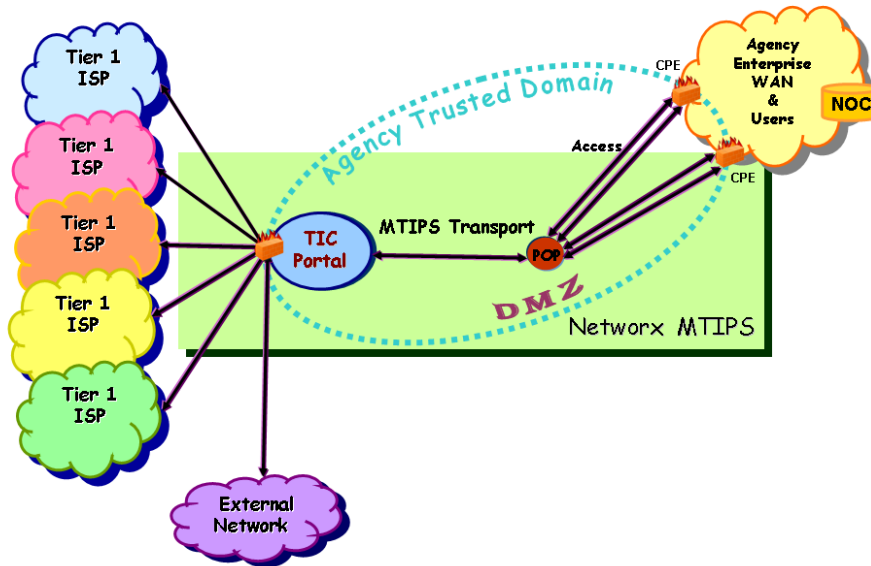
MTIPS solutions offered by Networkx contractors have been and shall be subject to periodic DHS Cybersecurity Compliance Validation (CCV) formerly known as TIC Compliance Validation (TCV). The Department of Homeland Security (DHS) is responsible for the "Compliance and Assurance Program (CAP)". The CAP employs a collaborative approach and measures, monitors and validates the implementation of cross-government initiatives and assesses cyber risks. Under CAP, MTIPS subscriber Agencies shall complete an annual Cybersecurity Compliance Validation (CCV) self-assessment and DHS will conduct an on-site CCV every three years. The MTIPS contractors shall participate in an annual DHS led CCV assessment.

The General Services Administration (GSA) is modifying MTIPS to allow subscribing Agencies to comply with TIC 2.0 requirements as in the "Trusted Internet Connections (TIC), Reference Architecture Document, Version 2.0" issued by the Department of Homeland Security (DHS), in March 24, 2011. The Department of Homeland Security has issued memorandum FISM 11-01 to announce the release of the above mentioned architectural document to Federal Agencies regarding compliance to TIC 2.0.

This modification adds the capabilities that have been identified as differences between TIC 1.0 and TIC 2.0. Where appropriate, the requirements have been tagged with the TIC 2.0 Formal ID as identified in Appendix B of the TIC 2.0 Reference Architecture Document. The TIC 2.0 Formal ID pattern has three fields, as follows [Security Family].[Security Function].[Capability Number].

The TIC 2.0 Architectural Document classifies capabilities in two categories, Critical and Recommended. All TIC 2.0 Critical capabilities are included in the MTIPS Basic Service requirements with the exception of a few that are included as Features in Section C.2.4.1.5.2 (e.g., Remote Access). As stated in the TIC 2.0 Architectural Document, Recommended Capabilities will become Critical in future MTIPS refresh cycles. Networkx contractors shall support the evolution of MTIPS as DHS initiates and requires future technical refresh cycles; e.g., TIC 3.0 and beyond.

MTIPS is comprised of the network infrastructure to transport Internet Protocol traffic between the Agency Enterprise WAN and the Trusted Internet Connection (TIC) Portal; together they create an Agency TIC Trusted Domain (DMZ) for Internet Protocol traffic. The architectural framework of MTIPS is illustrated in Figure C.2.4.1.5-1.



**Figure C.2.4.1.5-1 Networkx MTIPS Notional Architecture**

MTIPS enables the Government to react more effectively to cyber security attacks thus reducing malicious penetrations and theft of critical data. Exchange of information through the TIC Portal is closely monitored by an integral MTIPS Security Operations Center (SOC) to protect Agency IP traffic.

The MTIPS provided transport shall serve as a “collection” network for TIC Portal connectivity insulating an Agency’s internal network from the Internet and other external networks

The TIC Portal shall function as an OMB approved Multi-Service Trusted Internet Connection Access Provider (TICAP) capable of hosting multiple Agencies and able to manage and correlate multiple independent traffic streams for each subscribing Agency. The TIC Portal shall provide security services to multiple clients, but allow for specific controls based on Agency coordination, when necessary.

#### **C.2.4.1.5.1 Service Description**

Each contractor shall build *at a minimum* two (2) TIC Domestic Portals that are physically independent *while maintaining physical diversity from the TIC Portals to their servicing Internet Exchange Point*. The contractor shall provide management staff *at each* TIC Portal. Expansion beyond two TIC portals will require justification through a

written Business Case which will need to be approved by the Department of Homeland Security (DHS).

Network contractors providing MTIPS shall refer to the guidance from the Federal Network Security (FNS), DHS in the publication "Guidance for Requesting Approval of an Additional Trusted Internet Connection Location" issued in March 09, 2011. The guidance is applicable to expansions of the TIC Portals, in/outside the CONUS.

#### C.2.4.1.5.1.1 Functional Definition

The MTIPS generic functional model depicted in Figure C.2.4.1.5-2 subsumes the following set of functions and sub functions.

- (1) TIC Portal [TIC Access Points]
  - a. Access to *External Networks including the Internet.*
  - b. Hosted Einstein Enclave.
  - c. Security Operations Center (SOC).
  - d. ~~ICD 705 Sensitive Compartmented Information Facility (SCIF).~~
- (2) Transport Collection and Distribution (MTIPS Transport).

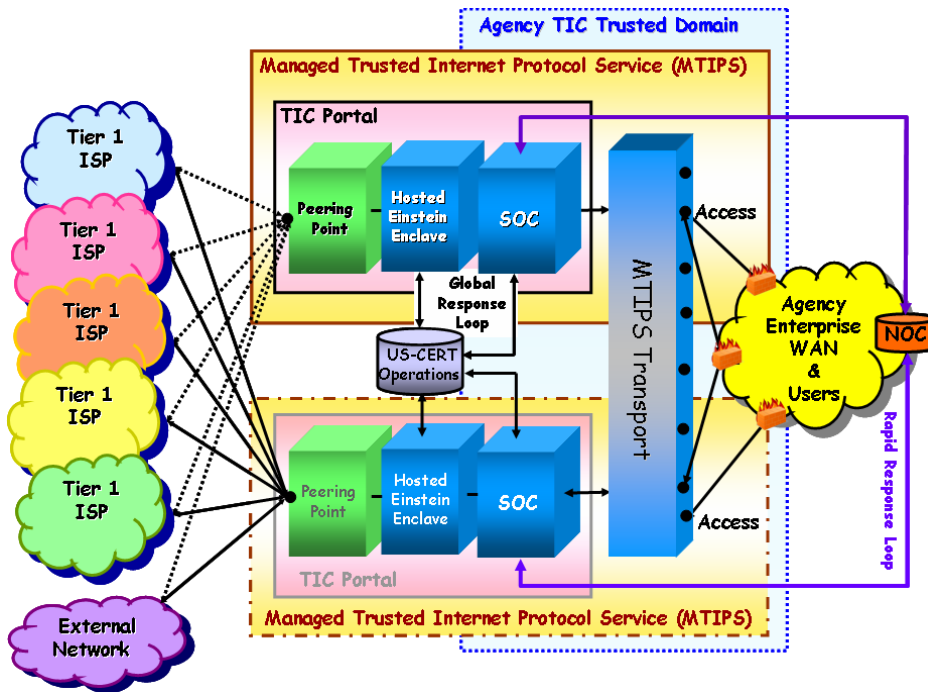


Figure C.2.4.1.5-2 MTIPS Context Architecture

The traffic collection and distribution supports the transport of Government-only IP traffic between Agency Enterprise WANs and TIC Portals utilizing the secure functionality of the SOC. The TIC Portal SOC monitoring and management systems shall be dedicated to the management and monitoring of the subscribing Agencies hosted by the contractor's portal and shall be isolated from commercial customers.

The contractor shall verify in writing with DHS before providing MTIPS service delivery to an Agency, in that the *Authorizing Official (AO)* has signed the required Memorandum of Agreement (MOA) with DHS which documents that the approved model banner language has been implemented throughout the Agency enterprise. This MOA is a legal requirement for the MTIPS delivery model, which includes the EINSTEIN capabilities. The contractor shall always ensure that only Federal U.S. Government traffic is sent to the EINSTEIN enclave. *The MOA form can be found at <http://www.gsa.gov/portal/content/104213>.*

The contractor shall meet DHS' TIC CCV before providing MTIPS service delivery to an Agency. This process can be initiated by the contractor after certification activities have occurred on the specific vendors implemented MTIPS architecture, policies, and procedures. Compliance can be completed before the Agency AO's *Security Assessment and Authorization (formerly known as C&A)* process. DHS will conduct periodic TIC compliance reviews (CCVs).

Section C.2.4.1.5.8 of this document has been revised to reflect the current practices applied by GSA during the Security Assessment and Authorization process (formerly known as C&A) on behalf of the Agencies and is not intended to change/add new requirements.

#### **C.2.4.1.5.1.2 Standards**

MTIPS shall comply with the following standards, as applicable, and when commercially available. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards.

1. Applicable Internet Engineering Task Force (IETF) RFCs.
2. T1.276-2003 American National Standard for Telecommunications — Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.
3. IP/MPLS Forum.
4. IEEE
  - a. 802.1Q
  - b. 802.1P
  - c. 802.3AD
5. Metro Ethernet Forum (MEF).

6. The PCI Data Security Standard (PCI DSS).
7. All new versions, amendments, and modifications to the above documents and standards when offered commercially.
8. MTIPS providers shall comply with current and future regulations, policies, requirements, standards, and guidelines for Federal U.S. Government technology and cyber security, including those listed below. Contractors shall comply with the new document versions, amendments, and modifications. Those most notable include minimum expectations for MTIPS specified security services identified in this SOW. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions.
9. E-Government Act of 2002, Title III (Federal Information Security Management (FISMA)).
10. NIST Federal Information Processing Standards Publication (FIPS) PUB 140-2— Security Requirements for Cryptographic Modules.
11. NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems.
12. United States Computer Emergency Readiness Team (US CERT) reporting requirements. (<http://www.us-cert.gov/federal/reportingRequirements.html>)
13. The Health Insurance Portability & Accountability Act of 1996 (HIPAA) Standards for the Security of Electronic Health Information.
14. The Sarbanes-Oxley Act of 2002.
15. The Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338, November 12, 1999 (GLBA).
16. The PCI Data Security Standard (PCI DSS).
17. *Intelligence Community Directive ICD 705, Sensitive Compartmented Facilities, rescinds Director of Central Intelligence Directive DCID 6/9* — Physical Security Standards for Sensitive Compartmented Information Facilities refer to requirements in Section C.2.4.1.5.1.4 (3)(b & c).
18. Standards included in Networkx Contract Section C.2.4.3.1.2, Collocated Hosting Service (CHS).
19. Standards included in Networkx Contract Section C.2.7.3.1.2, Network Based IP Virtual Private Network Service (NBIP-VPNS).
20. Standards included in Networkx Contract Section C.2.10.1.1.2, Managed Firewall Service (MFS).
21. Standards included in Networkx Contract Section C.2.10.2.1.2, Intrusion Detection and Prevention Service (IDPS).
22. Standards included in Networkx Contract Section C.2.10.4.1.2, Anti-Virus Management Service (AVMS).

23. Department of Homeland Security Management Directive Number 11042, DHS MD11042, 2005.
24. Electronic Code of Federal Regulation, Title 49, PART 1520--Protection Of Sensitive Security Information.
25. IETF RFC 1757 — Remote Network Monitoring Management Information Base.
26. NIST suite of documents for conducting C&A.
  - a. SP 800-18 Rev 1 — Guide for Developing Security Plans for Federal Information Systems.
  - b. SP 800-30 — Risk Management Guide for Information Technology Systems.
  - c. SP 800-34 Rev 1— — Contingency Planning Guide for Information Technology.
  - d. SP 800-37 Rev 1 — Guide for *Applying the Risk Management Framework to Federal Information Systems: A Life Cycle Approach*.
  - e. SP 800-53 Rev 3 — Recommended Security Controls for Federal Information Systems *and Organizations*.
  - f. Annex 3 to SP 800-53 Rev 3 — High Impact Baseline.
  - g. SP 800-53 A Rev 1 — Guide for Assessing the Security Controls in Federal Information Systems *and Organizations: Building Effective Security Assessment Plans*.
  - h. SP 800-59 — Guideline for Identifying an Information System as a National Security System.
  - i. SP 800-60 Rev 1 — Guide for Mapping Types of Information and Information Systems to Security Categories: *(Two (2) Volumes) – Volume 1 Guide and Volume 2 Appendices*.
  - j. SP 800-64 Rev 1 — Security Considerations in the Information System Development Life Cycle.
  - k. . SP 800-84 — Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.
  - l. SP 800-45 Rev 2 — Guidelines on Electronic Mail Security.
  - m. SP 800-46 Rev1— Guide to Enterprise Telework and Remote Access Security.
  - n. SP 800-61 Rev 1 — Computer Security Incident Handling Guide.
  - o. SP 800-81 Rev 1 — Secure Domain Name System (DNS) Deployment Guide.
  - p. SP 800-111— Guide to Storage Encryption Technologies for End User Devices.

27. Designation and Sharing of Controlled Unclassified Information (CUI), <http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html>
28. All commercially available standards for any applicable underlying access and transport services.
29. OMB Memo M-05-22 — Transition Planning for Internet Protocol Version 6 (IPv6).
30. OMB Memo M-06-16 — Protection of Sensitive Agency Information.
31. OMB Memo M-07-16 — Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
32. National Strategy for Trusted Identities in Cyberspace (NSTIC).
33. GSA Public Buildings Service Standards, PBS-100.
34. National Archives and Records Administration existing General Records. Schedules.
35. The Health Information Technology for Economic and Clinical Health (HITECH).
36. NIST SP 500-257— A Profile for IPv6 in the U.S. Government – Version 1.0.
37. NIST SP-500-273 — IPv6 Test Methods: General Description and Validation.

#### **C.2.4.1.5.1.3 Connectivity**

The MTIPS providers shall connect and interoperate with:

1. The Public Internet [*External Connections*] — MTIPS shall enable the subscribing Agency's users to connect to the Internet through the TIC Portal.
2. Global Response Loop [*Secure Communications / TM.COM.01*]— Provides US-CERT *with* a cross-Agency view and allows for coordination across TIC Portals through the following means:
  - a. US-CERT Network Operations Center to exchange threat alerts. Refer to <http://www.uscert.gov/federal/reportingRequirements.html>
  - b. TS/SCI communications (e.g. voice, email) between MTIPS provider personnel and US-CERT.
  - c. Provide communications between TIC Portals.
  - d. Provide communications between SOC(s) and TIC Portals through procedures, incident coordination and response (e.g., voice, secure e-mail, VPN).
3. Rapid Response Loop [*TM.COM.02 / TO.RES.01*] — Enables TIC Portal to Agency communications for the dissemination of threats/events to/from the Agency and the implementation of control mechanisms directed from the Agency.
4. Other Agency IP Networks (*External or Internal Connections*). See Requirements C.2.4.1.5.2.1 (7, 9 and 10) for *External Connections, Remote Access and Extranet Connections*.

#### **C.2.4.1.5.1.4 MTIPS Technical Capabilities**

#### C.2.4.1.5.1.4.1 TIC Portal Capabilities

The following TIC Portal capabilities are mandatory, unless marked optional:

1. **TIC Portal Access to *External Networks including the Internet*** —To ensure that Agencies are able to exchange traffic with the Internet and external networks at all times the TIC Portal shall comply with the following requirements when establishing interconnecting relationships:
  - a. The TIC Portals shall connect to the Internet via Tier 1 Internet Service Providers (ISPs).
  - b. The contractor shall budget enough interconnection bandwidth to accommodate increasing Agency's demands.
  - c. Alternate Routing — The contractor's TIC Portal shall provide multiple, physically diverse connectivity to interconnection points. *[TM.TC.01]*.
    - i. The TIC Portal shall enable alternate routing functions to keep the portals operating at all times.
    - ii. The TIC Portal shall enable Internet connectivity to a subscribing Agency via at least two Tier 1 ISPs, over physically diverse, high speed links *following the National Communications System (NCS) recommendations for Route Diversity.*
    - iii. *In the event that a TIC Portal, acting as primary, is unable to provide the security services specified in this document; the contractor shall ensure that the security services are provided by an alternate TIC Portal (secondary).*
    - iv. The contractor shall ensure that a technical architecture is implemented which supports EINSTEIN monitoring of all traffic at *alternate* TIC Portals in the event of any failure of *any* TIC Portal location. *The contractor shall consider single and multiple failure scenarios in the development of the technical architecture to demonstrate that KPIs and SLAs required in this document are met.*
  - d. The contractor shall establish and provide interconnection points in CONUS and shall support OCONUS and Non-Domestic traffic.
  - e. Private interconnection agreements shall be established to connect the TIC Portal to the Internet by one or both of the following mean:
    - i. Direct Circuit Interconnection, where the two parties share point-to-point circuits (i.e., neutral locations).
    - ii. Exchanged-Based Interconnection Model, that takes place in a neutral exchange site. At the TIC Portal all government traffic shall be separated from commercial traffic.
  - f. Inter-carrier Routing Requirements — The ISPs and external networks converging to a portal shall run BGP (eBGP, BGP4, etc.) or one of the options for inter-AS connectivity as specified by the IETF.



- i. The MTIPS contractor shall validate routing protocol information using authenticated protocols.
  - ii. The MTIPS shall configure Border Gateway Protocol (BGP) sessions in accordance with, but not limited to NIST SP 800-54.
  - iii. BGP sessions shall be protected with the MD5 signature option.
- g. **Support to Internet Protocol version 6 (IPv6)** — The contractor shall ensure that the MTIPS portals' public facing interfaces support both IPv4 and IPv6 dual-stack protocols in accordance with OMB Memorandum M-05-22, and the "IPv6 Transition Guidance" issued by the Federal CIO Council, Architecture and Infrastructure Committee. The contractor shall also transport both IPv4 and IPv6 (i.e. dual-stack) between external connections, including the Internet, and Agency's internal networks.

**2. Hosted National Cyber Protection System Sensor (NCPS) aka EINSTEIN 2 Enclave** — The EINSTEIN enclave, includes the EINSTEIN devices providing customized Intrusion Detection System (IDS) and network flow capabilities. The enclave in its entirety will be furnished by US-CERT. Maintenance and operations of the EINSTEIN enclave will be provided by US-CERT. At each TIC Portal the contractor shall provide a copy of all traffic transiting the portal (e.g. mirroring of traffic) to a 10Gbps Ethernet interface of a DHS owned and operated tap which feeds the two separate network devices providing the capabilities identified above.

- a. The EINSTEIN enclave shall be hosted in the contractors secured facility.
- b. **EINSTEIN Enclave to US-CERT Communications** — Each of the two EINSTEIN 10Gbps enclave network device components are equipped with one 1Gbps Ethernet management port to connect to the US-CERT securely utilizing a VPN directly to/from each device over the Internet.

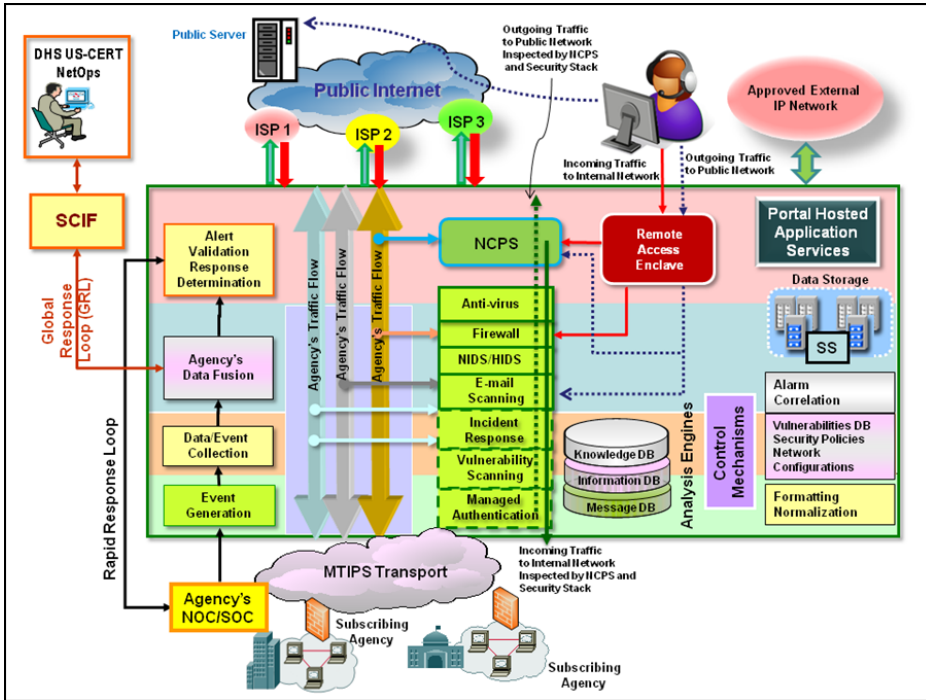
The contractor shall:

- i. Provide Internet connectivity for management ports of EINSTEIN enclave devices.
- ii. Provide 1000BaseT Internet connection cabling directly to management ports.
- iii. Provide IPv4 addresses for the network management port of the customized IDS and network flow devices (2 total ports per 10Gbps capability). Management ports allow for US-CERT operations, maintenance, exchanging of alarm, alert and control messages to/from the EINSTEIN enclave devices.
- iv. Provision Internet bandwidth for the Agency customer link being monitored.

1. For an OC-12 link, 20 Mbps.
  2. For an OC-48 link, 75 Mbps.
  3. For an OC-192 link, 300 Mbps.
  4. For a 1 GigE link, 30 Mbps.
  5. For a 10 GigE link, 300 Mbps
- v. Provide session load balancing for traffic above 10Gbps to ensure that the EINSTEIN enclave has the necessary visibility into traffic flowing through the TIC Portal. The EINSTEIN portal will be built out appropriately based on 10Gbps Ethernet traffic needs. It is critical that the contractor communicate with DHS on the physical link speeds being installed for Agency clients, as well as ongoing discussions with potential clients to ensure that any necessary equipment is procured and installed to provide coverage. Asynchronous routing where Internet bound traffic could flow out one TIC Portal and back in another TIC Portal due to Border Gateway Protocol (BGP) route preferences on the Internet is an understood monitoring risk.
- c. EINSTEIN enclave operational requirements — The contractor shall support the following:
- i. Physical Space — The contractor shall support the following physical space requirements for the EINSTEIN enclave:
    1. Provide 11U of rack space for each allocation of 10 Gbps Ethernet bandwidth monitored.
    2. Provide physical access to EINSTEIN enclave devices when necessary.
  - ii. EINSTEIN Devices — The contractor shall support the EINSTEIN devices as follows:
    1. The hosting facility shall maintain temperature and humidity control at all times.
    2. The hosting facility shall be equipped with generator backup power at all times to support business continuity functions. This shall include the ability to shut down the main power source in the event of an emergency.
    3. The EINSTEIN appliances' tap operational requirements shall be met as follows. The contractor shall provide:
      - a. Power of 100-240 Volts AC, at 47 – 63 Hz and a maximum power of 15 W.
      - b. Operating temperature of 0 – 45 degrees C.
      - c. Storage temperature of -20 – 100 degrees C.
      - d. Non-condensing Humidity of 5% – 95%.

- iii. EINSTEIN devices providing customized IDS and network flow capabilities — In support of the each device the contractor shall:
1. Provide electrical power for the NetFlow Collector as follows:
    - a. AC input voltage of 100 – 240 V AC, single phase 100 to 240 V AC.
    - b. AC input at line frequency of 50 – 60 Hz.
    - c. .AC input nominal power 600 W
  2. Operate the network flow device at the following environmental conditions.
    - a. Operating temperature, 0° C – 40° C
    - b. Non-condensing Non-Condensing Relative Humidity of 10% – 90%.
  3. Provide electrical power for the customized IDS as follows:
    - a. Electrical current of 5 Amps @110V / 2.5 Amps @ 220V.
    - b. Voltage 100 – 127V / 200 – 240V.
    - c. Maximum power of 550 Watts.
  4. Operate the customized IDS at the following environmental conditions:
    - a. Air Conditioner at a rating of 2048 BTU per hour
    - b. Operating Temperature, 0°C – 40°C.
- iv. Data Storage — The contractor shall support the EINSTEIN Enclave storage as follows:
1. Provide electrical power:
    - a. Maximum continuous power of 478 Watts and peak power of 550 Watts.
    - b. Rated input Voltage Range of 100 – 240 Volts and actual input voltage range of 90 – 264 Volts.
    - c. Operating electrical current of 7.2 Amps at 100V or 3.6 Amps at 200V.
  2. Operate the enclave storage at the following environmental conditions:
    - a. Operating Temperature of 10° – 35°C (50° – 95°F) and storage temperature of -40° – 65°C (-40° – 149°F).
    - b. Non-condensing relative humidity of 20% – 80% and non-condensing storage humidity of: 5% – 95%.\

- v. Rebooting — The contractor shall provide basic support to US-CERT in rebooting (powering on/off devices) when necessary
  - vi. Troubleshooting Connectivity — The contractor shall provide support in the physical and/or logical troubleshooting with US-CERT being able to access the management port of EINSTEIN network equipment.
  - vii. Troubleshooting TIC Portal Traffic Coverage — The contractor shall provide support in the physical and/or logical troubleshooting with US-CERT being able to see all traffic flowing through the MTIPS TIC Portal.
- 3. TIC Portal Security Operations Center (SOC)** — The TIC Portal SOC is the set of tools, appliances and processes that collect, reduce, normalize, correlate, fuse, and manage event data from a variety of devices that support the MTIPS operations. For the SOC, these devices include firewalls, Network Intrusion Detection Devices (NIDS), Host-based IDS (HIDS), and other platforms that may collect TIC Portal-relevant event data. The SOC tools also provide reports customized to Agency's requirements [Refer to Section C.2.4.1.5.2.1— MTIPS Features] but as a minimum shall support TIC Portal authorities / analysts by identifying security events of interest that may be negatively affecting the TIC Portal environment. The subscribing Agency's security authorities / analysts then will be empowered to react and trigger appropriate control mechanisms, thus creating a Rapid Response Loop. This is illustrated in Figure C.2.4.1.5-3 below.



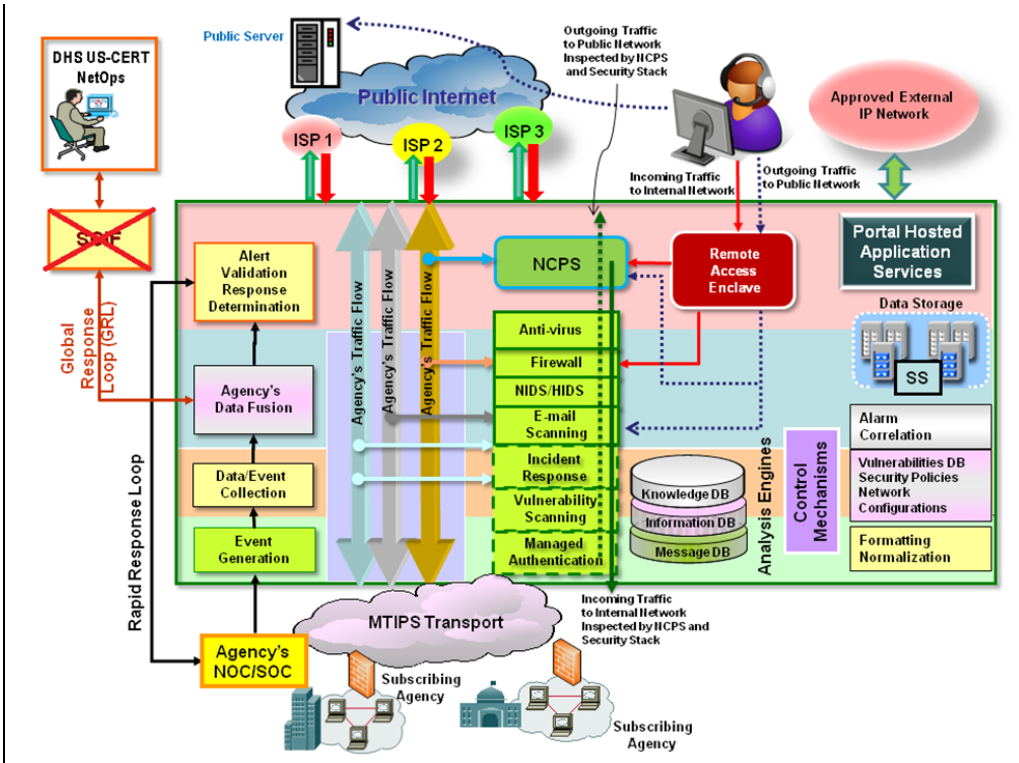


Figure C.2.4.1.5-3 The TIC Portal Security Operation Center Architecture

The primary goal of the SOC is to provide analysis/correlation and management structure to mitigate the threat presented by external attacks. The contractor shall provide the following security functions:

- a. Support to all SOC functions. The contractor shall be responsible for monitoring, incident response, vulnerability management, vulnerability assessment, incident reporting, engineering support, and TIC Portal SOC standard security policy enforcement at the hosting facility. The contractor shall describe clearly the building blocks of the proposed security solution and their internal components. The following items shall be included:
  - i. Architectural diagram and its description.
  - ii. TIC Portal physical locations appropriately labeled..
  - iii. Consistency on the labeling of the architectural building blocks and the proposal's text.

- iv. Clear relationship between the solution's building blocks and their internal components.
  - v. Physical locations of the solution's building blocks and their components.
  - vi. A thorough description of the interconnection mechanisms used if and when building blocks/components are not physically collocated.
  - vii. Functional relationship between the SOC and the NOC.
  - viii. Redundancy of the security stack at each TIC Portal.
  - ix. Storage network or systems, and their physical location.
- b. Provide trained, qualified, and cleared staff (U.S. citizens) to support security functions 24x7. The SOC shall be staffed with at least two (2) people with appropriate credentials to manage technical aspects of the network attacks.
  - c. All systems accessible from the Internet shall reside in the Agency's Trusted Domain.
  - d. All inbound and outbound connections shall be set to a default "deny" policy.
  - e. The basic SOC shall protect Controlled Unclassified Information (CUI) data.
  - f. The basic SOC shall provide event validation to determine if alerts/threats/events generated by different sources [sensors, SOC infrastructure] after being correlated in the appropriate context are relevant to the Agency's business to be escalated and examined by the security authorities.
  - g. The SOC shall support escalation functions.
  - h. The SOC shall be the central coordination point of contact (POC) for computer security incidents across the SOC for the subscribing Agency.
  - i. The SOC architecture shall limit outbound connections so that only needed services are allowed. The contractor shall keep an inventory of such services that shall be verified daily.
  - j. The SOC shall monitor for data exfiltration / infiltration or remote control attempts.
  - k. The SOC shall provide centralized, secured, and unified management of security events in order to protect the integrity of the US Government data and infrastructure. The contractor may use Security Information and Event Management (SIEM) tools.
  - l. The SOC shall be built using multi-sensor data fusion models or competing data correlation technologies.
  - m. The SOC shall monitor Agency's traffic streams and shall fuse this information and analyze it to deduce changing trends in intrusion behavior.

- n. All the devices involved in the SOC implementation shall be synchronized via Network Time Protocol (NTP) Stratum 1 system as a stable Primary Reference Time Server (PRTS) synchronized within 0.25 seconds relative to Coordinated Universal Time (UTC) and clearly designating time zone in time stamps to ensure consistency. (See i, ii and iii). The primary synchronization method may be an out-of-band National Institute of Standards and Technology/United States Naval Observatory (NIST/USNO) reference time source (Stratum 0) such as the Global Positioning System (GPS) or WWV radio clock.
  - i. All MTIPS event recording clocks shall be synchronized to within 3 seconds relative to Coordinated Universal Time (UTC).
  - ii. All MTIPS log timestamps shall include the date and time, with at least to-the-second granularity.
  - iii. Log timestamps that do not use Coordinated Universal Time (UTC) shall include a clearly marked time zone designation. The intent is to facilitate incident analysis between TICAPs and TIC networks and devices.
- o. At the request of the Agency, the MTIPS contractor shall be able to selectively filter and store a subset of inbound and outbound traffic. The contractor shall support storage capacity to retain at least 24 hours of the data generated by the Agency's selected traffic flows. In addition, the contractor shall provide off-site storage capabilities for all backup data collected by the TIC Portal SOC.
- p. The SOC architecture previously depicted in Figure C.2.4.1.5-3, shall comprise the following building blocks at a minimum:
  - i. Event Generators — "Sensors" and "pollers" are the mechanisms that generate (create) events on deployed components of the SOC. They are heterogeneous by nature as they include all the types listed below. The event generators shall perform the following functions:
    1. Log events on a variety of platforms and devices (e.g., NIDS, firewalls)
    2. E-mail Scanning and Filtering Functions — All scanning and email protection shall be performed as specified by NIST 800-45 Revision 2, "Guidelines for Electronic Mail Security". All the required protections are in addition to malware scanning and content filtering performed by the Agency's mail servers and end-user's host systems. The contractor shall tailor their malware and content filtering services for individual Agency mail domains. The contractor shall support:
      - a. Monitoring of unencrypted inbound/outbound SMTP messages and filtering based on, but not limited to:



- unauthorized/known bad mail source or destination, suspicious text patterns, unauthorized file attachments and malware.
- b. Scanning of SMTP messages for spam filtering.
  - c. *Communications between the contractor and the subscribing Agency to coordinate the actions to be taken when email messages are categorized as suspicious. The Agency's mail domain can take at least the following actions: block the message, deliver the message, sanitize malicious content and tag undesirable content. Note: this is intended to be an additional option which agency mail operators can specify with capability [TS.CF.04]. It does not require quarantining potentially suspicious mail.*
  - d. Anti-spam methods including fingerprinting, blacklists, open relay blocking, honey pots, Bayesian probability, heuristic and rule-based filtering, as appropriate.
  - e. The capability to distinguish between legitimate email and spam, reducing false negatives and positives.
  - f. The SOC's ability to customize spam lists, and specify domains, IP, and email addresses which are to be allowed or blocked.
  - g. Ensure that the anti-spam filters generate events to be forwarded to the Event collectors.
3. Firewall Functions — The SOC shall be equipped with firewalls. The contractor shall support the following:
- a. Support Network-based firewalls.
  - b. Ensure that firewall generated alerts/events are forwarded to the Event Collectors.
  - c. Ensure that the default setting for all firewall ports with inbound or outbound access to the Internet is "deny" or its functional equivalent.
  - d. Ensure that inbound traffic on explicitly approved ports will be allowed to establish connections to Government workstations and servers.
  - e. Ensure that HTTPS traffic is proxied and filtered via the firewall based on URL and/or direction from US-CERT (Global Response Loop), regardless of the direction of traffic (inbound/outbound), unless an exception is granted.

- f. Capture and keep firewall generated event logs that include relevant system information. Applicable capture metrics and retention periods are included in Section C.2.4.1.5.1.4.1(3)(p)(iv)(3).
- g. Ensure that the firewalls have the capability to filter based on all of the following:
  - i. Transmission Control Protocol (TCP).
  - ii. User Datagram Protocol (UDP).
  - iii. IP addresses
  - iv. Domain names
  - v. Incoming network interfaces
- h. Filter inbound traffic to the SOC to reject the following:
  - i. Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself.
  - ii. Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
  - iii. Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks. *Inbound filtering rules shall block traffic from packet source addresses assigned to internal networks and special use addresses (IPv4-RFC5735, IPv6-RFC5156).*
  - iv. Inbound traffic from a non-authenticated source system containing Simple Network Management Protocol (SNMP) traffic.
  - v. Inbound traffic containing IP source routing information.
  - vi. Inbound or outbound network traffic containing a source or destination address of the local host.
  - vii. Inbound network traffic containing a source address of 0.0.0.0 or outbound containing a destination address of 0.0.0.0.
  - viii. Inbound or outbound traffic containing directed broadcast addresses.
- i. Employ various protection techniques including but not limited to stateful packet inspection, by which the

firewall goes beyond just examining a packet's source and destination, but also verifies its legitimacy. The firewall shall confirm requests made, and match open connections to valid packets prior to allowing them through the network.

- j. Support additional functions included in Section C.2.10.1 (MFS) as applicable to the MTIPS solution.
4. Network Intrusion Detection and Protection Functions — The SOC shall be equipped with Intrusion Detection and Protection components. The contractor shall support the following functions:
- a. Equipment vendor, *US-CERT* and Agency supplied custom, *critical signatures including signatures for the application layer. [TS.INS.02]*.
  - b. Detection of precursor activities such as unauthorized network probes, sweeps, and scans that may indicate a potential attack.
  - c. Perform anomaly detection in order to identify a typical traffic trends and unusual behaviors that may indicate a potential attack.
  - d. Analyze system activity for known attacks such as Denial of Service (DoS) and/or Reconnaissance Efforts. *The contractor shall mitigate the impact on non-targeted MTIPS subscribers from a DOS attack on a particular subscriber Agency. This may included diverting information flooding types of denial of service attacks targeting a particular subscriber Agency in order to maintain service to other agencies. [TO.RES.03]*.
  - e. Applicable functionality as specified by Networkx Contract Section C.2.10.2 applicable to the MTIPS solution.
  - f. Ensure that IDPS generated events be forwarded to Event Collectors.
5. Anti-Virus Protection Functions — Support shall be accomplished by meeting applicable requirements to the MTIPS solution included in the Anti-Virus Management Service (AVMS) specified by Networkx Contract Section C.2.10.4. The AVMS generates events that will be forwarded to Event Collectors.
6. The event generators shall collect all user interaction with the SOC components.

- ii. Event Collectors — Event collectors gather information from sensors and pollers to provide the following functions.
  1. The event collectors shall collect and store events on a variety of platforms and devices (e.g., NIDS, firewalls).
  2. The event collectors shall provide integrity of data collection, storage, and management.
  3. Data Collection — Raw messages collection shall be performed to reflect the operating states of security appliances and network elements of the TIC Portal.
    - a. The collection of raw data shall include the following:
      - i. Protocols (e.g., Syslog, SNMP, SMTP, HTTP/XML, FTP, etc.).
      - ii. Intrusion types (e.g., malicious code, SYN floods, Trojan horse, virus, worm, network worm, spyware, etc.).
      - iii. Identification of sources and targets.
  4. Provide data recovery and backup functions for both disaster recovery and contingency planning.
  5. Message Database — Raw data collected shall be presented and stored as formatted and normalized messages. This is because such data may be presented by the sensors in multiple, unpredictable formats, as they may be formatted using “de facto” or other available standards (i.e., HTTP logs in NCSA format, common schema, etc.).
    - a. The message database shall support standard database structures and standards (e.g., SQL, ODBC).
- iii. Analysis Engines shall determine what infrastructure comprises TIC Portal components (i.e. single server, multiple servers, etc.). The Analysis engines provide (a) Data Fusion functions and (b) Alert Validation and Response Determination Functions. The Analysis Engines shall comply with the following requirements:
  1. Information Database — The information database shall perform the following functions:
    - a. Provide a breadth of rule sets sufficient to cover the technologies and threats in the TIC Portal environment.
    - b. Provide the ability to analyze and group data to form intelligent alerts.
    - c. Draw data from various sources.

2. Knowledge Database — The knowledge database shall perform the following functions:
  - a. Identify attacks based on misuse of privileges.
  - b. Provide a capability to create custom correlation rules.
  - c. Perform analysis and response near real-time after event detection to prevent further attacks.
  - d. Provide categorization of security events detected in order to search for data that indicates anomalous events.
  - e. Perform forensic analysis on security incidents to learn valuable lessons about attacks and implement changes proactively based on knowledge learned.
3. Control Mechanisms — The following control mechanisms shall be supported as part of the Rapid Response Loop.
  - a. The contractor shall provide the capability and authority to the subscribing Agency to block IP addresses or net blocks that are suspicious or have been deemed threatening either by the Agency via the Rapid Response Loop or by US-CERT via the Global Response Loop. Agency's measures will be notified to the TIC SOC personnel via phone, fax, or email.
  - b. The contractor shall support, as a minimum, the control mechanisms outlined in Network Contract Section C.2.10.2.1.4 (18) through (20) (IDPS).
  - c. The contractor shall allow Agency customers to recover, retrieve or release e-mail blocked as SPAM from inbound/outbound SMTP messages.
- iv. Systems Logs — The contractor shall store, maintain and secure logs / files from TIC Portal components. The minimum required functions are:
  1. Capture and store logs / files from *services (e.g., DNS/DNSSEC, DHCP, etc.)* and installed TIC Portal equipment such as firewalls, routers, servers and other designated network devices required to establish an audit trail of activity sufficient to reconstruct security relevant events.
  2. The audit trail shall include the identity of each entity accessing the system including source and destination IP addresses. The following shall be recorded where they exist:

- a. Time/ time-zone and date access.
  - b. Time and date the entity terminated access.
  - c. Activities performed using an administrator's identification.
  - d. Activities that could modify bypass or negate the network's security safeguards.
3. Retain all such audit log data for a minimum of 7 days online and up to 5 years of historical log data.
- a. The contractor shall provide online access to at least 7 days of session traceability and audit ability by capturing and storing logs / files from installed TIC equipment.
  - b. The contractor shall maintain the logs needed to establish an audit trail of administrator, user and transaction activity and sufficient to reconstruct security-relevant events occurring on, performed by and passing through TIC systems and components. This capability is intended for immediate, online access in order to trace session connections and analyze security-relevant events.
  - c. Regarding the historical logs, the contractor shall document procedures for log retention and disposal, including, but not limited to, administrative logs, session connection logs and application transaction logs.
  - d. Record retention and disposal schedules shall be performed in accordance with the National Archives and Records Administration existing General Records Schedules, in particular Schedule 12, "Communications Records" and Schedule 20, "Electronic Records;" or NARA approved Agency-specific schedule.
4. Protect all stored audit trails from actions such as unauthorized access, modification, and destruction that would negate its forensic value.
5. Logs shall be reviewed daily for intrusions, incidents, or events.
6. Intrusions, incidents, and events shall be reported and root cause analysis completed and shared with the subscribing Agency and US-CERT.
- v. Reporting — The contractor shall:

1. Compile attack and threat events (*logs*) from various sources including the contractor's SOC, Agency's diversity connected/subscribed to MTIPS, US-CERT broadcasted attacks and threats, etc.
  2. Develop and distribute security advisories and provide notification to Agency's leadership to ensure timely and accurate notifications. Each subscribing Agency will identify its security leadership. Notifications to Agency's are via email, phone, fax, etc.
  3. Develop, update, and report monthly metrics depicting SOC health and status, automating where appropriate (i.e., reports available through a console).
  4. Provide monthly reports on meeting security operations KPIs included in Section C.2.4.1.5.4.1.
  5. *Identify, retrieve and report on specific subscribing Agency data, without divulging any other Agency's data.*
- q. Rapid Response Loop Component — The contractor shall provide subscribing Agencies with a web-based administrative tool that provides basic security alerts, incidents and reports as described in the following:
- i. Provide a near real-time monitoring, incident handling, and statistical analysis interface.
  - ii. Provide a mechanism for organizing and prioritizing incoming alert information.
  - iii. Provide visualization tools permitting the identification of trends in alarm data.
  - iv. Enable analysts to display, sort, filter, and query data contained in records of all types.
  - v. Permit customization to add views, change views, and create new views of data .
  - vi. Export record and analysis data in a variety of ways, such as screen, printer, e-mail, file, text, HTML, PDF, and third-party reporting tools.
- r. The TIC Portal components shall function on hardened and patched platforms in compliance with the applicable NIST standards.
- s. The SOC shall provide alert and health status of MTIPS components.
- t. The SOC shall be able to accommodate network and system event data without degradation of performance.
- u. The contractor shall build two instances of the TIC Portal SOCs that are manned with qualified personal 24x7x365 and are located in two different physically diverse locations *with at least 10 miles of separation*

[TM.PC.06]. The contractor may build the SOC using a distributed architecture where some components are not physically collocated, thus becoming virtual TIC Portal SOC's which may be managed remotely. However, the contractor shall ensure that all instantiations of such components and systems regardless of their physical location are part of the Agency's Trusted Domain. That is all of them are devoted to inspecting, filtering and correlating Government's traffic.

- ~~4. ICD 705 Sensitive Compartmented Information Facility (SCIF) — The contractor shall provide controlled space which may be collocated with the SOC but logically outside the security boundary. Refer to Section C.2.4.1.5.8. The SCIF shall comply with ICD 705, "Sensitive Compartmented Information Facilities." which rescinds DCID 6/9 [TM.COM.01].~~
- ~~a. The contractor shall provide redundant SCIFs, ICD 705 controlled office space of at least 6 ft x 6 ft. The contractor shall ensure to support at least up to 10 times space and power expansion.~~
  - ~~b. The contractor shall explain contingency measures and processes to ensure continuous Global Response Loop functionality.~~
  - ~~c. The SCIF shall house a Government furnished (US CERT) classified phone and classified email account at the Top Secret level.~~
  - ~~d. At a minimum, one (1) person cleared with Top Secret (TS/SCI) security clearance shall have access to each of the SCIFs 24x7x365 to handle secure communications (e.g., voice, e-mail) in the managed secure space with authority to report, acknowledge and initiate action based on TOP SECRET/SCI level information, including tear line information, with US-CERT.~~
  - ~~e. The two qualified people (or more than two depending on the number of portals offered by the contractor) with TOP SECRET/SCI clearance shall be available to respond within 2 hours of the notification, 24x7x365, with authority to report, acknowledge and initiate action based on TOP SECRET/SCI level information, including tear line information, with US-CERT. The two-hour timer starts when US-CERT issues the notification to all SCIFs involved in the incident. The contractor shall provide space to accommodate Secure Terminal Equipment (STE) and Secure FAX machine.~~
  - ~~f. The cleared personnel in (e) to handle classified information shall be qualified to function as Senior NOC/SOC management with authority to take actions on behalf of the Agency as determined by the Agency.~~
  - ~~g. The MTIPS SCIF shall be located at the MTIPS portal facilities or within 30 minutes of the TIC management location, during normal conditions, in order for authorized personnel to exchange classified information, evaluate the recommendations, initiate the response and report operational status with US-CERT within two hours of the notification.~~



**5.4. Content Filtering/Inspection of Encrypted Traffic Procedure** — The contractor shall document the procedure or plan that explains how it inspects and analyzes encrypted traffic. The document shall include a description of defensive measures taken to protect MTIPS subscribers from malicious content or unauthorized data exfiltration when traffic is encrypted. The subscriber Agencies requiring the contractor to inspect encrypted traffic, header and payload, can do so by using Feature 1.

**6.5. Asymmetric Routing** — The MTIPS portal stateful inspection devices shall correctly process traffic returning through asymmetric routes to a different MTIPS stateful inspection device; or shall document how return traffic is always forced to return to the originating MTIPS portal stateful inspection device.

**7.6. Federal Video Relay Service (FedVRS) Support** — The MTIPS portal shall support Federal Video Relay Service (FedVRS) for the Deaf ([www.gsa.gov/fedrelay](http://www.gsa.gov/fedrelay)) network connections, including but not limited to devices implementing stateful packet filters. Please refer to <http://www.fedvrs.us/supports/technical> for FedVRS technical requirements.

**8.7. E-Mail Forgery Protection** — The MTIPS contractor shall support the following:

- a. The MTIPS portal shall include the results of the domain-level sender forgery analysis when determining potentially suspicious or undesirable email for email received from other Agency mail domains known to have domain-level sender authentication (for example Domain Keys Identified Mail or Sender Policy Framework). This capability is intended to support domain-level sender authentication, but does not necessarily confirm a particular sender or message is trustworthy.
- b. Scoring criteria for this capability shall be aligned with the National Strategy for Trusted Identities in Cyberspace (NSTIC).
- c. The MTIPS contractor shall take Agency specific actions for email determined to be suspicious or undesirable.

**9.8. [Optional]** The contractor shall support signing procedures for outgoing email messages to ensure that they have been digitally signed at the Domain Level (for example Domain Keys Identified Mail) in order to allow receiving Agencies to verify the source and integrity of email. This capability is intended to support domain-level sender authentication, but does not necessarily confirm a particular sender or message is trustworthy. Signing procedures shall be in alignment with the National Strategy for Trusted Identities in Cyberspace.

**10.9. Domain Name System (DNS) and DNS Security Extensions (DNSSEC)** — The MTIPS portals shall be equipped with resolving/recursive (also known as caching) name servers to properly filter DNS queries, and to perform validation of DNS Security Extensions (DNSSEC) signed domains for MTIPS subscribers. The DNS/DNSSEC servers configurations shall be in accordance but not limited to the following recommendations from NIST SP 800-81 Revision 1:

- a. The MTIPS contractor shall deploy separate recursive name servers from authoritative name servers to prevent cache poisoning.
- b. The MTIPS portal shall filter DNS queries for known malicious domains.
- c. The MTIPS portal shall log at least the query, answer and client identifier.

**41.10. Uninterrupted Operations** — The MTIPS portals shall be equipped for uninterrupted operations for at least 24 hours in the event of a power outage, and shall conform to specific physical standards including, but not limited to the following:

- a. Electrical systems shall meet or exceed the building, operating and maintenance standards as specified by the GSA Public Buildings Service Standards, PBS-100.
- b. The MTIPS portals systems and components shall be connected to uninterruptable power in order to maintain mission and business-essential functions including, but not limited to, TIC systems, support systems and powered telecommunications facilities, including at the DEMARC or MPOE.
- c. Uninterruptable power systems, HVAC and lighting shall be connected to an on-site, automatic, standby/emergency generator capable of operating continuously (without refueling) for at least 24 hours.

**42.11. Internet Protocol Version 6 (IPv6)** — The contractor shall ensure that all TIC systems and components of the TIC portals support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22, and the “IPv6 Transition Guidance” issued by the Federal CIO Council, Architecture and Infrastructure Committee.”

- a. The MTIPS contractor shall ensure that TIC portals’ systems implement IPv6 capabilities, without compromising IPv4 capabilities or security. IPv6 security capabilities shall achieve at least functional parity with IPv4 security capabilities.

**43.12. [Optional] Data Loss/Leak Prevention** — The contractor shall support Data Loss (Leak) Prevention (DLP) program. The contractor shall document all aspects of the DLP supported by the MTIPS.

#### **C.2.4.1.5.1.4.2 MTIPS Transport Collection and Distribution Capabilities**

The following MTIPS capabilities are mandatory unless marked optional:

1. The contractor shall allow Agency’s Internet bound traffic to reach the Internet via one of the two TIC Portals.
2. The contractor shall support failover mechanisms that will reroute Agency’s traffic to the second Contractor provided TIC Portal. This will allow Agencies to have access to the Internet even in cases of transport failures (e.g. fiber cuts) or during cyber attacks.

3. The contractor shall support link (backbone) aggregation of the diverse access speeds between the subscribing Agency's SDP and the TIC Portal.
4. The contractor shall provide interworking services at the POP for Agency locations to transparently access MTIPS using the following services:
  - a. The contractor's ATM networks.
  - b. The contractor's FR networks.
  - c. The contractor's Ethernet networks (optional).
  - d. The contractor's NBIP-VPN networks.
5. An Agency Trusted Domain (DMZ) shall be created by the contractor to ensure that Agency's traffic is protected and physically isolated when transported to the portal and the public Internet. The DMZ includes the access portion of the service as well as the MTIPS transport. The contractor shall ensure that the traffic is not sniffable and ports cannot be spoofed.
6. The contractor shall ensure that Agency's traffic to the Internet from an Agency's site is not routed to another site before being routed to the TIC Portal.
7. The contractor shall provide, install/configure and maintain a firewall (inner firewall) at the Agency's SDP (i.e., edge of the Agency's WAN), which in conjunction with the firewall at the TIC Portal SOC (outer firewall) enable the fulfillment of requirement (5). The inner firewall should be provided separately via a SED and not be included in the MTIPS basic port price. The contractor shall describe in detail the chosen solution.
  - a. The contractor may choose to implement a Layer 2 or a Layer 3 solution which shall include the access link as part of the DMZ.
  - b. The contractor shall make sure that the inner firewall is visible to the contractor's NOC and the TIC Portal SOC as part of the MTIPS basic service.
8. The Agency may use Feature 8 in Section C.2.4.1.5.2.1 to encrypt links from the Agency's SDP that is the edge of the WAN into the TIC Portal, in compliance to FIPS 140-2, to create the Agency's DMZ. The encryption removes the need of the inner firewall. The contractor shall manage the SED used to fulfill this requirement.
9. The firewall(s) supported shall be compliant to the TIC Portal SOC standard security policy, as described in Section C.2.4.1.5.1.4 (3).
10. Inter-Agency traffic shall be routed through and inspected by the TIC Portal *if the connection is classified as an external connection*.
11. During emergencies, if the public Internet is under attack, the Government traffic shall be isolated from the public Internet and Inter-Agency traffic flows shall be re-routed (loopback) to create a Government only Extranet. This may be

accomplished by routers located at the Internet access end of the TIC Portal, as described in Section C.2.4.1.5.1.4.1(1).

12. The contractor shall provide flexible traffic routing with full connectivity to the Internet, only through the TIC Portal.
  - a. To facilitate congestion management.
  - b. For continuity of operations.
    - i. In cases of telecommunications (connection) failure (such as a circuit outage or a line break).
    - ii. In cases of a Denial-of-Service (DoS) attack that utilizes most, if not all available bandwidth.
13. The contractor shall provide subscribing Agencies with a web-based administrative tool to view the following:
  - a. Operational state.
  - b. Order status.
  - c. Other transport parameters associated with each MTIPS.

#### **C.2.4.1.5.1.5 MTIPS Basic Service Summary**

1. The contractor shall provide a summary of all the functions and capabilities included in the MTIPS basic service offering.
2. The contractor shall characterize all functions and capabilities included with the basic service. As follows:
  - a. State if the characterization is bandwidth dependant.
  - b. Numerical characterization of functions and capabilities. As a minimum, the basic service shall include:
    - i. Storage space (Gigabytes).
    - ii. Number of concurrent sessions.
    - iii. Firewall throughput
    - iv. Anti-virus throughput.
    - v. Maximum number of policies/rules.
    - vi. Maximum number of VPNs.
    - vii. Maximum number of new sessions.
3. Please explain how the dimensioning of the solution ensures that the performance metrics and SLAs are met.
4. Please quantify the impact of the backhauling of traffic over the performance metrics required.

#### **C.2.4.1.5.2 Features**

The MTIPS features delineated in Section C.2.4.1.5.2.1 are mandatory unless marked optional.

**C.2.4.1.5.2.1 MTIPS Features**

ID Number	Name of Feature	Description
1	Encrypted Traffic	The TIC Portal shall monitor, scan and filter <i>the</i> incoming and outgoing encrypted traffic traversing MTIPS (e.g., email, authorized / known bad mail, FTP and web traffic) which is proxied / non-proxied based on URL or IP address. <i>The TIC portal shall analyze all encrypted traffic for suspicious patterns that might indicate malicious activity and shall keep logs of at least the source, destination and size of the encrypted connections for further analysis.</i>
2	Agency Security Policy Enforcement	The contractor shall adhere to and support the subscribing Agency's security policy to ensure security regulations compliance.  The contractor shall support Agency's operational models and specific security rules. These shall be negotiated between the Agency and the contractor.  The contractor shall support adjustments to the Agency's security strategy based on threats identified by the TIC Portal SOC. For example, adjustments to the security policy could be made by the Agency's authorities after the SOC identifies changing trends in intrusion behavior
3	Forensic Analysis	<i>The contractor shall support full, real-time, header and payload, raw packet capture of selected Agency's traffic flows and shall support subsequent forensic traffic analysis of cyber incidents as required by the Agency (administrative, legal, audit or other operational purposes).</i>  The Agency will identify technical requirements such as, but not limited to traffic of interest (relevant traffic to capture).  The Agency will require support to engineering parameters applied to the traffic capture such as, but not limited to packet capture rate and data retention period (e.g., 5% of the Agency's traffic traversing the TIC Portal for a period of 60 days).
4	Custom Reports	<i>The contractor shall provide reports as required by the subscribing Agency, including ad-hoc reports.</i>
5	Agency NOC/SOC Console	<i>The contractor shall provide additional features and functions customized to Agency's specifications not covered by the Web portal included in the basic service as per requirement Section C.2.4.1.5.1.4.2 (12).</i>
6	Custom Security Assessment and Authorization Support [formerly known as Certification & Accreditation (C&A)]	<ol style="list-style-type: none"> <li>1. Agencies opting for security controls more stringent than the NIST High-Impact Baseline will negotiate Agency-unique requirements directly with the contractor.</li> <li>2. The contractor shall provide additional support to the Agency in the Security Assessment and Authorization (C&amp;A) process for systems and services provided under the contract in accordance with the following prescribed activities:</li> </ol>

ID Number	Name of Feature	Description
		<ul style="list-style-type: none"> <li>a. OMB Circular A-130 Appendix III — Management of Federal Information Resources.</li> <li>b. NIACAP (NSTISSI 1000) — National Information Assurance Certification and Accreditation Process.</li> <li>c. NIST SP 800-37 Rev 1 — Guidelines for <i>Applying the Risk Management Framework to Federal Information Technology Systems: A Security Life Cycle Approach</i>.</li> <li>d. DIACAP (DoD 8510.01) — DoD Information Assurance Certification and Accreditation Process.</li> <li>e. Agency specific requirements for <i>Security Assessment and Authorization (C&amp;A)</i>.</li> </ul> <p>3. The contractor shall ensure that the <i>Security Assessment and Authorization (C&amp;A)</i> deliverables comply with all applicable federal laws, regulations, policies, guidelines, and standards.</p>
7	External Network Connection	<p>The contractor shall enable the Agency to connect to external IP networks at their physical locations. The traffic exchanged shall be IP traffic only and compliant to TIC Portal's interconnecting requirements.</p> <p><i>The TIC Portal shall support dedicated external connections to external partners (e.g., non-TIC federal Agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities shall be supported for external dedicated VPN and private connections implemented using Network transport services, i.e. private lines or other dedicated connections SONETS, E-LINE, NBIP-VPNS, etc. at the TIC Portal:</i></p> <ul style="list-style-type: none"> <li>1. <i>The connection shall terminate in front of NCPS (EINSTEIN) to allow traffic to/from the external connections to be inspected. The NCPS device and the security stack at the portals are the public facing side of the TIC Zone. The incoming traffic from the external network shall be inspected by the NCPS device and the security stack before reaching the internal network.</i></li> <li>2. <i>The connection shall terminate in front of the full suite of TIC sensors/capabilities to allow traffic to/ to be inspected.</i></li> <li>3. <i>When connecting over the public networks including the Internet, the VPN connections from external connections shall be encrypted, compliant to NIST FIPS 140-2.</i></li> <li>4. <i>Connections terminated in front of NCPS may use split tunneling.</i></li> </ul> <p>If required by the Agency, the MTIPS contractor shall configure telecommunications <i>service priority (TSP)</i> for external connections, including to the Internet, to provide for</p>

ID Number	Name of Feature	Description
		<p><i>priority restoration of telecommunication services.</i></p> <p><i>The External Network Connection Feature is subject to performance measures established by Networx depending on the transport service selected for connectivity and included in Networx Contracts Sections C and J.</i></p> <p><i>Regarding filtering/monitoring performance at the portal, the External Network connection shall comply with KPIs established in Section C.2.4.1.5.4.1.</i></p>
8	Encrypted DMZ	<p>The contractor shall support encryption, FIPS 140-2 compliant, from the Agency's SDP at the edge of the Agency's WAN to the MTIPS Portal.</p> <p>The contractor shall provide encryption devices and shall manage the devices.</p>
9	Remote Access	<p>The MTIPS portal shall support telework/remote access for subscriber Agency's authorized staff and users using ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet. For permanent VPN connections for branch offices or business partners use Feature 7 or 10 as appropriate. In addition to supporting the requirements of OMB M-06-16, "Protection of Sensitive Agency Information," the following baseline capabilities shall be supported for telework/remote access at the MTIPS portal:</p> <ol style="list-style-type: none"> <li>1. The VPN connection shall terminate behind NCPS (EINSTEIN device) and full suite of TIC sensors/capabilities so that all outbound traffic to/from the VPN users to external connections, including the Internet, can be inspected by NCPS (EINSTEIN device) and the MTIPS portal security devices. In the case of outgoing traffic from the VPN users, the "Remote Access Enclave" shall connect to the aggregation devices located at the MTIPS transport interface before connecting to the portal's security stack and the NCPS so that the outgoing traffic from the remote user/teleworker be inspected prior to reaching the Public Internet. This traffic flow is shown by a dotted arrow.</li> <li>2. The VPN connection shall terminate in front of MTIPS-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from remote access users to internal networks to be inspected. Refer to the solid arrows in Figure C.2.4.1.5-3.</li> <li>3. All VPN connections shall be NIST FIPS 140-2 compliant. (see NIST SP 800-46 Rev1).</li> <li>4. The telework VPNS shall not be capable of split tunneling (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of NCPS.</li> <li>5. The contractor shall use multi-factor authentication (see NIST SP 800-46 Rev1).</li> <li>6. VPN concentrators and Virtual-Desktop/Application</li> </ol>

**GS00T07NSD0038**  
**Modification Number: PS449**

ID Number	Name of Feature	Description
		<p>Gateways (Remote Access Enclave) shall use hardened appliances and shall be maintained in a separate network security boundary depending on the contractor's implementation.</p> <p>7. Should telework/remote clients use Government Furnished Equipment (GFE), the VPN connection may use access at the IP network-level and access through specific Virtual Desktops/Application Gateways.</p> <p>8. If telework/remote clients use non-GFE, the VPN connection shall only use access through specific Virtual Desktops/Application Gateways.</p> <p>MTIPS subscriber Agencies may support additional telework/remote access connections for authorized staff and users using equivalent Agency-managed security controls within their internal network security boundary. (FYI to contractors →Inventory of these additional telework/remote access connections will be responsibility of the subscriber's Agency-level NOC/SOC. )</p> <p>When Agency users telework with non-GFE equipment, it will be difficult to verify the configuration, sanitization of temporary and permanent data storage, and analysis of possible compromises. Therefore, the subscribing Agency will be responsible to document in accordance with OMB M-07-16 if sensitive data may be accessed remotely using non-GFE, and informing the MTIPS Contractor of the appropriate security configuration policies to implement.</p> <p>The following components/functions shall be used to implement Remote Access for Teleworkers' Connections at the MTIPS portals:</p> <ul style="list-style-type: none"> <li>• The contractor shall support SSL and IPSec VPNs to connect to the MTIPS portals. The contractor shall provide the computer client (agent) if required by the Agency.</li> <li>• The contractor shall support a minimum of 2 Mbps per user of guaranteed bandwidth at the portal (Remote Access Enclave).</li> <li>• The contractor shall support "bands" of teleworkers [CONUS and OCONUS], users as follows: <ul style="list-style-type: none"> <li>○ Single User</li> <li>○ 2 to 5 Users</li> <li>○ 6 to 50 Users</li> <li>○ 51 to 100 Users</li> <li>○ &gt; 100 Users</li> </ul> </li> <li>• If the contractor provides the computer's Agent/client, it shall be considered a Service Enabling Device (SED)</li> <li>• The contractor shall support VPN Encryption Algorithm</li> </ul>



ID Number	Name of Feature	Description
		<p>compliant to FIPS 140-2, i.e., 128-bit AES</p> <ul style="list-style-type: none"> <li>• Access/Transport over the Internet maybe Agency provided or end-user provided</li> <li>• Multi-factor authentication services shall be supported, they include passwords and Cryptographic Tokens or PIVs</li> <li>• Management Functions shall be supported as described in Section C.3 to include the following as a minimum: <ul style="list-style-type: none"> <li>○ Plan, Design and Test</li> <li>○ Installation</li> <li>○ Help-Desk (24x7x365)</li> <li>○ Select from In-band or Out-of-band remote management</li> <li>○ Web portal</li> <li>○ Training for end-users or Agency trainer</li> <li>○ Security policy management</li> <li>○ Service Enabling Devices (SEDs)</li> <li>○ Back-up Services</li> </ul> </li> <li>• At the portal, the contractor shall build a separate DMZ (Remote Access Enclave) for Remote Access services to secure VPN concentrators and the rest of the infrastructure required to provide the service, e.g., Application Gateways, Virtualized Infrastructure, etc.</li> <li>• The contractor shall commit to Key Performance Indicators as required by Section C.2.4.1.5.4.</li> </ul> <p>The contractor shall also support customized remote access implementations for teleworkers to meet Agency-specific requirements.</p>
10	Extranet Connections	<p>The TIC portal shall support dedicated extranet connections to internal partners (e.g., TIC Federal Agencies, closed networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated connections to other internal networks provided by Network transport services. The following baseline capabilities shall be supported for extranet dedicated VPN and private line connections at the TIC Portal:</p> <ol style="list-style-type: none"> <li>1. The connection shall terminate behind NCPS (EINSTEIN) and full suite of TIC sensors/capabilities so that all outbound traffic to/from the extranet connections to external connections, including the Internet, is inspected by NCPS (EINSTEIN)</li> <li>2. The connection shall terminate in front of the MTIPS-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from extranet connections to internal networks, including other extranet</li> </ol>

ID Number	Name of Feature	Description
		<p>connections, to be inspected.</p> <p>3. VPN connections over shared public networks, including the Internet shall be NIST FIPS 140-2 compliant.</p> <p>4. Split tunneling shall not be allowed. Any VPN connection that allows split tunneling is considered an external connection, and must terminate in front of NCPS (EINSTEIN).</p> <p>MTIPS subscribers may support dedicated extranet connections with internal partners using equivalent Agency-managed security controls at non-TIC Portal locations. The Agency-level NOC/SOC shall be responsible for maintaining the inventory of extranet connections with internal partners and coordinating Agency-managed security controls.</p> <p>The following components/functions may be used to establish/design and build VPN for Extranet connections:</p> <ul style="list-style-type: none"> <li>• IPsec VPN from the fixed remote location (business partners, remote Agency's sites, other agencies' sites, etc.) to the MTIPS portals</li> <li>• The contractor shall provide Access and Transport over the Internet or the contractor's private networks from the fixed remote location to the MTIPS portals</li> <li>• The contractor shall provide Service Enabling Devices (SEDs) at the remote site to include LAN nodes of different sizes (bandwidth/users)</li> <li>• Multi-Factor Authentication: Passwords, Cryptographic Tokens or PIV shall be supported</li> <li>• Management Functions shall be supported as described in Section C.3 to include the following as a minimum: <ul style="list-style-type: none"> <li>○ Plan, Design and Test</li> <li>○ Installation</li> <li>○ Help-Desk (24x7x365)</li> <li>○ Select from In-band or Out-of-band remote management</li> <li>○ Web portal</li> <li>○ Training for end-users or Agency trainer</li> <li>○ Security policy management</li> </ul> </li> <li>• Performance requirements are in accordance with established NBIP-VPNS and Section C.2.4.1.5.4</li> </ul> <p>The contractor shall also support customized remote access implementations for extranet connections to meet Agency-specific requirements.</p>
11	Inventory/Mapping Service	The Agency may request from the MTIPS contractor to keep an inventory or a complete map of all networks connected to the MTIPS portal. The MTIPS contractor shall maintain a complete map, or other inventory, of all subscriber Agencies' networks

ID Number	Name of Feature	Description
		connected to the TIC access portal. The MTIPS contractor validates the inventory through the use of network mapping devices. Static translation tables and appropriate points of contact shall be provided to US-CERT on a quarterly basis, to allow in-depth incident analysis.

### C.2.4.1.5.3 Interfaces

The contractor shall support the User-to-Network interfaces (UNIs) defined in Section C.2.4.1.5.3.1 for the provisioning of MTIPS.

#### C.2.4.1.5.3.1 User-to-Network Interface for MTIPS

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
1	Asynchronous Transfer Mode (ATM)	<ol style="list-style-type: none"> <li>1. T1</li> <li>2. T3</li> <li>3. E1</li> <li>4. E3</li> <li>5. OC-3c</li> <li>6. OC-12c</li> </ol>	IP/PPP over ATMS
2	Cable High Speed Access (Optional)	320 Kbps up to 10 Mbps	IP/PPP
3	Ethernet	<ol style="list-style-type: none"> <li>1. 1 Mbps up to 1 GbE (Gigabit Ethernet)</li> <li>2. 10 GbE (Optional)</li> </ol>	IP/PPP over Ethernet
4	Frame Relay (FR)	<ol style="list-style-type: none"> <li>1. 56 Kbps with 32 Kbps CIR</li> <li>2. Fractional T1               <ol style="list-style-type: none"> <li>1. 128 Kbps with 64 Kbps CIR</li> <li>2. 256 Kbps with 128 Kbps CIR</li> <li>3. 384 Kbps with 128 Kbps CIR</li> <li>4. 512 Kbps with 256 Kbps CIR</li> <li>5. 768 Kbps with 384 Kbps CIR</li> </ol> </li> <li>3. T1               <ol style="list-style-type: none"> <li>1. 1.536 Mbps with 768 Kbps CIR</li> <li>2. 1.536 Mbps with 1024 Kbps CIR</li> </ol> </li> <li>4. Fractional T3               <ol style="list-style-type: none"> <li>1. 3 Mbps</li> <li>2. 6 Mbps</li> <li>3. 12 Mbps</li> <li>4. 24 Mbps</li> <li>5. 45 Mbps</li> </ol> </li> <li>5. T3</li> </ol>	IP/PPP over FRS

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
		6. E1 7. E3	
5	IP over SONET	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c	IP/PPP over SONET
6	Electrical Interfaces for Dedicated Wireline Access	1. DS0 2. Fractional T1 3. T1 4. Fractional T3 5. T3 6. E1 [Optional] 7. E3 [Optional]	IP/PPP
7	Broadband Access (Optional)	xDSL access at 1.5 to 6 Mbps downlink, and 384 Kbps to 1.5 Mbps uplink	IP/PPP
8	Satellite Access (Optional)	See Networx Contract Section C.2.16.2.4.3.1 Satellite Access Arrangement Interfaces	

#### C.2.4.1.5.4 MTIPS Performance Metrics

The performance levels and AQL of KPIs for MTIPS in Sections C.2.4.1.5.4.1 through C.2.4.1.5.4.3 are mandatory unless marked optional.

##### C.2.4.1.5.4.1 Performance Metrics for TIC Portal

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(TIC Portal)	Routine	99.5%	≥ 99.5%	See Note 1
Grade of Service (GOS) (Failover Time)	Routine	1 minute	≤ 1 minute	See Note 2
Grade of Service (GOS) (Monitoring and Correlation)	Routine	Real Time	≤ 4 hours 90% of the time	See Note 3
	Critical	Real Time	≤ 4 hours 99.9% of the time	
Grade of Service (GOS) (Configuration/Rule Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	See Note 4
		Within 2 hours for an Urgent priority change	≤ 2 hours	
EN (Firewall Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	See Note 5
		Within 4 hours of a Medium	≤ 4 hours	

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
		category event		
		Within 30 minutes of a High category event	≤ 30 minutes	
<b>EN (Intrusion Detection/Protection Security Event Notification)</b>	Routine	Within 24 hours of a Low category event	≤ 24 hours	
		Within 10 minutes of a High category event	≤ 10 minutes	
<b>Grade of Service (GOS) (Virus Updates and Bug Fixes)</b>	Routine	Normal Priority Update 24 hours	≤ 24 hours	See Note 6
		Urgent Priority Update 2 hours	≤ 2 hours	

Notes:

1. The TIC Portal availability is calculated as a percentage of the total reporting interval time that all the TIC Portal components are operationally available to the Agency. Availability is computed by the standard formula:

$$Availability(TICPortal) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Failover Time for the TIC Portal is the time that it takes to switch from one TIC Portal instance to another provided by the same contractor.
3. The GOS (Monitoring and Correlation) — The monitoring and correlation agents in the contractor’s SOC shall detect a security event within 4 hours of its initiation at (a) 90% AQL for Routine, and (b) 99.9% AQL for Critical service levels. The monitoring and correlation systems shall provide real time fusion.
4. The GOS (Configuration/Rule Change) value represents the elapsed time between the configuration/change request and the change completion. The value is measured by logs/reporting. Changes are initiated and prioritized by the Agency, or may be implemented in response to an event. Changes initiated by the contractor require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
5. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification to the Agency. Events are categorized as follows:
  - a. Low — Events in the Low category have a negligible impact on service. They include incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.
  - b. Medium — Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.

- c. High — Events in the High category represent violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software, and configuration problems, which should be immediately reported via email, pager, or telephone, as specified by the Agency.
- 6. *The GOS (Virus Updates and Bug Fixes)* represents the time between the release of the virus updates and bug fixes (patches), and their deployment. This indicator ensures automatic and timely delivery of updates/bug fixes.

**C.2.4.1.5.4.2 Reserved**

**C.2.4.1.5.4.3 Performance Metrics for MTIPS Transport Collection and Distribution**

For MTIPS Transport Collection and Distribution, the nomenclatures of “*end-to-end*” and “*Networx core*” refer to the connectivity from the Agency’s SDP to the access point of connection to the TIC Portal.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(Port)	Routine	99.95%	≥ 99.95%	See Note 1
	Critical	99.995%	≥ 99.995%	
Latency (CONUS)	Routine	60 ms	≤ 60 ms	See Note 2
	Critical	50 ms	≤ 50 ms	
GOS(Data Delivery Rate)	Routine	99.95%	≥ 99.95%	See Note 3
	Critical	99.995%	≥ 99.995%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	
EN(Security Incident Reporting)	Routine	Near real time	≤ 30 min	See Note 5

Notes:

1. Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(Port) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

For *critical user type*, the contractor would provide essentially 100% uptime for customer’s Internet connection with high availability equipment, redundancy, automatic restoration, and reconfiguration

2. Latency is the average one-way time for IP packets to travel over the Neworx core network. The Backbone Latency metric does not apply for DSL, Cable High Speed, and Satellite access methods.

3. Network packet delivery is a measure of IP packets successfully sent and received over the Network core network.
4. See Network Contract Section C.3.3.1.2.4 for the definitions and measurement guidelines.
5. Security incident reporting to DHS US-CERT must be performed in near real-time, (congruent with NIST 800-61 Rev 1), not to exceed 30 minutes, from the time of detection.

#### **C.2.4.1.5.5 MTIPS Network Operations and Management**

##### **C.2.4.1.5.5.1 Network Management**

The contractor shall provide Network Management. See Network Contract Section C.3.3.1 for the Network Management requirements.

##### **C.2.4.1.5.5.2 Security Management**

The contractor shall provide Security Management. See Network Contract Section C.3.3.2 for the Security Management requirements.

The contractor shall support the following operational functions applicable to the contractor's networks and equipment, in addition to the functions specified in Section C.3 of the Network contracts:

1. Remote management of all contractor's network equipment and servers shall be carried through an encrypted connection (e.g., SSH, HTTPS, etc) *[TS.CF.10]*.
2. Management of all contractor's network equipment and servers shall require strong authentication (e.g., one-time password, cryptographic key exchange, etc.) instead of relying on static userID and password, even if the userID and password are encrypted. *[TS.CF.10]*.
3. All contractor's networks shall be instrumented so that US-CERT/DHS and internal federal security personnel have visibility into both EINSTEIN and applicable packet data.
4. The contractor shall create a connection control program where machines that will be connected to new systems shall be fingerprinted, and base-lined (*inventory of all TIC portal systems*). This meta-data shall be archived and the systems shall be audited weekly to maintain the baseline. Included with authorization are the name, telephone number, and email of the system administrator responsible for controlling that machine. The database of system administrators shall be verified at least once a month. *[TO.MG.01]*.
5. The contractor shall create scanners to audit the contractor's systems for deviation from baseline at least once a month.

##### **C.2.4.1.5.5.2.1 MTIPS Rapid Response Loop**

The contractor shall create and document for each subscribing Agency Rapid Response loop functionality as follows:

1. The Contractor shall create Rapid Response loop functionality as follows:
  - a. Threats, near-real time alerts and computer related incidents are collected by the TIC Portal SOC.
  - b. The threats, alerts, and computer security related incidents and suspicious activities collected are sent to the subscribing Agency's NOC/SOC or appointed Agency security authorities / representatives.
  - c. Agency authority/representative analyzes the severity of threats and security related incidents and make decisions to react.
  - d. Agency authority/representatives contact TIC Portal SOC personnel and relate decisions to protect Agency's networks via phone, fax, or email. See Requirements in Section C.2.4.1.5.1.4.1 (3) (p) (3) Control Mechanisms (Rapid Response Loop).



2. The contractor shall include in the Rapid Response Loop documentation the procedure used shall also report incidents or suspicious activity, near real-time, to the DHS US-CERT per FISMA.

**C.2.4.1.5.5.2.2 MTIPS Global Response Loop**

1. The MTIPS contractor participating in the EINSTEIN program shall ensure that resources are in place to enable the Global Response Loop. The Global Response Loop works as follows:
  - a. The EINSTEIN appliances will transmit collected, analyzed, and correlated alerts and events to US-CERT.
  - b. US-CERT will collect and correlate threats and events from all EINSTEIN appliances deployed across TICAPs.
  - c. US-CERT will declare global security threats and will primarily disseminate them to TIC Portal SOC(s) via the ~~classified phone and email functioning in the SCIF that may be collocated at the SOC.~~ appropriate communications channels, i.e., e-mail, telephone, etc.
2. The contractor shall comply with the following requirements:
  - a. Disseminate US-CERT broadcasted alerts to Agency NOC/SOC or Agency designated authorities.
  - b. Ensure that (b) triggers a Rapid Response Loop as described in Section C.2.4.1.5.5.2.1.
  - c. Store US-CERT broadcasted alerts as known threats in the SOC Knowledge Database.

Formatted: Not Highlight

**C.2.4.1.5.5.2.3 Roles and Responsibilities**

The roles and responsibilities of the subscribing Agency and the contractor for the basic MTIPS operations are described in Table C.2.4.1.5-1 below. The contractor shall agree with the subscribing Agency on specific requirements to support an Agency’s mission. The contractor shall initiate the management process with a discovery session with the subscribing Agency.

**Table C.2.4.1.5-1 Subscribing Agency & Contractor Roles for MTIPS Security Operations**

ID Number	TIC SOC Security Support Services O&M Functions	Subscribing Agency Role	Contractor Role
1	Security Device Monitoring	1.Receive alerts from distributed devices 2. Monitor devices	1. Provide devices’ alerts and system reporting 2. Monitor devices.
2	Security Device	1. Validate alerts	Provide initial alerts’ analysis

ID Number	TIC SOC Security Support Services O&M Functions	Subscribing Agency Role	Contractor Role
	Administration & Management	2. Determine response	
3	Security Engineering	Review for implementation and support	Design for implementation and support
4	Audit Log Management	Acceptance and oversight	Acceptance and oversight
5	Transition and Implementation	Acceptance and oversight	Acceptance and oversight
6	Access Controls (security devices)	Grant access based on verification	Implement and monitor access controls
7	Firewall Management	Oversight, review and approval	Manage all firewall rules and configurations
8	Network Intrusion Security Event Detection / Analysis / Prevention	Global oversight	1. Monitor 2. Initial analysis 3. Provide reports on anomalous network events
9	Network Anti-Virus Management	Oversight	1. Manage scanning devices 2. Monitor incoming traffic
10	Incident Response and Management	Oversight and engineering support	Proactive & Reactive engineering support
11	Vulnerability Assessment and Management	Compliance tracking and oversight	Conduct assessment in accordance with schedule
12	Change and Configuration Management	Initiate and approve changes	Initiate and implement changes
13	Security Reporting	Review and oversight	Produce status & performance reports in accordance with schedule
14	Security Policy Enforcement and Review	Create policy guidance and review	1. Enforce policy guidance 2. Provide recommendations

#### C.2.4.1.5.5.2.4 Security Domain Overview

The following presents an overview of the MTIPS security domains and clearly differentiates the FISMA Security Assessment and Accreditation of the SOC from the other MTIPS components.

**Table C.2.4.1.5-2 MTIPS Security Domain Overview**

Component	Description	Requirement	Compliance	Approval	Comments
<b>SOC</b>	<b>Physical (secured contractor facility)</b>	<b>Security Assessment and Accreditation</b>	<b>FISMA</b>	<b>GSA</b>	<ul style="list-style-type: none"> <li>• Cleared personnel</li> <li>• Redundant sites</li> </ul>
<i>SCIF</i>	<i>Physical (on-site)</i>	<i>Security Assessment and Accreditation</i>	<i>ICD-705</i>	<ul style="list-style-type: none"> <li>• <i>DHS (New)</i></li> <li>• <i>Existing</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>TS-cleared personnel</i></li> <li>• <i>GFE</i></li> <li>• <i>COMSEC</i></li> </ul>
<i>Hosted EINSTEIN Enclave</i>	<i>Sensor</i>	<i>Security Assessment and Accreditation</i>	<i>FISMA</i>	<i>DHS</i>	<ul style="list-style-type: none"> <li>• <i>US-CERT-managed</i></li> <li>• <i>Carrier provides co-location</i></li> </ul>
<i>Internet Access</i>	<i>Network Transport Service</i>	<i>N/A</i>	<i>N/A</i>	<i>N/A</i>	<i>Not Applicable</i>
<i>MTIPS Transport</i>	<i>Network Transport Service</i>	<i>Responsibility of Subscribing Agency</i>			
<i>Access to Agency Enterprise WAN</i>	<i>Network Access Arrangement</i>	<i>Responsibility of Subscribing Agency</i>			

**C.2.4.1.5.6 Disaster Recovery**

The contractor shall provide Disaster Recovery. In the event of a MTIPS system failure or compromise, the contractor shall have the capability to restore operations to a previous clean state. Backups of configurations and data shall be maintained off-site in accordance with the contractor's continuity of operations plan and to be consistent with Networkx operational requirements. See Networkx Contract Section C.3.3.3 for the Disaster Recovery requirements.

**C.2.4.1.5.7 Service Level Agreements**

The IPS is offered by the Networkx Contracts as unprotected IPS as required in Section C.2.4.1 and as MTIPS as described in Section C.2.4.1.5. Agencies have the ability to select how to access the Internet.

The Networkx Contract in Section J.13 defines the required Service Level Agreements (SLAs) that contractors shall meet. An SLA is an agreement between the GSA and the contractor to provide a service at a performance level that meets or exceeds the specified performance objective(s).

Therefore, the contractors supporting MTIPS shall comply with the following:

1. Guidelines on the Networkx SLAs included in Section J.13.1 of the Networkx Contract.
2. SLA Measurement Guidelines provided in Networkx Contract Section J.13.2 SLA Measurement Guidelines
3. SLA Performance Objectives for MTIPS as included in Section J.13.3.9.1.
  - a. Service-Independent Performance Objectives — The contractor shall meet the service-independent SLAs in Networkx Contract Section J.13.3 SLA Performance Objectives.
4. Credit Arrangements — The contractor shall meet the requirements in Networkx Contract Section J.13.4 Credit Arrangements.
5. In the SLA the contractor shall document that the subscribing Agency retains ownership of its data collected by the contractor at the MTIPS portal.

**C.2.4.1.5.8 MTIPS Security Assessment and Authorization Requirements  
(formerly known as Certification and Authorization, C&A)**

A contractor entering into an agreement for services to the GSA and Federal Clients, shall be contractually subject to all federal and GSA IT security directives, standards, policies, and reporting requirements. The contractor shall comply with FISMA associated guidance and directives to include all applicable, current and new FIPS, NIST Special Publication (SP) 800 series guidelines (FIPS and NIST SPs available at: <http://csrc.nist.gov/>), GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of Government IT. Compliance references shall include at a minimum:

1. Federal Information Security Management Act (FISMA) of 2002; available at: <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>
2. Clinger-Cohen Act of 1996 also known as the “Information Technology Management Reform Act of 1996”; available at: [http://www.cio.gov/Documents/it\\_management\\_reform\\_act\\_feb\\_1996.html](http://www.cio.gov/Documents/it_management_reform_act_feb_1996.html)
3. Privacy Act of 1974 (5 U.S.C. § 552a).
4. Homeland Security Presidential Directive (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors”, August 27, 2004; available at: <http://www.idmanagement.gov/>.
5. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources”, and Appendix III, “Security of Federal Automated Information Systems”, as amended; available at: [http://www.whitehouse.gov/omb/circulars\\_a130\\_a130trans4/](http://www.whitehouse.gov/omb/circulars_a130_a130trans4/).
6. OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies.” (Available at: [http://www.whitehouse.gov/omb/memoranda\\_2004](http://www.whitehouse.gov/omb/memoranda_2004)).

7. FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems."
8. FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems."
9. FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."
10. NIST Special Publication 800-18 Rev 1, "Guide for Developing Security Plans for Federal Information Systems."
11. NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."
12. NIST Special Publication 800-34 Revision 1, "Contingency Planning Guide for Information Technology Systems."
13. NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."
14. NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems."
15. NIST Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations."
16. NIST Special Publication 800-53A, Revision 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans."
17. NIST Special Publication 800-88, "Guidelines for Media Sanitization"

In addition to complying with the requirements under paragraph C.3.3.2 of the Network Contract, the contractor shall comply with the GSA policies as identified below as well as any new/updated directives and guides (these documents are referenced within the GSA IT Security Policy and are available upon request to the GSA MTIPS ISSO):

1. GSA Information Technology (IT) Security Policy, CIO P 2100.1( ).
2. GSA Order CIO P 2181.1 "GSA HSPD-12 Personal Identity Verification and Credentialing Handbook".
3. GSA Order CIO 2104.1, "GSA Information Technology (IT) General Rules of Behavior"
4. GSA Order CPO 1878.1, "GSA Privacy Act Program"
5. GSA IT Security Procedural Guide 01-01, "Identification and Authentication"
6. GSA IT Security Procedural Guide 01-02, "Incident Response"
7. GSA IT Security Procedural Guide 01-05, "Configuration Management"
8. GSA IT Security Procedural Guide 01-07, "Access Control"
9. GSA IT Security Procedural Guide 01-08, "Audit and Monitoring"

10. GSA IT Security Procedural Guide 04-26, "FISMA Implementation"
11. GSA IT Security Procedural Guide 05-29, "IT Security Training and Awareness Program"
12. GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing"
13. GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk"
14. GSA IT Security Procedural Guide 06-32, "Media Protection Guide"
15. GSA IT Security Procedural Guide 07-35, "Web Application Security Guide"
16. GSA IT Security Procedural Guide 08-39, "FY 2011 IT Security Program Management Implementation Plan"
17. GSA IT Security Procedural Guide 08-43, "Key Management Guide"
18. GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)"
19. GSA IT Security Procedural Guide 10-50, "Maintenance Guide"
20. GSA IT Security Procedural Guide 11-51, "Conducting Penetration Test Exercise Guide"

#### **C.2.4.1.5.8.1 GSA Security Compliance Requirements**

FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems", is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in eighteen security-related areas. Contractor systems supporting GSA shall meet the security requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 3 (hereafter described as NIST 800-53) "Recommended Security Controls for Federal Information Systems."

GSA has determined that the security category of the information and information system used to provide SOC functions for MTIPS shall be established at the High Impact Level in accordance with FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems", and that baseline security controls shall be established as identified in NIST 800 -53 and other associated directives and guides identified and/or provided by GSA.

#### **C.2.4.1.5.8.2 Security Assessment and Authorization Activities (formerly known as C&A)**

The implementation of a new federal government IT system requires a formal approval process known as Security Assessment and Authorization (formerly known as C&A). NIST Special Publication 800-37, Revision 1 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk", provides guidance for performing the Security Assessment process. The contractor system shall have a valid Security Assessment and authorization (approved by GSA) prior to being placed into operation and processing government information. Failure to obtain and maintain a valid Security Assessment and Authorization shall be grounds for termination

of the contract. The system shall have a new Security Assessment and Authorization conducted (and approved by GSA) at least every three (3) years or at the discretion of the Authorizing Official (AO) when there is a significant change to the system's security posture. All NIST 800-53 controls shall be tested and assessed no less than every 3 years unless otherwise determined by the AO.

#### **C.2.4.1.5.8.2.1 Authorization of System**

1. The contractor shall comply with Security Assessment and Authorization requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the Security Assessment and Authorization is based on the System's NIST FIPS Publication 199 categorization. At a minimum, the contractor shall create maintain and update the following Security Assessment and Authorization documentation:
  - a. System Security Plan (SSP) shall be completed in accordance with NIST Special Publication 800-18, Revision 1 and other relevant guidelines. The SSP shall also include, at a minimum, the following appendices consisting of required policies and procedures across 18 control families mandated per FIPS 200.
  - b. Security Accreditation Boundary Scope Document (BSD) Update as identified in NIST 800-37, Rev 1. A template shall be provided upon request to the GSA MTIPS ISSO.
  - c. Interconnection Agreements developed in accordance with NIST Special Publication 800-47.
  - d. GSA NIST 800-53 R3 Control Tailoring Worksheet as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk". A template shall be provided upon request to the GSA MTIPS ISSO. Column E of the worksheet titled "Contractor Implemented Settings" shall document with all contractor implemented settings that are different from the GSA defined setting and where the GSA defined setting allows a contractor to deviate.
  - e. GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk". A template shall be provided upon request to the GSA MTIPS ISSO.
  - f. Rules of Behavior for information system users as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk".
  - g. System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk".
  - h. Contingency Plan (including Disaster Recovery Plan and Business Impact Assessment) completed in agreement with NIST Special Publication 800-34 Rev 1.

- i. Contingency Plan Test Plan and Report completed in agreement with GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing."
  - j. Privacy Impact Security Assessment completed as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk".
  - k. Plan of Action and Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)."
  - l. All FIPS 199 High impact information systems shall complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities on an annual basis. All penetration test exercises shall be coordinated through the GSA Office of the Senior Agency Information Security Officer (OSAISO) at [itsecurity@gsa.gov](mailto:itsecurity@gsa.gov) per the GSA IT Security Procedural Guide 11-51.
2. All FIPS 199 Low, Moderate, and High impact information systems are encouraged (not a requirement) by GSA OSAISO to conduct a code analysis using tools to examine the software for common flaws and document results in a Code Review Report.
  3. At the moderate impact level and higher, the government shall be responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk."
  4. If the government is responsible for providing a Security Assessment/Risk Security Assessment and Penetration Test, the contractor shall allow GSA employees (or GSA designated third party contractors) to conduct Security Assessment and Accreditation activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk". Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Government information. This includes the general support system infrastructure.
  5. Identified gaps between required 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Security Assessment report shall be tracked for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)." Depending on the severity of the gaps, the government may require them to be remediated before an Authorization to Operate (ATO) is issued.
  6. The contractor is responsible for mitigating all security risks found during the Security Assessment and Authorization and continuous monitoring activities. All high-risk vulnerabilities shall be mitigated within 30 days and all moderate risk vulnerabilities shall be mitigated within 90 days from the date vulnerabilities are



formally identified. The government shall determine the risk rating of vulnerabilities.

#### **C.2.4.1.5.8.2.2 Continuous Monitoring**

Maintenance of the security authorization to operate shall be through continuous monitoring of security controls of the contractor's system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables shall be updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

#### **C.2.4.1.5.8.2.3 Quarterly Deliverables**

The following deliverables shall be provided to be provided to the GSA COTR/ISSO/ISSM on a Quarterly basis.

1. Plan of Action & Milestones (POA&M) Update
2. Vulnerability scanning reports for Operating System, Web Application, and Database scans (as applicable).
3. Vulnerability scanning results shall be managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission.

#### **C.2.4.1.5.8.2.4 Annual Deliverables**

The following deliverables shall be provided to the GSA COTR/ISSO/ISSM initially and as updates (if required) on an annual basis.

1. System Security Plan (SSP)
2. Security Accreditation Boundary Document (BSD)
3. User Certification/Authorization Review (Annotated on POA&M)
4. Information Security Awareness and Training
5. System(s) Baseline Configuration Standard Document
6. System Configuration Settings
7. Contingency Plan
8. Configuration Management Plan
9. Contingency Plan Test Plan
10. Contingency Plan Test Report
11. Incident Response Test Report

12. Information System Interconnection Agreements
13. Rules of Behavior
14. *GSA NIST 800-53 R3 Control Tailoring Worksheet*
15. GSA NIST SP 800-53 rev3 Baseline Summary of Controls Table
16. Independent penetration test and report
17. Annual FISMA Data Call (Data Call format provided by Executive Agent each Fiscal Year)

#### **C.2.4.1.5.8.3 Document and Policy Update**

The contractor shall develop and keep current all other documents and policies as identified in the “GSA 800-53 R3 Control Tailoring” worksheet. A template shall be provided upon request to the GSA MTIPS ISSO and shall be used as a guide to maintain update requirements.

#### **C.2.4.1.5.8.4 HSPD-12 Compliance Requirements**

Homeland Security Presidential Directive 12 (HSPD-12) applies to each contractor SOC. The contractor shall comply with HSPD-12 as implemented by OMB Memorandum-05-24 (M-05-24), “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.”

#### **C.2.4.1.5.8.5 Custom Security Assessment and Authorization Support for Agency-Unique Requirements**

The contractor shall provide Custom Security Assessment and Authorization Support by Feature ID Number 6, Figure 2.4.1.5.2.1 MTIPS Features. Custom support may address Agency-unique requirements for the Initial Security Assessment and Authorization, Continuous Monitoring, and/or system changes and Three-Year FISMA Re-authorization. Negotiated scope of work shall be incremental using the minimum Security Assessment and Authorization Support baseline of the basic MTIPS service.

#### **C.2.4.1.5.8.6 Release of Contractor Security Assessment and Authorization Documentation to Subscribing Agencies**

The contractor shall directly manage the release of all Security Assessment and authorization documentation to subscribing Agencies IAW with contractor’s information security requirements. All Security Assessment and Authorization documentation shall be treated as critical unclassified information (CUI) and protected accordingly.

#### **C.2.4.1.5.9 Supply Chain Risk Management (SCRM) Plan**

MTIPS shall include a Contractor Supply Chain Risk Management (SCRM) Plan to address counterfeit and illegally modified products.

The MTIPS supply chain consists of organizations, people, activities, information, resources, and also the information and communication technology (ICT) equipment,

subcomponents and software. The products are installed into the MTIPS configuration, from the contractor, system integrators, ICT re-sellers, and ICT and component *Original Equipment Manufacturers* (OEMs). Genuine ICT are ICT equipment, components and software that are as represented by their suppliers, whether named brand products or commodity products specified only by performance characteristics.

The contractor shall develop a SCRM Plan to reduce supply chain risks to performance and security of the contractor's MTIPS throughout the contractor's Multi-Agency TICAPs solution life cycle.

#### **C.2.4.1.5.9.1 SCRM Plan Requirements**

The SCRM Plan shall provide sufficient detail for the Government to determine the contractor reasonably understands the MTIPS Supply Chain. The contractor shall ensure that Genuine ICT will be employed in the MTIPS, and shall manage the risk that counterfeit or illegally modified products will be employed within the MTIPS. The SCRM Plan shall describe the processes and practices the contractor shall employ to ensure that Genuine ICT is employed in the contractor's MTIPS. As a result, a body of evidence will be generated through SCRM Plan execution. The body of evidence will provide the Government assurance that Genuine ICT is employed in the contractor's Multi-Agency TICAP solution.

The technical proposal for a SCRM Plan shall address, at a minimum, how the contractor.

1. Ensures within its processes that requirements for Genuine ICT are levied upon its direct suppliers, whether systems integrator, reseller or OEM. The requirements for assurance and supporting evidences shall include:
  - a. That system integrators perform all steps to ensure contractor's SCRM plan will be performed for ICT in delivered configuration.
  - b. That the equipment resellers from whom the contractor purchases ICT for use within the MTIPS have valid licenses for OEM equipment and software.
  - c. That the ICT OEM is exercising quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product.
  - d. Ensures traceability of assurance and evidence of genuineness of ICT back to the licensed product and component OEMs.
2. Ensures that products and components are not repaired and shipped as new products and components provided to the Government.
3. Ensures the MTIPS will be monitored for counterfeit throughout the life cycle to include maintenance and repair.
4. Ensures independent verification and validation of assurances and supporting evidence, as required

### **C.2.4.2 Dedicated Hosting Services (DHS)**

Dedicated Hosting Services (DHS) provide Agencies the alternative of hiring a contractor for Web hosting operations. DHS are fully managed by the service provider. The various equipment and facilities comprising the Web hosting environment are operated and administered by the service provider.

#### **C.2.4.2.1 Service Description**

##### **C.2.4.2.1.1 Functional Definition**

Web hosting refers to the process of publishing a Web site and making it available for worldwide Web access. In particular, an Agency hires a Web Hosting company to store its content (Web pages) on a dedicated server, located in the hosting company's Internet Data Center (IDC). A dedicated server is leased strictly to a single Agency; in addition, other infrastructure - including Internet connectivity - is also dedicated or leased for the exclusive use of the Agency.

##### **C.2.4.2.1.2 Standards**

DHS shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

- RFC 1034 - Domain names - concepts and facilities
- RFC 1035 - Domain names - implementation and specification
- RFC 1123 - Requirements for Internet Hosts - Application and Support
- RFC 2181 - Clarifications to the DNS Specification
- RFC 4033 – Domain Name System Introduction and Requirements
- RFC 4034 – Resource Recorded for the DNS Security Extensions
- RFC 4035 – Protocol Modifications for the DNS Security Extensions

The contractor shall comply with new versions, amendments, and modifications made to the above listed documents/standards, when offered commercially.

##### **C.2.4.2.1.3 Connectivity**

Dedicated Hosting Services include the provision of high-speed Internet connectivity – with the Internet Data Centers (IDC). These centers are administered and operated by the contractor.

Any Agency Web site hosted by a third party shall be readily accessible via the worldwide Web.

##### **C.2.4.2.1.4 Technical Capabilities**

Dedicated hosting is a fee-for-service arrangement whereby an Agency hires a contractor for its Web site operations.

The contractor shall provide server configurations to include processor and storage capacity, software, and data center and network connectivity to meet Agency needs.

The following Dedicated Hosting Services capabilities are mandatory unless indicated otherwise: Servers - Hardware

Servers shall include but not be limited to:

1. Single Server configurations
2. Multi-Server or Cluster configurations

Servers – Software Platform

Software platforms shall include but not be limited to:

1. Linux/Apache Web Server
2. Microsoft Windows®/IIS
3. UNIX/Apache Web Server (where UNIX includes HP-UX, IBM AIX, Sun Solaris, etc.)

Standard Operating Environment – Monitoring and Management

The contractor shall provide monitoring and management services including but not limited to:

1. System Availability Monitoring/Management
  - a. Root/administrator-level management
  - b. CPU Utilization
  - c. Physical and Virtual Memory Monitoring
  - d. Storage Capacity
  - e. Server Process Monitoring
  - f. Service Monitoring
  - g. ASCII Log File Monitoring
2. Web Monitoring/Management
  - a. URL/Content Status Monitoring
  - b. Latency and Response Time
  - c. Web Server Log
  - d. File System Utilization
  - e. Web Server Auto-restart
  - f. Domain Administration - i.e. the registration or transfer of a domain name (e.g. [www.gsa.gov](http://www.gsa.gov)). The Government will be responsible for domain name registration fees.

Security (Software Platform)

The contractor shall provide security of the software platform that includes but is not limited to:

- a. Continuous security patch updates
- b. Vulnerability scanning and remedial actions
- c. Firewall
- d. Remote and client-side suspect activity monitoring
- e. Automated detection and logging of suspect activity
- f. Traffic pattern monitoring

#### Security (Building and Facilities)

The IDC shall maintain security on a 24x7 basis. Preferred security methods shall include guards, closed-circuit monitors, alarm-triggered doors with secure card-key access, biometric scanner, and "person-trap" restricted access.

#### *Network Connectivity and Bandwidth*

Each IDC shall support direct Internet connectivity that provides high availability and scalability. Redundancy shall include:

- a. Dual access routers/switches with IEEE 802.3 Ethernet port speeds available from 10 Mps to 1,000 Mps (one Gbps) or higher
- b. Routers/switches shall be dual homed to IP backbone/point-of-presence.

The contractor shall provide Internet bandwidth as needed by the Agency. The contractor shall provide the Agency with burstable bandwidth that automatically scales from the committed information rate (CIR) up to either the full capacity of the interface or the available information rate (AIR) as agreed by the Agency.

#### Power Systems

IDC facilities shall include redundant and high-availability power to government-leased equipment that guarantees availability of power during scheduled maintenance activities and random outages.

Dual power shall be provided to each rack from independent Power Distribution Units (PDUs) to eliminate PDU loss as a single point of failure. By default, each full rack shall be provisioned with 12 outlets connecting to one 110V, 20A circuit.

Dual or redundant N+1 Uninterruptible Power Supplies (UPS) shall be supported. UPS systems shall receive power both from commercial power feeders and diesel-fuel generators.

#### Fire Detection and Suppression

A Very Early Smoke Detection Apparatus (VESDA) system shall be provided for fire detection. The VESDA air sampling system detects invisible byproducts of materials as they degrade during the pre-combustion stages of an incipient fire.

A fire suppression system shall be provided. Acceptable systems include (but are not limited to) multi-zone, pre-action, dry pipe systems.

Cooling Systems

Redundant cooling systems shall be provided in all IDCs.

**C.2.4.2.2 Features**

The following Dedicated Hosting Services features in Section C.2.4.2.1 are mandatory unless indicated otherwise:

**C.2.4.2.1 Dedicated Hosting Services Features**

ID Number	Name of Feature	Description
1	Load Balancing (intra-Internet Data Center solution)	Applicable with multiple servers, this feature shall distribute requests across a pool of servers according to Agency load-balancing criteria.
2	Restoration	The service provider shall restore Agency Web site data using the most recent back-up upon request.
3	Web Server Traffic Analyses	<p>The contractor shall provide comprehensive reporting including but not limited to:</p> <ul style="list-style-type: none"> <li>• User Profile by region and most requested pages</li> <li>• Most frequently downloaded files</li> <li>• Activity by day-of-week and hour-of-day</li> <li>• Most active cities and states</li> <li>• Most accessed directories</li> </ul>
4	Application Hosting [Optional]	<p>The emergence of the Internet and the re-writing of enterprise software for the client-server and Web services models have transformed the way enterprise software applications are provided to end-users. Instead of in-Agency installations, these applications can now be hosted by third parties.</p> <p>The contractor (i.e. Application Service Provider [ASP]) shall provide hosted applications including but not limited to:</p> <ul style="list-style-type: none"> <li>• <i>Customer Relationship Management (CRM)</i> for the management of government's relationship with its constituents. At present, CRM systems are</li> </ul>

ID Number	Name of Feature	Description
		<p>only partially relevant in the public sector. In future, federal Agencies may increasingly adopt best private sector practices regarding customer care and support.</p> <ul style="list-style-type: none"> <li>• <i>Database Systems</i> for management of large-scale structured sets of data; supporting ad hoc query facilities; and, providing report generation capabilities.</li> <li>• <i>Document Management</i> including library services and management of workflow and collaboration.</li> <li>• <i>E-mail/Messaging</i> Leading E-mail/Messaging software is increasingly the target of malicious programming and unauthorized use. Many organizations are turning to ASPs in order to mitigate the security risks associated with electronic mail. ASPs offer advanced and up-to-date security managements systems and procedures.</li> <li>• <i>Enterprise Resource Planning (ERP)</i> for the management of various functions within a federal Agency, including human resources, finance, procurement, and supply chain.</li> <li>• <i>Human Resource Applications</i> for the administration of benefits, time and labor, salary, pension, et cetera. Moreover, HR systems support self-service applications, allowing managers to initiate personnel actions or change position descriptions, avoiding the burden of paper and e-mails. Employees, using browser-based self-service, can manage life events and benefits, such as health insurance coverage, retirement savings, or changing their W-4.</li> </ul>

**C.2.4.2.3 Interfaces**

The Dedicated Hosting Services provider shall provide Internet connectivity at each IDC. Refer to Section C.2.4.1, Internet Protocol Services.

**C.2.4.2.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for DHS shall be measured and monitored as defined in Section C.2.4.2.4.1.

**C.2.4.2.4.1 Dedicated Hosting Services Performance Metrics**



Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (Internet Connection)	Routine	99.99 %	≥ 99.99 %	See Note 1
Availability (Web Site)	Routine	99.7%	≥ 99.7 %	See Note 2
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Internet Connection availability is calculated as a percentage of the total reporting interval time that the Internet Connection is operationally available to the Agency.

Availability is computed by the standard formula:

$$Av(\text{InternetConnection}) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Web Site availability is calculated as a percentage of the total reporting interval time that the Web Site is operationally available to the Agency. Availability is computed by the standard formula:

3. See C.3.3.1.2.4 for the TTR definitions and measurement guidelines.

### **C.2.4.3 Co-located Hosting Services (CHS)**

Agencies that presently own and operate Web hosting environments, but require direct high-speed Internet connections or more secure facilities, may opt for co-located hosting services (CHS). With CHS, Agencies are provided a secure space located in an Internet Data Center (IDC) which includes power supply, climate control, smoke detection, fire suppression, and site surveillance (i.e. motion detection, close circuit television cameras, et cetera).

#### **C.2.4.3.1 Service Description**

##### **C.2.4.3.1.1 Functional Definition**

Co-located Hosting Services allow Agencies to co-locate government-furnished (GFP) within the service provider's Internet Data Center (IDC). The service provider maintains the IDC facilities and infrastructure. Agencies have 24-hour/7-day access to leased space and GFP in the IDCs.

CHS cater to Agencies electing to control its Web hosting platforms, while also seeking the benefits of co-locating such platforms in highly secure IDC sites. CHS also address the so-called *last mile* problem - the potential bandwidth limitations between Agency buildings and Internet Service Providers. By opting for collocation, Agencies obviate the need for substantial investment in high-speed access solutions.

##### **C.2.4.3.1.2 Standards**

Co-located Hosting Service shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

- RFC 1034 - Domain names - concepts and facilities
- RFC 1035 - Domain names - implementation and specification
- RFC 1123 - Requirements for Internet Hosts - Application and Support
- RFC 2181 - Clarifications to the DNS Specification
- RFC 2535 - Domain Name System Security Extensions

The contractor shall comply with new versions, amendments, and modifications made to the above listed documents/standards, when offered commercially.

##### **C.2.4.3.1.3 Connectivity**

Government-furnished property (principally servers), located within IDCs, shall be connected to the Internet described in Section C.2.4.1 – Internet Protocol Services.

##### **C.2.4.3.1.4 Technical Capabilities**

Co-located Hosting Services shall entail the leasing of rack space in an Internet Data Center (IDC). The contractor shall provide Agencies with 24x7 access to leased space and GFP in the IDCs. The IDC shall support the following capabilities:

### Basic Storage Space

The basic storage space shall be configured and leased on a per-rack basis. The following options shall be provided:

- Quarter rack (18" x 19" x 36" – One Shelf)
- Half rack (36" x 19" x 36" – Three Shelves)
- Full rack (72" x 19" x 36" – Six Shelves)

### Security (Building and Facilities)

The IDC shall maintain security on a 24x7 basis. Preferred security methods shall include guards, closed-circuit monitors, and alarm-triggered doors with secure card-key access, biometric scanner, and "person-trap" restricted access. The contractor shall describe the offered security methods and procedures.

### Network Connectivity and Bandwidth

Each IDC shall support direct Internet connectivity, offering high availability and scalability. Redundancy shall include:

- dual access routers/switches shall be supported with port speeds available from 10 Mps to 1,000 (One Gbps) or higher; and
- all collocation routers/switches shall be dual homed to IP backbone/point-of-presence.

The contractor shall provide Internet bandwidth as needed by the Agency. The contractor shall provide the Agency with burstable bandwidth that automatically scales from the committed information rate (CIR) up to either the full capacity of the interface or the available information rate (AIR) as agreed by the Agency.

The contractor shall describe its Internet infrastructure (e.g., Tier-1 backbone connectivity) – or business relationships with other Network Service Providers – that ensure minimal latency, fewest possible Autonomous System *hops*, et cetera.

### Power Systems

IDC facilities shall include redundant and high-availability power to government-furnished equipment, guaranteeing availability of power during scheduled maintenance activities and outages.

Dual power shall be provided to each rack from independent Power Distribution Units (PDUs), eliminating PDU loss as a single point of failure. By default, each full rack shall be provisioned with 12 outlets connecting to one 110V, 20A circuit.

Dual or redundant N+1 Uninterruptible Power Supplies (UPS) shall be supported. UPS systems shall receive power both from commercial power feeders and diesel-fuel generators.

*Fire Detection and Suppression*

A Very Early Smoke Detection Apparatus (VESDA) system shall be provided for fire detection. The VESDA air sampling system detects invisible byproducts of materials as they degrade during the pre-combustion stages of an incipient fire.

A fire suppression system shall be provided; acceptable systems include (but are not limited to) multi-zone, pre-action, dry pipe systems.

*Cooling Systems*

Redundant cooling systems shall be provided in all IDCs.

**C.2.4.3.2 Features**

The following CHS features in C.2.4.3.2-1 shall be supported:

**C.2.4.3.2.1 CHS Features**

ID Number	Name of Feature	Description
1	Analog Line	Contractor shall provide an analog line (i.e., <i>plain old telephone service</i> ) for Agency cabinets and/or cages for PSTN dial-up access. Analog lines allow Agencies to remotely configure and manage equipment.
2	Cabinets/Cages	Cabinets or cages equipped with locks shall be available for additional security.
3	Host Administrative Tasks	On behalf of the Agency, IDC staff shall intervene and perform minor unscheduled tasks including: <ul style="list-style-type: none"> <li>• Rebooting of government-furnished equipment (limited to power cycling).</li> <li>• Manual entry of commands to servers from a keyboard.</li> <li>• Inspection and reading of alarm indicators and displays.</li> <li>• Securing cabling to connections.</li> <li>• Setting a dip switch.</li> </ul>
4	Periodic Hardware Check (Ping)	The contractor shall ping devices every five minutes. If ping failures occur and devices become unreachable, then the service provider will notify the Agency.
5	Reporting	The use of a "virtual console" shall be available, allowing Agencies to view, monitor, and update trouble tickets and power availability statistics. The "virtual console" will support online reporting via a Web browser.

ID Number	Name of Feature	Description
6	Seismic Bracing	Seismic bracing mitigates the risk to servers and computer equipment in the event of seismic activity, thus reducing damage and disaster recovery costs. The contractor shall provide seismic bracing at IDCs located in areas rated as Seismic Zone Nos. 3 or 4 per NEBS Telcordia GR-63 Standard.
7	Storage Media Change	IDC staff shall change storage media in the Agency's storage drive on a mutually agreed schedule.

**C.2.4.3.3 Interfaces**

The CHS provider shall provide Internet connectivity at each IDC. Refer to Section C.2.4.1 – Internet Protocol Services.

**C.2.4.3.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for CHS are defined in Section C.2.4.3.4.1.

Key performance indicators for Internet connectivity are specified in Section C.2.4.1 – Internet Protocol Services.

**C.2.4.3.4.1 Performance Metrics for CHS**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (Internet Connection)	Routine	99.99 %	≥ 99.99 %	See Note 1
Availability (Site Power)	Routine	100 %	100 %	See Note 2
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Internet Connection availability is calculated as a percentage of the total reporting interval time that the Internet Connection is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(InternetConnection) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Site Power availability is calculated as a percentage of the total reporting interval time that the Site Power is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(SitePower) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

3. See C.3.3.1.2.4 for the TTR definitions and measurement guidelines.

#### **C.2.4.4 Reserved**

#### **C.2.4.5 Internet Facsimile Service (IFS)**

Internet Facsimile Service (IFS) provides Agencies with reliable and cost effective transmission of documents. The service streamlines faxing by using the IP Protocol and advanced internet and web technologies, thereby making the management of the document delivery process more efficient.

##### **C.2.4.5.1 Service Description**

###### **C.2.4.5.1.1 Functional Definition**

Internet Facsimile Service provides the functions of traditional faxing using Internet protocols for part of or all the transmission rather than relying solely on the Public Switched Telephone Network (PSTN). The service increases versatility of faxing by allowing the Agency to send and receive faxes via several means including traditional fax machines, desktop computers, host environments, and the web. IFS also provides broadcast and multicast capabilities enabling the processing of high volume communications. IFS supports secure faxing to meet Agency security needs as necessary.

###### **C.2.4.5.1.2 Standards**

Internet Facsimile Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Internet Engineering Task Force Request for Comments (IETF-RFC) 1939 — Post Office Protocol (POP) - Version 3
2. IETF RFC 3949 — File Format for Internet Fax
3. IETF RFC 2306 — Tag Image File Format (TIFF) - F Profile for Facsimile
4. IETF RFC 2532 — Extended Facsimile Using Internet Mail
5. IETF RFC 2821 — Simple Mail Transfer Protocol (SMTP)
6. IETF RFC 3192 — Minimal FAX Address Format in Internet Mail
7. IETF RFC 3950 — Tag Image File Format Fax eXtended (TIFF-FX) - image/tiff-fx MIME Sub-type Registration
8. IETF RFC 3302 — Tag Image File Format (TIFF) - image/tiff MIME Sub-type Registration
9. IETF RFC 3501 — Internet Message Access Protocol (IMAP) - Version 4rev1
10. IETF RFC 3965 — A Simple Mode of Facsimile Using Internet Mail

11. International Telecommunication Union Telecommunication Standardization Sector Recommendation (ITU-T) F.185 — Internet facsimile: Guidelines for the support of the communication of facsimile documents
12. ITU-T Recommendation T.4 — Standardization of Group 3 facsimile terminals for document transmission
13. ITU-T Recommendation T.30 — Procedures for document facsimile transmission in the general switched telephone network
14. ITU-T Recommendation T.37 — Procedures for the transfer of facsimile data via store-and-forward on the Internet
15. ITU-T Recommendation T.38 — Procedures for real-time Group 3 facsimile communication over IP networks
16. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 140 - 2 — Security Requirements for Cryptographic Modules
17. All new versions, amendments, and modifications of the above when offered commercially
18. All appropriate standards for any applicable underlying Network access and transport services

#### **C.2.4.5.1.3 Connectivity**

Internet Facsimile Service shall provide incoming and outgoing faxing connectivity through traditional fax machines, desktops, LANs, and the Web. The service shall also process incoming faxes from the general public to Agency locations as specified by subscribing Agencies.

#### **C.2.4.5.1.4 Technical Capabilities**

The following Internet Facsimile Service capabilities are mandatory:

1. The contractor shall support incoming and outgoing faxing via traditional fax machines, mainframes/LANs, email, and the Web. This shall include:
  - a. Fax-to-Fax
  - b. Fax-to-Email
  - c. Email-to-Fax
  - d. Web-to-Fax
2. The service shall support connections between the ITU-T T.4/ PSTN and Internet mail, and vice versa, as indicated in the following examples:
  - a. On-ramp faxing, which allows fax calls from a traditional machine to be converted to an email message with a TIFF attachment.
  - b. Off-ramp faxing, which enables a fax email with a TIFF attachment to be converted into a format that can be delivered to a traditional fax machine.

3. The service shall support the conversion of T.30 fax signals coming from the PSTN into T.38 Internet Fax Protocol (IFP) packets and vice versa, as applicable.
4. The service shall allow the routing of faxes to existing e-mail addresses for mail clients such as MS Outlook/Exchange and Lotus Notes.
5. The service shall support the processing of file attachments from common applications that include, but are not limited to, MS Word, MS Excel and MS PowerPoint; Corel WordPerfect Office, and Adobe Acrobat. In addition, the service shall handle graphic formats such as TIFF, JPEG and GIF.
6. The service shall prevent the potential loss of documents caused by busy, heavily used, or otherwise unavailable fax machines. Documents shall be delivered to the destination machine once it becomes available or sent to an alternate delivery point, as specified by the Agency.
7. The service shall provide delivery and completion alerts at fax machines and computers.
8. The contractor shall provide around the clock, Web-based administration and management tools, including secure access to reports; account information for creating and maintaining fax lists and user profiles; and for drafting and sending of messages, as required.
9. The contractor shall provide IFS on a 24x7 basis.
10. The service shall support remote and/or secure web access to service information which shall include, but not be limited to the following:
  - a. Delivery Status
  - b. Error Notifications
  - c. Detail Status per recipient for a specified period
  - d. Completion Receipts for electronic faxes (web, email)
  - e. Date, time, and duration of transmission
  - f. Page Count
  - g. Identity of sender and recipient
  - h. Fax Count for a specified period
11. The service shall be scalable to ensure system availability for low and high volume faxing.

**C.2.4.5.2 Features**

The Internet Facsimile Service features in Section C.2.4.5.2.1 are mandatory, unless marked optional:

**C.2.4.5.2.1 Internet Facsimile Service Features**

ID Number	Name of Feature	Description
1	Back Office Integration (Optional)	The contractor shall support the integration of the fax service with Agency back office systems and applications, using for example, SMTP, Java, or standard Extensible Markup Language (XML) Application Programming Interfaces (APIs), as applicable.



ID Number	Name of Feature	Description
		Among other capabilities, this shall enable optimized document delivery, enhanced routing for customized Agency needs, and Directory Integration allowing an Agency to create profiles from existing user lists.
2	Fax Broadcast	The contractor shall provide a fax broadcast or multicast capability to enable an Agency to send documents to a large number of recipients at once.
3	Fax on Demand (Optional)	The contractor shall provide the capability for an Agency to make various documents, libraries, or frequently requested documents (brochures, forms, guides, for example) available to relevant constituencies. Users shall be able to access the information via fax at any time, and the Agency shall be provided with the means of updating documents as necessary.
4	Private Network Connection (Optional)	The contractor shall allow an Agency to access the contractor's fax platform directly via a private network connection. This feature shall support both inbound and outbound faxing.
5	Tailored Delivery (Optional)	The service shall allow an Agency to personalize or tailor documents according to recipient needs. For example, names, sentences, logos, or form fields may be customized for each addressee.

**C.2.4.5.3 Interfaces**

Internet Facsimile Service shall support the User-to-Network Interfaces (UNIs) defined in Section C.2.4.1 Internet Protocol Service (IPS), as applicable.

**C.2.4.5.4 Performance Metrics**

The performance level and Acceptable Quality Level (AQL) of the Key Performance Indicators (KPIs) for Internet Facsimile Service in Section C.2.4.5.4.1 are mandatory:

**C.2.4.5.4.1 Internet Facsimile Service Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Note:

1. IFS availability is calculated as a percentage of the total reporting interval time that the IFS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(IFS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definition and measurement guidelines.

### **C.2.4.6 Content Delivery Network Services (CDNS)**

Content Delivery Network Services (CDNS) efficiently and rapidly deliver Agency's content to Web browsers worldwide. The CDNS provider will incorporate equipment and algorithms to cache content on geographically dispersed servers on the Internet. When a request is made from a particular location for specific content, the server that can most rapidly and efficiently provide the content is dynamically identified.

Content delivery network services reduce the Internet infrastructure required to provide a domestic or global Web presence. By subscribing to CDNS, Agencies obviate the need for substantial investments in Web servers, firewalls, LAN switches, application software, and co-locations services.

#### **C.2.4.6.1 Service Description**

##### **C.2.4.6.1.1 Functional Definition**

A Content Delivery Network consists of a collection of surrogate servers that attempt to offload work from origin<sup>5</sup> servers by delivering content on their behalf. The servers belonging to a CDNS may be located at the same site as the origin server, or at different locations around the network, with some or all of the origin server's content cached or replicated amongst the CDNS servers. For each request, the CDNS attempts to locate a CDN server close to the client Agency to serve the request, where the notion of "close" could include geographical, topological, or latency considerations.

CDNS address the following technical and operational issues:

- Latency – the delay in delivering Web content to the end-user
- Scalability – Web services automatically scale-up while the end-user requests increase
- Reliability –content is always available and its integrity is assured (i.e. not been altered by third parties including "hackers")
- Flash crowd control – i.e., effectively meeting demand during periods of unexpected high usage

##### **C.2.4.6.1.2 Standards**

CDNS shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Reserved
2. Hyper Text Transfer Protocol (HTTP) and Secure HTTP (HTTPS)
3. Internet Engineering Task Force – Request for Comments (IETF- RFC)

---

<sup>5</sup> An *origin* server is where content originates.

#### 4. Secure Sockets Layer (SSL)

The contractor shall comply with new versions, amendments, and modifications made to the above listed documents/standards, when offered commercially.

##### **C.2.4.6.1.3 Connectivity**

Content delivery/distribution is an application-layer service supported by the connectionless data services available with the Internet Protocol (IP) suite. The service provides data transfer from the origin server to the CDNS via IP. [Refer to Section C.2.4.1 – Internet Protocol Services.]

##### **C.2.4.6.1.4 Technical Capabilities**

The following CDNS capabilities are mandatory unless indicated otherwise:

###### Content Distribution

###### 1. Static Content Download Service

This service provides fast, secure, and reliable download of content - including text, video, music, et cetera. Such content will likely be stored on CDNS servers deployed globally at the edge of the Internet for faster access.

###### 2. Real-time Streaming (Webcasting)

The CDNS provider shall deliver streams in real-time. (The CDNS shall encode the signal when sent in raw signal format by the content provider.)

Real-time streaming content shall include (but not be limited to) RealNetworks Real Media, Microsoft Windows Media, and Apple QuickTime.

###### 3. On-demand Streaming

The CDNS provider shall host (i.e., provide storage) and deliver streams on demand or when requested by end-users. (The CDNS shall encode the signal when sent in raw signal format by the content provider.)

On-demand streaming content shall include (but not be limited to) Real Media, Microsoft Windows Media, and Apple QuickTime.

###### *Site Monitoring/ Server Performance Measurements*

CDNS shall require continuous monitoring to ensure performance and quality of service. Measurements shall include but not be limited to:

- Availability (refer to Section C.2.4.6.4.1)
- Latency (refer to Section C.2.4.6.4.1)
- FTP Load
- CPU Load
- Memory Usage
- SSL Service Load
- HTTP Port Service Load
- HTTP Connections Queue Statistics

The contractor shall provide statistics via a performance dashboard – a secure, Web-based portal accessible by Agency clients on a 24x7 basis. The performance dashboard shall be consistent with commercial best practice.

**C.2.4.6.2 Features**

The CDNS features in Section C.2.4.6.2.1 are mandatory unless indicated otherwise.

**C.2.4.6.2.1 CDNS Features**

ID Number	Name of Feature	Description
1	Failover Service	The contractor shall provide Failover Service. This service monitors single-location Web sites (maintained by Agencies or third-parties under contract to Agencies)) and redirects traffic to a CDNS in the event of failure. This service shall ensure that end-users do not experience delays, site inaccessibility, or error messages.
2 (Optional)	Redirection and Distribution Service (Global Load Balancing)	<p>The contractor shall provide Redirection and Distribution Service (Global Load Balancing). When users type-in a Web site address or Universal Resource Locator (URL), they rely on Domain Name System (DNS) servers to direct them through the Internet and connect them to the specified Web server. Redirection and distribution services ensure that all Web requests are directed to the closest, most available cache server. Typically a set of surrogate servers is provisioned to cache content for the content provider's origin server, enabling requests to bypass congested areas.</p> <p>Redirection and Distribution Services may employ any proven technique(s) including, but not limited to:</p> <ul style="list-style-type: none"> <li>• DNS Redirection</li> <li>• URL Rewriting</li> <li>• Layer-4 Switching</li> <li>• Layer-7 Switching</li> <li>• HTTP Redirection</li> </ul>

**C.2.4.6.3 Interfaces**

The CDNS provider shall provide Internet connectivity to the Agency's origin server(s). Refer to Section C.2.4.1 – Internet Protocol Services.

**C.2.4.6.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Content Delivery Service in Section C.2.4.6.4.1 below are mandatory:

**C.2.4.6.4.1 Performance Metrics for CDNS**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (CDNS network)	Routine	100 %	100 %	See Note 1
Latency (static content download)	Routine	Mean = 1.5 sec	Mean < 1.5 sec	See Note 2
GOS (Time to refresh content)	Routine	5 minutes	< 5 minutes	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. CDNS availability is calculated as a percentage of the total reporting interval time that the CDNS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(CDNS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. The Latency KPI assumes an average “page weight” of 200 kByte and the end-user is served by a broadband connection with a minimum (effective) download speed of 512Kps. Latency is the client-observed response time for downloading the set of images comprising a page from the CDNS server.

3. See C.3.3.1.2.4 for the TTR definitions and measurement guidelines.

**C.2.5 Dedicated Service**

**C.2.5.1 Private Line Service (PLS)**

Private Line Service provides dedicated, reliable full duplex bandwidth for Agency-specific data networks and mission critical applications. The ranges of line speeds and reliability options provided by this service allow Government users to satisfy an array of diverse requirements. This service can be used for various applications such as voice, data, video, multimedia, and encrypted communications.

### C.2.5.1.1 Service Description

#### C.2.5.1.1.1 Functional Definition

Private Line Service provides dedicated duplex transmission connectivity between two or more designated end points over which Agency service applications traverse at Agency-specified bandwidths. The connectivity between the end points are permanently established unless a service request for modification, move, or disconnect is received.

#### C.2.5.1.1.2 Standards

Private Line Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. ANSI T1.102/107/401/403/503/510 for T1
2. Telcordia PUB GR-499-CORE for T3
3. ANSI T1.105 and 106 for SONET
4. Telcordia PUB GR-253-CORE for SONET
5. ITU-TSS G.702 and related Recommendations for E1 and E3
6. Telcordia PUB SR-TSV-002275, TR-NWT-000965, and TR-NWT-000335 for analog
7. Telcordia PUB GR-418-CORE for reliability/performance
8. All new versions, amendments, and modifications to the above documents and standards when offered commercially.

#### C.2.5.1.1.3 Connectivity

Private Line Service shall connect to and interoperate with:

1. Government specified terminations (e.g., SDPs such as PBXs, Multiplexers, Routers, Video codecs, and Group 4 FAXs)
2. All other networks including other Network Universal and Network Enterprise contractors' networks, where additional coordination between networks will be required for interoperability.

#### C.2.5.1.1.4 Technical Capabilities

The following Private Line Service capabilities are mandatory unless marked optional:

1. Transparency to any protocol used by Government furnished property (GFP).
2. Data transparency treatment of all bit sequences transmitted by GFP through the SDP.

The following categories (i.e., data rates) of PLS service shall be supported:

- (a) **DS0**. Information payload data rates of 56 Kbps and 64 Kbps.

- (b) **T1**. Line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 service as follows:
  - (1) Channelized T1. In this mode, 24 separate DS0s clear channels of 56 or Kbps 64 Kbps shall be supported.
  - (2) Unchannelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
- (c) **Fractional T1**. Two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps.
- (d) **T3**. Line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 service as follows:
  - (1) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
  - (2) Unchannelized T3. In this mode, a single 43.008 Mbps payload shall be supported.
- (e) **Fractional T3**. Three, four, five, or seven adjacent DS1 clear-channels.
- (f) **E1** (For Non-US Use) [Optional]. Line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:
  - (1) Channelized E1. In this mode, 30 separate DS0 clear channels shall be supported.
  - (2) Unchannelized E1. In this mode, a single 1.92 Mbps information payload shall be supported.
- (g) **E3** (For Non-US Use) [Optional]. Line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:
  - (1) Channelized E3. In this mode, 16 separate E1 channels shall be supported.
  - (2) Unchannelized E3. In this mode, a single 30.72 Mbps information payload shall be supported.
- (h) **SONET OC-1** [Optional]. Single SONET OC-1 channel with the information payload data rate of 49.536 Mbps over an interface with a line rate of 51.840 Mbps.
- (i) **SONET OC-1 Virtual Tributary** [Optional]. Seven Virtual Tributary (VT) groups over a single SONET OC-1 interface with a line rate of 51.840 Mbps. Each VT group shall be able to independently carry four T1 or two DS1C or one DS2

channel(s); where each T1 has a line rate of 1.544 Mbps and payload data rate of 1.536 Mbps, and each DS1C has a line rate of 3.152 Mbps and information payload data rate of 3.072 Mbps, and each DS2 has a line rate of 6.312 Mbps and information payload data rate of 6.144 Mbps.

- (j) **SONET OC-3.** [Optional] Line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c service as follows:
  - (1) Channelized OC-3. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, shall be supported.
  - (2) Concatenated OC-3c. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps shall be supported.
- (k) **SONET OC-12.** [Optional] Line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c.
  - (1) Channelized OC-12. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, shall be supported.
  - (2) Concatenated OC-12c. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps shall be supported.
- (l) **SONET OC-48.** [Optional] Line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c.
  - (1) Channelized OC-48. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, shall be supported.
  - (2) Concatenated OC-48c. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps shall be supported.
- (m) **SONET OC-192.** [Optional] Line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c.
  - (1) Channelized OC-192. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, shall be supported.
  - (2) Concatenated OC-192c. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps shall be supported.
- (n) **Subrate DS0** [Optional]. This category of PLS shall support subrate DS0 at information payload data rates of 4.8, 9.6, and 19.2 Kbps.
- (o) **Analog** [Optional]. This category of PLS shall support a 4 kHz bandwidth.

#### C.2.5.1.2 Features

The following Private Line Service features listed in Section C.2.5.1.2.1 are mandatory unless marked optional:



## C.2.5.1.2.1 Private Line Service Features

ID Number	Name of Feature	Description
1	Multipoint Connection (Optional)	<p>The contractor shall allow interconnection of three or more subscribers' premises as follows:</p> <ol style="list-style-type: none"> <li data-bbox="548 512 1159 636">1. <u>Branch-Off</u>. In this mode, all SDPs shall be treated as one shared medium and each point shall be able to autonomously send and receive data. The CPE application will ensure master/slave mode of operation (e.g., polling scheme used in IBM 3270 mode of data communication).</li> <li data-bbox="548 646 1159 768">2. <u>Drop-and-Insert</u>. In this mode, previously specified channels of a channelized T1, T3, SONET OC-3, or SONET OC-12 service category shall be able to be dropped off and new channels shall be able to be simultaneously picked up or inserted</li> </ol>
2	Special Routing	<p>The contractor shall provide different routes for PLS circuits based on the following arrangements:</p> <ol style="list-style-type: none"> <li data-bbox="548 846 1159 1314">1. <u>Transport Diversity</u>. Between connecting POPs, the contractor shall supply two or more physically separated routes for PLS circuits. These diverse routes shall not share common telecommunications facilities or offices. The contractor shall maintain a minimum separation of 30 feet throughout all diverse routes. The Government recognizes that uncompromised (i.e., adhering to the minimum separation requirements as described above) diversity may not be available in some locations. Where uncompromised diversity is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the compromise. Each pair of circuits that must be diverse from each other constitutes a relationship pair. For example, three circuits ordered as being diverse from each other constitute three relationship pairs, i.e., 1 and 2, 1 and 3, and 2 and 3. If diversity is not available or the compromised diversity is not acceptable to the Government, it shall be negotiated on an individual case basis.</li> <li data-bbox="548 1325 1159 1518">2. <u>Transport Avoidance</u>. Between connecting POPs, the contractor shall supply the capability for a customer to define a geographic location or route on the network to avoid. The Government recognizes that avoidance may not be available in some locations. Where avoidance is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the reasons for the unavailability.</li> </ol> <p>The contractor shall establish an internal control (i.e., electronic flagging of routes) to prevent accidental dismantling of diversified/avoidance routes, especially during routine route optimization initiatives by the contractor.</p> <p>The contractor shall provide, within 30 calendar days of the implementation of transport diversity or avoidance, and again thereafter whenever a change is made, a graphical representation</p>

ID Number	Name of Feature	Description
1	Multipoint Connection (Optional)	The contractor shall allow interconnection of three or more subscribers' premises as follows: <ol style="list-style-type: none"> <li><u>Branch-Off</u>. In this mode, all SDPs shall be treated as one shared medium and each point shall be able to autonomously send and receive data. The CPE application will ensure master/slave mode of operation (e.g., polling scheme used in IBM 3270 mode of data communication).</li> <li><u>Drop-and-Insert</u>. In this mode, previously specified channels of a channelized T1, T3, SONET OC-3, or SONET OC-12 service category shall be able to be dropped off and new channels shall be able to be simultaneously picked up or inserted</li> </ol>
		(e.g., diagrams/maps) of transport circuit routes to show where diversity or avoidance has been implemented. The contractor shall provide, at least 30 calendar days in advance of implementation, written notification to the Agency (with a copy to the PMO) requesting Government approval of any proposed reconfiguration of routes that were previously configured for transport diversity or avoidance.  When a user selects an explicit diversity and/or avoidance, the performance level of the PLS circuit will be specified by the user at the service ordering time.
3	Analog Line Conditioning (Optional)	The contractor shall provide voice grade C (e.g., C3) and D (e.g., D6) conditioning for analog lines (Standard: Telcordia Pubs: TR-NWT-000335 and TR-NWT-000965).
4	Low Bit Rate Voice (Optional)	The contractor shall allow for voice at 32 Kbps and for analog data at 4.8 Kbps utilizing contractor provided equipment and shall conform to Adaptive Differential Pulse Code Modulation (ADPCM) according to North American adaptation of ITU-TSS recommendation G.721 (compression of a ITU-TSS B.711 voice band signal at 32 Kbps) as modified by ANSI.
5	7.5 kHz Audio (Optional)	The contractor shall allow a 7.5 kHz audio signal, delivered and received in analog form, which shall be compressed by the contractor provided equipment for transmission over a DS0 channel. The audio quality shall not be less than what is available using ADPCM compression technology (standard: ITU-TSS G.726).

### C.2.5.1.3 Interfaces

The User-to-Network-Interfaces (UNIs) at the SDP, as defined in Section C.2.5.1.3.1, are mandatory unless marked optional:

#### C.2.5.1.3.1 Private Line Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 Kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
5	T1 (with ESF) (Std: Telcordia SR-TSV-002275; ANSI T1.403)	Up to 1.536 Mbps	Transparent
6	T3 (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	Transparent
7 [Optional]	E1 (Std: ITU-TSS G.702)	Up to 1.92 Mbps	Transparent
8 [Optional]	E3 (Std: ITU-TSS G.702)	Up to 30.72 Mbps	Transparent
9 [Optional]	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	Transparent
10 [Optional]	Electrical: SONET STS-1/EC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	Transparent
11 [Optional]	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
12 [Optional]	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
13 [Optional]	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
14 [Optional]	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
15 [Optional]	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
16 [Optional]	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
17 [Optional]	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
18 [Optional]	SONET OC-192c (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
19 [Optional]	RJ-x (e.g., RJ-11/45)	4/7.5 kHz Bandwidth	Transparent

#### C.2.5.1.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Private Line Service circuits in Section C.2.5.1.4.1 are mandatory unless marked optional:

#### C.2.5.1.4.1 Private Line Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (POP-to-POP) [Optional]	Routine	99.8%	≥ 99.8%	See Note 1
	Critical (Optional)	99.98%	≥ 99.98%	
Availability (SDP-to-SDP)	Routine	99.4%	≥ 99.4%	
	Critical (Optional)	99.98%	≥ 99.98%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	

Notes:

1. Availability.
  - a. For data rates of T1 and higher, a service is considered unavailable when a PLS circuit experiences 10 consecutive severely errored seconds (SES) [Standard: Telcordia PUB GR-418-CORE]. An unavailable circuit is considered available when restoration activities have been completed and 30 consecutive minutes have passed without any errored seconds to account for stability and proving period. However, if there is no error second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time
  - b. For data rates lower than T1, cumulative outage time is calculated based on trouble ticket data.
  - c. PLS availability is calculated as a percentage of the total reporting interval time that PLS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

Critical level of Service for availability only applies to T1 and above data rates.

2. Refer to Section C.3.3.1.2.4 for definition and how to measure.

#### C.2.5.2 Synchronous Optical Network Services (SONETS)

SONET is the U.S. standard for fiber optic synchronous transmission rates from 51.84 Mbps to beyond 13.27 Gbps while Synchronous Digital Hierarchy (SDH) is the International Telecommunications Union version, which begins at 155 Mbps. SONET transport is highly reliable and provides proactive performance monitoring that prevents single and multiple failures and further enables self-healing functions and robust network management.

### C.2.5.2.1 Service Description

#### C.2.5.2.1.1 Functional Definition

SONETS supports a wide range of digital signals with different capacities and its interworking capability enables seamless communications between devices that support dissimilar protocols such as ATM, Frame Relay, and IP. SONETS enables Agencies to transport voice, data, and video throughout the United States and internationally.

#### C.2.5.2.1.2 Standards

SONETS Services shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. Telcordia Technologies
  - a. GR-1031 OTGR Section 15.6: Operations Interfaces Using OSI Tools: Test Access Management(10/97) [Optional]
  - b. GR-1042 Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Overview: Synchronous Optical Network (SONET) Transport Information Model (12/98) [Optional]
  - c. GR-1042-IMD Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Details: Synchronous Optical Network (SONET) Transport Information Model (12/98) [Optional]
  - d. GR-1110 Broadband Switching System (BSS) Generic Requirements (12/00)
  - e. GR-1209 Generic Requirements for Passive Optical Components (03/01)
  - f. GR-1230 SONET Bi-Directional Line-Switched Ring Equipment Generic Criteria (12/98)
  - g. GR-1250 Generic Requirements for Synchronous Optical Network (SONET) File Transfer (12/99)
  - h. GR-1345 Framework Generic Requirements for Element Manager (EM) Applications for SONET Subnetworks (12/00) [Optional]
  - i. GR-1365 SONET Private Line Service Interface Generic Criteria for End Users (12/94)
  - j. GR-1374 SONET Inter-Carrier Interface Physical Layer Generic Criteria For Carriers (12/94)
  - k. GR-1400 SONET Dual-Fed Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria (01/99)
  - l. GR-199 OTGR Section 12.2: Operations Application Messages - Memory Administration Messages (08/02)
  - m. GR-253 Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria (09/00)
  - n. GR-2837 ATM Virtual Path Ring Functionality in SONET - Generic Criteria (02/98) [Optional]
  - o. GR-2842 ATM Service Access Multiplexer Generic Requirements (11/96) [Optional]

- p. GR-2875 Generic Requirements for Digital Interface Systems (05/96) [Optional]
- q. GR-2891 SONET ATM Virtual Path Digital Cross-Connect Systems - Generic Criteria (12/98) [Optional]
- r. GR-2899 Generic Criteria for SONET Two-Channel (1310/1550-NM) Wavelength Division Multiplexed Systems (09/95)
- s. GR-2900 SONET Asymmetric Multiples Functional Criteria (09/95) [Optional]
- t. GR-2918 DWDM Network Transport Systems with Digital Tributaries for Use in Metropolitan Area Applications: Common Generic Criteria (01/03)
- u. GR-2950 Information Model for SONET Digital Cross-Connect Systems (DCSS) (02/99)
- v. GR-2954 Transport Performance Management Based on the TMN Architecture (12/97) [Optional]
- w. GR-2955 Generic Requirements for Hybrid SONET/ATM Element Management Systems (EMSS) (11/98) [Optional]
- x. GR-2979 Generic Requirements for Optical Add-Drop Multiplexers (OADMs) and Optical Terminal Multiplexers (OTMs) (12/01)
- y. GR-2980 Generic Criteria for ATM Layer Protection Switching Mechanism (12/98) [Optional]
- z. GR-2996 Generic Criteria for SONET Digital Cross-Connect Systems (01/99)
- aa. GR-3000 Generic Requirements for SONET Element Management Systems (EMSs) (11/99) GR-3001 Generic Requirements for SONET Network Management Systems (NMS's) (12/99) [Optional]
- bb. GR-3004 Generic Requirements for the Operations Interface Between Hybrid SONET/ATM Element Management Systems and Network Management Systems (02/99) [Optional]
- cc. GR-3008 OTGR Section 6.9: Network Maintenance: Access and Testing - SONET STS-1 and SUB-STIS-1 TSC/RTU and DTAU Functional Requirements (12/98)
- dd. GR-303 Integrated Digital Loop Carrier System Generic Requirements, Objectives, and Interface (12/00)
- ee. GR-3101 Generic Requirements for Asynchronous Transfer Mode (ATM) Element Management Systems (EMSs) (08/00) [Optional]
- ff. GR-3102 Generic Requirements for Asynchronous Transfer Mode (ATM) Network Management Systems (10/00) [Optional]
- gg. GR-376 Generic Operations Interfaces Using OSI Tools: Network Data Collection (12/98) [Optional]
- hh. GR-436 Digital Network Synchronization Plan (06/94)
- ii. GR-496 SONET Add-Drop Multiplexer (SONET ADM) Generic Criteria (12/98)
- jj. GR-499 Transport Systems Generic Requirements (TSGR): Common Requirements (12/98)
- kk. GR-782 SONET Digital Switch Trunk Interface Criteria (06/00)

- ll. GR-826 OTGR Section 10.2: User Interface Generic Requirements For Supporting Network Element Operations (06/94) [Optional]
  - mm. GR-834 Network Maintenance: Access and Testing Messages (06/00)
  - nn. GR-836 Generic Operations Interfaces Using OSI Tools: Information Model Overview: Transport Configuration and Surveillance For Network Elements [Optional]
2. ANSI Standards:
- a. ANSI T1.105: SONET - Basic Description including Multiplex Structure, Rates and Formats.
  - b. ANSI T1.105.01: SONET - Automatic Protection Switching
  - c. ANSI T1.105.02: SONET - Payload Mappings
  - d. ANSI T1.105.03: SONET - Jitter at Network Interfaces
  - e. ANSI T1.105.03a: SONET - Jitter at Network Interfaces - DS1 Supplement
  - f. ANSI T1.105.03b: SONET - Jitter at Network Interfaces - DS3 Wander Supplement
  - g. ANSI T1.105.04: SONET - Data Communication Channel Protocol and Architectures
  - h. ANSI T1.105.05: SONET - Tandem Connections Maintenance
  - i. ANSI T1.105.06: SONET - Physical Layer Specifications
  - j. ANSI T1.105.07: SONET - Sub-STS-1 Interface Rates and Formats Specification
  - k. ANSI T1.105.09: SONET - Network Element Timing and Synchronization
  - l. ANSI T1.119: SONET - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Communications
  - m. ANSI T1.119.01: SONET: OAM&P Communications Protection Switching Fragment
3. ITU-T Standards:
- a. Physical Interfaces
    - i. G.703 (10/98)
    - ii. G.957 (06/99)
    - iii. G.692 (10/98)
    - iv. K.20 (05/98)
    - v. G.691 (04/00)
  - b. Network Architecture
    - i. G.805 (11/95), (03/00)
    - ii. G.803 (06/97), (03/00)
    - iii. I.322 (02/99)
  - c. Structures & Mappings
    - i. G.704 (10/98)
    - ii. G.707 (10/00) - Amendment 1
    - iii. G.7041 (10/01) GENERIC FRAMING PROCEDURE
    - iv. G.7042 (10/01) LCAS

- v G.708 (10/98)
- vi G.832 (10/98)
- d. Equipment Functional Characteristics
  - i G.664 (06/99)
  - ii G.781 (06/99)
  - iii G.783 (10/00)
  - iv G.958 (01/94)
  - v G.705 (04/00)
  - vi G.806 (04/0)
- e. Laser Safety
  - i G.664 (06/99)
- f. Transmission Protection
  - i G.841 (10/98), (08/02)
  - ii G.842 (04/97)
  - iii G.808.1 (2003)
  - iv M.2102 (03/00)
- g. Equipment Protection
  - i M.3100 Amendment
- h. Equipment Management
  - i G.784 (06/99)
- i. Information Model
  - i G.773 (03/93)
  - ii G.774 (09/92), (11/96), (04/00)
  - iii G.774.01 (11/94), (11/96), (04/00)
  - iv G.774.02 (11/94), (11/96), (04/00)
  - v G.774.03 (11/94), (11/96), (04/00)
  - vi G.774.04 (07/95), (11/96), (04/00)
  - vii G.774.05 (07/95), (11/96), (04/00)
  - viii G.774.06 (04/00)
  - ix G.774.07 (11/96), (04/00)
  - x G.774.08 (04/00)
  - xi G.774.09 (04/00)
  - xii G.774.10 (04/00)
- j. Network Management
  - i G.831 (08/96), (03/97)
  - ii T.50 (09/92)
  - iii G.85x.y (11/96)
- k. Error Performance (network level view)
  - i G.826 (02/99)
  - ii G.827 (02/00)
  - iii G.827.1 (11/00)
  - iv G.828 (02/00)
  - v G.829 (02/00)



- vi M.2101 (02/00)
- vii M.2101.1 (04/97)
- viii M.2102 (02/00)
- ix M.2110 (04/97)
- x M.2120 (04/97), (02/00)
- xi M.2130 (02/00)
- xii M.2140 (02/00)
- I. Error Performance (equipment level view)
  - i G.783 (10/00)
  - ii G.784 (06/99)
- m. Jitter and Wander Performance
  - i G.813 (08/96)
  - ii G.822 (1988)
  - iii G.823 (03/93), (03/00)
  - iv G.824 (03/93), (03/00)
  - v G.825 (03/93), (02/99)
  - vi G.783 (10/00), (04/97), (03/99), (06/98)
- n. Leased Lines
  - i M.13sdh (02/00)
- o. Synchronization (Clocks & Network Architecture)
  - i G.803 (06/97), (02/99)
  - ii G.810 (08/96)
  - iii G.811 (09/97)
  - iv G.812 (06/98)
  - v G.813 (08/96)
- p. Test Signals
  - i O.150
  - ii O.181
- 4. Institute of Electrical and Electronics Engineers, Inc. (IEEE):
  - a. IEEE 802.3, 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY
  - b. IEEE 802.3ae, 10Gbit Ethernet
  - c. 802.17, Resilient Packet Rings (RPR) – In progress
  - d. 802.1ah, Ethernet First Mile – In progress
- 5. Optical Internetworking Forum (OIF):
  - a. User to Network Interface version 1.0, OIF-UNI-01.0
- 6. All new versions, amendments, and modifications to the above documents and standards when commercially available.

#### **C.2.5.2.1.3 Connectivity**

SONETS services shall connect to and interoperate with:

1. Government specified terminations (e.g., SDP-to-SDP, POP-to-POP)

2. All other networks including other Network contractors' networks where industry Standards are used.

#### C.2.5.2.1.4 Technical Capabilities

The following SONETS capabilities are considered mandatory unless marked optional:

1. End-to-End SONETS Delivery. The contractor shall support SONETS connections which may transverse networks in different regions.
2. Gateway functionality shall be provided (SONET to SDH and SDH to SONET conversion) as needed by Agency. [Optional]
3. The following Network Topologies shall be supported:
  - a. The contractor shall support Linear topologies like Point-to-Point
  - b. The contractor shall support Ring topology
  - c. The contractor shall support Mesh topology [Optional]
4. The contractor shall support the following protection methods:
  - a. On the Tributary Side the contractor shall support:
    - i. Automatic Protection Switching (APS) 1:N, where  $N \leq 14$
    - ii. APS 1+1
    - iii. Unprotected
  - b. On the Network Side the contractor shall support:
    - i. Unprotected
    - ii. Mesh Protection
    - iii. Unidirectional Path Switched Ring (UPSR)
    - iv. Bidirectional Line Switched Ring (BLSR)
    - v. Bidirectional Path Switched Ring (BPSR) or equivalent [Optional]
    - vi. 1+1
5. Transmux Capability (interconnects high bandwidth interface at one Agency location to lower bandwidth interface at another Agency location) shall be supported by the contractor:
  - a. DS3/STS1 transmuted to DS1 shall be supported
  - b. OC3 transmuted to DS3/STS1 shall be supported
  - c. OC12 transmuted to OC3/DS3/STS1 shall be supported
  - d. OC48 transmuted to OC12/OC3/DS3/STS1 shall be supported
  - e. [Optional] OC192 transmuted to OC48/OC12/OC3/DS3/STS1 shall be supported
6. The following Concatenation methods shall be included in SONETS:
  - a. Standard Concatenation. SONET specifications in GR-253 include standard concatenation, which allows OC-N signals to be grouped in

multiples of 3 STS-1s and treated as single entities. The following standard concatenated rates shall be supported:

- i STS-3c shall be supported
- ii STS-12c shall be supported
- iii STS-48c shall be supported
- iv [Optional] STS-192c shall be supported
- v STS-768c shall be supported [Optional]

b. Virtual Concatenation. The following standard rates shall be available for Agency procurement: [Optional]

- i. VT-1.5-7v for 10 Mbps Ethernet Connections
- ii. VT-2.0-5v for 10 Mbps Ethernet Connections
- iii. STS-1-2v for 100 Mbps Fast Ethernet Connections
- iv. STS-1-21v for 1 Gbps Ethernet Connections
- v. STS-3c-7v for 1 Gbps Ethernet Connections
- vi. The contractor shall support the following:
  1. High order concatenation – shall support STS-1/3c-Xv SPE, X = 1 up to 256 rates/entities
  2. Low order concatenation – shall support X VTn SPEs (n=1.5, 2, 3, 6) rates/entities

7. SONET Performance: All SONET Services contracted by the Agencies shall comply with the following performance indicators and with the Performance Metrics included in Section C.2.5.2.4.

- a. Jitter -- as specified in GR-253 - Jitter measurement shall be performed over a 60-second interval with band pass filters having frequencies cut off at 10 KHz and 4 KHz, a fall of 20db/decade, and a low-pass cut off frequency of at least 80 KHz. The contractor shall ensure these specifications are met at the SDPs.
- b. Restoration Time -- as specified by GR-253 for Automatic Protection Switching and by GR-1230, Section 6.1.1, re-routing of the traffic shall be performed to restore the SONETS (over redundant path) before the failure is repaired. The contractors shall reconfigure affected services for Rings  $\leq$  1200 KM as follows:
  - i. For Routine Users, the service shall be restored in less than 100 ms, when preemption of extra traffic is required
  - ii. For Critical Users, the service shall be restored in less than 60 ms including detection time (10ms)
  - iii. User-provisionable GR-253-CORE BER Threshold for Signal Failure (SF) shall be set to  $10^{-5}$ .
  - iv. User-provisionable GR-253-CORE BER Threshold for Signal Degradable (SD) shall be set to  $10^{-9}$ .

8. Performance Monitoring. The contractor shall support the Performance Monitoring parameters specified by GR-253. Monitoring of parameters shall be performed for each individual minute and recorded in registers of 15 minutes.

The last eight 15-minute registers shall be archived and made accessible to the Agency. The contractor shall store all measurements for the past 24 hours in a register. The following parameters shall be monitored and measured.

- a. Error Seconds (ES). An Errored Second is any one-second interval containing at least one error. Error Seconds shall be counted as 1-second intervals containing at least 1 error. The contractor shall measure performance based on percent of error seconds, which is calculated as 100 times the ratio of error seconds to total seconds in the available time during a fixed measurement period (24 hours). For all Network Users, % ES shall be less than 0.25% during the measurement period. It is acceptable quality level to observe ES during 1.8 minutes per month.
  - b. Severe Error Seconds (SES). A Severe Error Second is 1-second period with a BER of  $10^{-3}$  or worse for DS-1 and DS-3 signals. Severe Error Seconds (SES) for STS-n signals, is 1-second period that contains 30 percent or greater errored blocks or at least one severely disturbed period. A severely disturbed period occurs when all contiguous blocks are affected by a high bit error density over a period of 1 millisecond. Contractors shall measure performance based on percent of SES, which is calculated as 100 times the ratio of SES to total seconds in available time during a fixed measurement period (24 hours). For all Network Users, %SES shall be less than 0.035% during the measurement period. It is acceptable quality level to observe SES during 15.12 seconds per month
9. Interfaces. The contractor shall support all commercially available optical interfaces and shall comply with ANSI, Telcordia, and ITU standards. Reach and fiber types shall be supported as follows:
- a. Optical Interfaces from OC-1 up to OC-768 shall be supported. OC-768 shall be supported when available. Supported optical interfaces shall include the following reach modes:
    - i. SR-MLM, Short Reach Multi-Longitudinal Mode shall be supported
    - ii. IR1-SLM, Intermediate Reach – Single – Longitudinal Mode shall be supported
    - iii. LR1-SLM, Long Reach – Single – Longitudinal Mode shall be supported
    - iv. VSR4-01 (OC-192 Very Short Reach Interface, 12 fibers 850nm). Compliant to Implementation Agreement, OIF-VSR4-01.0 - Very Short Reach (VSR) OC-192 Interface for Parallel Optics shall be supported [Optional]

- v. VSR4-02 (OC-192 Very Short Reach Interface, 1 fiber 1310nm),  
Note: VSR4-02 has been included as the 4dB link option in VSR4-05 below shall be supported. [Optional]
  - vi. VSR4-03 (OC-192 Very Short Reach Interface, 4 fibers 850nm).  
Compliant to OIF-VSR4-03.0 - Very Short Reach (VSR) OC-192 Four Fiber Interface Based on Parallel Optics shall be supported. [Optional]
  - vii. VSR4-04 (OC-192 Very Short Reach Interface, 1 fiber 850nm).  
Compliant to OIF-VSR4-04.0 - Serial Shortwave Very Short Reach (VSR) OC-192 Interface for Multimode Fiber shall be supported. [Optional]
  - viii. VSR4-05 (OC-192 Very Short Reach Interface, OXC 1310nm).  
Compliant to OIF-VSR4-05.0 - Very Short Reach (VSR) OC-192 Interface Using 1310 Wavelength and 4 and 11 dB Link Budgets shall be supported. [Optional]
  - ix. VSR5-01 (OC-768 Very Short Reach Interface). Compliant to OIF-VSR5-01.0 - Very Short Reach Interface Level 5 (VSR-5): SONET/SDH OC-768 Interface for Very Short Reach (VSR) Applications shall be supported. [Optional]
- b. Electrical interfaces shall be supported from DS1 through STS-1.
10. Next Generation SONET [Optional] shall be supported:
- a. The contractor's network shall support all of the following:
    - i. Generic Framing Procedure, shall include:
      - 1. Frame Mapped Generic Framing Procedure
      - 2. Transparent Generic Framing Procedure
    - ii. Link Adjustment Capacity Scheme (LCAS) shall be supported to provide Virtual Concatenation as defined by ANSI T1.105 and G.707.
    - iii. Virtual Concatenation shall be supported
11. Reserved
12. Data Communications Channel (DCC) – The contractor shall provide the Agency with the ability to establish communication between its edge devices. [Optional]
13. Integrated Control Plane (i.e. ASON based, GMPLS) – The contractor shall support an integrated, intelligent control plane in order to speed up activation service times, provide control to Agencies to the contracted infrastructure and achieve inter- and intra-contractor interoperability when required. [Optional]
14. Reserved.

### C.2.5.2.2 Features for SONETS Services

The following SONETS Services features in Section C.2.5.2.1 are mandatory unless marked optional:

#### C.2.5.2.2.1 SONETS Services Features

ID Number	Name of Feature	Description
1 [Optional]	Bandwidth On Demand (BoD)	The contractor shall provide Agencies with the ability to increase or decrease bandwidth in increments of at least 1 Mbps without interrupting service. The contractor shall indicate available increments. Additional increments of 2Mbps, 50 Mbps, 100 Mbps, and 150 Mbps are optional.
2	Channelization	The contractor shall support SONET interfaces to the CPE to seamlessly interface with the contractor's SONET network for data transport. The following channelized arrangements shall be supported as a minimum: <ol style="list-style-type: none"> <li>1. STS-1 payload with VT1.5, VT2</li> <li>2. STS-1, STS-1 payload, VT1.5, VT2, STS-3c</li> <li>3. VC-11(DS1), VC-12 (E1), VC-3 (DS3, E3, other) [Optional]</li> <li>4. VC-4, VC-3, VC-11, VC-12 [Optional]</li> <li>5. Down to STS-1 (E3, other), [Optional]</li> <li>6. STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4 [Optional]</li> </ol>
3 [Optional]	Dedicated Metro Ring	The contractor shall support the consolidation of Agency's traffic within a highly reliable metro infrastructure. As a minimum, the following features shall be supported: <ol style="list-style-type: none"> <li>1. Node capacity from 3 to 16 nodes</li> <li>2. Sub-50 ms restoration times for single failures when less than 1200km of fiber are involved in the ring or span switch. If this condition is not met, the complete restoration shall take less than 100ms not including detection time.</li> <li>3. Aggregation and transport of bandwidth from DS1 up to 2.5 Gbps</li> <li>4. Protection architecture: UPSR/SNCP, 2FBR BLSR</li> <li>5. Transport to Ethernet traffic in the ranges from 50 Mbps up to 10 Gbps</li> <li>6. Off-ring connection available (to a remote POP or government Agency)</li> <li>7. Transmux functionality</li> <li>8. Optional Backup ring</li> <li>9. Multiplexing function at all nodes</li> </ol>
4 [Optional]	DS1 Rate Synchronization Service	The contractor shall provide the Agency with this feature to allow Agency's Stratum 2 or Stratum 3 clocks at its locations to synchronize to a Stratum 1 clock at the contractor's location. The DS1 to be used for synchronization shall be delivered through the following methods:

ID Number	Name of Feature	Description
		<ol style="list-style-type: none"> <li>External Timing</li> <li>Loop Timing,</li> <li>Line Timing, which terminates on a higher bit rate ADM</li> </ol>
5	Equipment Protection 1:1 - CPE	The contractor shall provide protection to User Network Interfaces at the SDP, where the protection channel is bridged to the failed working channel.
6	Equipment Protection 1+1 - CPE	The contractor shall provide protection to User to Network Interfaces at the SDP, where the protection channel is permanently bridged to the working channel.
7	Equipment protection – Network Side	Two channels facing the network shall be supported for full redundancy and equipment protection at the SDPs.
8	Framing for Electrical Interfaces	<p>The contractor shall support framing formats for the electrical interfaces listed in Section C.2.5.2.3 which shall include the following as a minimum:</p> <ol style="list-style-type: none"> <li>M-frame with M23 Multiplexing format [Optional]</li> <li>M-frame with C-parity</li> <li>Super Frame Format (SF) [Optional]</li> <li>Bipolar Alternate Mark Inversion (AMI) [Optional]</li> <li>Binary, 8 zero substitution line code (B8ZS)</li> <li>Non-ANSI SF [Optional]</li> <li>ANSI Extended Super frame (ESF) (ANSI T1403.1995)</li> <li>Non-ANSI ESF (AT&amp;T PUB 54016) [Optional]</li> </ol>
9 [Optional]	Geographic Diverse protection	The contractor shall support two geographically diverse delivery channels from SDP1 to SDP2.
10 [Optional]	Local and Remote Node Multiplexing	The contractor shall enable the multiplexing of different circuits into a high speed SONET signal. When service is ordered, the configuration of the low speed (tributary) interfaces shall be specified by the contractor. The contractor shall indicate the mixture and number of interfaces allowed for each of the high speed signals available.

### C.2.5.2.3 Interfaces for SONETS Services

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.5.2.3.1, are mandatory unless marked optional:

#### C.2.5.2.3.1 Interfaces for SONETS Services

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/ Protocol Type/Granularity
1	Optical	IEEE 802.3z	1310 nm	1.25Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1.25Gbps	Gigabit Ethernet
3	Optical	IEEE 802.3	1310 nm	125 Mbps	Fast Ethernet
4	Optical	GR-253, ITU-T G.707	1310 nm	155 Mbps	SONET or SDH

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/ Protocol Type/Granularity
5	Optical	GR-253, ITU- G.707	1310 nm	155 Mbps	SONET or SDH Concatenated
6	Optical	GR-253, ITU- G.707	1310 nm	622 Mbps	SONET or SDH
7	Optical	GR-253, ITU- G.707	1310 nm	622 Mbps	SONET or SDH Concatenated
8	Optical	GR-253, ITU-T G.707	1310 nm	622 Mbps	SONET Channelized
9	Optical	GR-253	1310 nm	155 Mbps	ATM over SONET
10	Optical	GR-253	1310 nm	622 Mbps	ATM over SONET
11	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gpbs	SONET or SDH
12	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gpbs	SONET or SDH Concatenated
13 [Optional]	Optical	GR-253, ITU-T G.707	1310 nm	10Gpbs	SONET or SDH
14	Electrical	ANSI T1	N/A	1.544 Kbps	DS1
15	Electrical	ANSI T1	N/A	45 Mbps	DS3
16	Electrical	ANSI T1	N/A		STS-1
17	Electrical	ANSI T1	N/A	DS1	DS0, Nx64 Kbps
18	Electrical	ANSI T1	N/A	DS3	DS3, Nx1.544Mbps, DS1
19	Electrical	ANSI T1	N/A	E1	Nx64 Kbps
20	Electrical	ANSI T1	N/A	E3	E1, Nx64 Kbps, DS0
21 (Optional)	Optical	GR-253, ANSI T1.105	1300 nm	OC-1	SONET STS-1 payload, VT1.5, VT2
22	Optical	GR-253, ANSI T1.105	1300 nm	OC-3 155 Mbps	SONET STS-1, STS-1 payload, VT1.5, VT2
23	Optical	GR-253, ANSI T1.105	1300 nm	OC-3c 155 Mbps	SONET STS-3c
24	Optical	G.707	1300 nm	STM-1 155 Mbps	SDH VC-11(DS1), VC-12 (E1), VC-3 (DS3, E3, other)
25	Optical	G.707	1300 nm	STM-1c 155 Mbps	SDH VC-4, VC-3, VC-11, VC-12
26	Optical	GR-253, ANSI T1.105	1300 nm	OC-12 622 Mbps	SONET Down to VT1.5 (DS1), VT2 (E1), STS-1 (DS3, E3, other), STS-3c



UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/ Protocol Type/Granularity
27	Optical	GR-253, ANSI T1.105	1300 nm	OC-12c 622 Mbps	SONET STS-12c
28	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
29	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c
30 (Optional)	Optical	OIF- VSR4-01.0	850 nm	OC-192	VSR4-01 OC-192 (12 fibers)
31 (Optional)	Optical	OIF-VSR4-03.0	1310 nm	OC-192	VSR4-02 OC-192 (1 fiber)
32 (Optional)	Optical	OIF-VSR4-03.0	850 nm	OC-192	VSR4-03 OC-192 (4 fibers)
33 (Optional)	Optical	OIF-VSR4-04.0	850 nm	OC-192	VSR4-04 OC-192 (1 fiber)
34 (Optional)	Optical	OIF-VSR4-05.0	1310 nm	OC-192	VSR4-05 OC-192
35 (Optional)	Optical	OIF-VSR5-01	850 nm	OC-768	VSR5-01 OC-768
36	Electrical	GR-253, ANSI T1.105	850 nm	STS-1/EC-1 51.84 Mbps	SONET/STS-1, VT1.5 mapping
37 (Optional)	Optical	GR-253	1550 nm	2.5 Gbps	SONET or SDH
38 (Optional)	Optical	GR-253	1550 nm	10 Gbps	SONET or SDH

#### C.2.5.2.4 Performance Metrics for SONETS Services

The contractor shall support In-Service Monitoring (ISM) at the SONET Layer and shall not rely on performance observed and measured at higher layers of the network.

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for SONETS Services in Section C.2.5.2.4.1 are mandatory unless marked optional:

##### C.2.5.2.4.1 SONETS Performance Metrics

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(SONETS) (SDP-to-SDP)	Routine	99.9%	≥ 99.9%	In Service Monitoring See Note 1
	Critical (Optional)	99.999%	≥ 99.999%	

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	
Bit Error Rate (BER)	Routine	10 <sup>-12</sup>	≤ 10 <sup>-12</sup>	Out-Of-Service Monitoring See Note 3

Notes:

- SONETS shall be measured in-service and on an end-to-end basis. COT(HR) shall be calculated based on ES and/or SES as defined by GR-253, G.826 through G.829 and shall be expressed in Hours. Availability is computed by the standard formula:

$$Av(SONETS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

- Refer to Section C.3.3.1.2.4 for definitions and how to measure.
- Bit Error Rate (BER) -- this KPI shall be measured out-of-service (OOS) at service turn-up or when requested by the subscribing Agency (i.e. after a failure). Both directions of the SONETS Connection shall be tested. The duration of the BER test shall be determined using criteria included in recommendations such as ITU-T M.2100 and service acceptance testing criteria as included in Section E.2.

**C.2.5.3 Dark Fiber Services (DFS)**

Network service providers have deployed substantial infrastructures of interconnecting fiber cable and these are commonly available for use by Agencies. The simplest Dark Fiber Service is a point-to-point connection between two locations. A more elaborate configuration enables Agencies to interconnect any number of selected locations. A Dark Fiber is an optical fiber through which no light is transmitted. A fiber cable typically contains many optical fibers, which are either “lit” to carry a signal or “unlit” to be used at a future date.

C.2.5.3.1 Service Description

**C.2.5.3.1.1 Functional Definition**

Agencies will acquire dark fiber and have the option of either providing their own opto-electronics equipment or leasing opto-electronics equipment from the contractor. If Agencies choose to provide their own opto-electronics equipment, Dark Fiber Services provides them with the flexibility of not only designing their optical networks to meet their unique mission requirements but also of owning and managing them so that network infrastructure can be readily modified as needed. If Agencies choose to acquire opto-electronics equipment from the contractor, Dark Fiber Services provides them with the flexibility of contracting turnkey services from the contractor.

DFS is acquired as a facility which will allow the Agency to the unconditional right to use of the fiber route, this means capacity such as a fiber pair in a fiber-optic cable, or the entire fiber-optic cable.

**C.2.5.3.1.2 Standards**

Dark Fiber Services shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. Electronic Industry Alliance/Telecommunications Industry Association (EIA/TIA)
  - a. EIA/TIA-559, Single Mode Fiber Optic System Transmission Design
  - b. Optical Fiber System Test Procedures (OFSTPs) including:
    - i. OFSTP-2, Effective Transmitter Output Power Coupled into Single Mode Fiber Optic Cable
    - ii. OFSTP-3, Fiber Optic Terminal Receiver Sensitivity and Maximum Receiver Input
    - iii. OFSTP-7, Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant
    - iv. OFSTP-14, Measurement of Optical Power Loss of Installed Multi-Mode Fiber Cable Plant
    - v. OFSTP-10, Measurement of Dispersion Power Penalty in Single Mode Systems
    - vi. OFSTP-11, Measurement of Single Reflection Power Penalty for Fiber Optic Terminal Equipment
2. Telcordia Standards
  - a. GR-20-CORE, Generic Requirements for Optical Fiber and Optical Fiber Cable
  - b. GR-63-CORE, Network Equipment-Building System (NEBS), Generic Equipment Requirements
  - c. GR-253-CORE, Synchronous Optical Network (SONET) Transport Systems: Common Criteria Physical Layer
  - d. GR-326-CORE, Generic Requirements for Single Mode Connectors and Jumper Assemblies

3. American National Standards Institute (ANSI)
  - a. ANSI Z136.2-1998, American National Standard for the Safe Use of Optical Fiber Communications Systems Utilizing Laser Diode and LED Sources
4. International Electrotechnical Commission (IEC)
  - a. IEC 60825-1, Edition 1.2 2001-08 Safety of Laser Products, Part 1: Equipment Classification, Requirements and User's Guide, Consolidated Edition – International Restrictions
  - b. IEC 60825-2, Safety of Laser Products, Part 2: Safety of Optical Fiber Communications Systems (OFCS) – International Restrictions.
5. Code of Federal Regulations (CFR)
  - a. 21 CFR 1040, Performance Standard for Laser Products
6. International Telecommunications Union (ITU-T)
  - a. ITU-T G.655 (10/2000)
  - b. ITU-T G.652 (10/2000)
  - c. ITU-T G.694.1
  - d. ITU-T K.25 (02/2000)
  - e. ITU-T L.35 (10/1998)
7. Regulations and Permits – The contractor shall be responsible for all permits, easements, and rights of way, to include Host Nation agreements/approvals. The contractor shall be responsible for complying with local Government regulations. If obstacles are found during the process, which will affect Agency's schedule negatively, the contractor shall coordinate solutions with the Government.
8. All new versions, amendments, and modifications to the above documents and standards when commercially available.

#### **C.2.5.3.1.3 Connectivity**

Dark Fiber Services shall connect to and interoperate with:

1. The Internet Service Provider (ISP) chosen by the Agency. When connecting their locations to (an) ISP POP(s), Agencies are responsible for providing required terminating equipment at each end.
2. Inter-Agency or Intra-Agency LANs within the same vicinity. This service shall enable an Agency to interconnect via Inter-Agency or Intra-Agency LAN to selected locations situated within the same metro area (i.e., city). Examples of supported configurations are outlined in Section C.2.5.3.1.4 , paragraph 2.
3. The contractor's Long Haul or Metro networks. This service shall enable an Agency to connect its locations(s) to the nearest contractor's wire center, LEC wire center, Hut, IXC POP, or CLEC collocation facility as applicable.

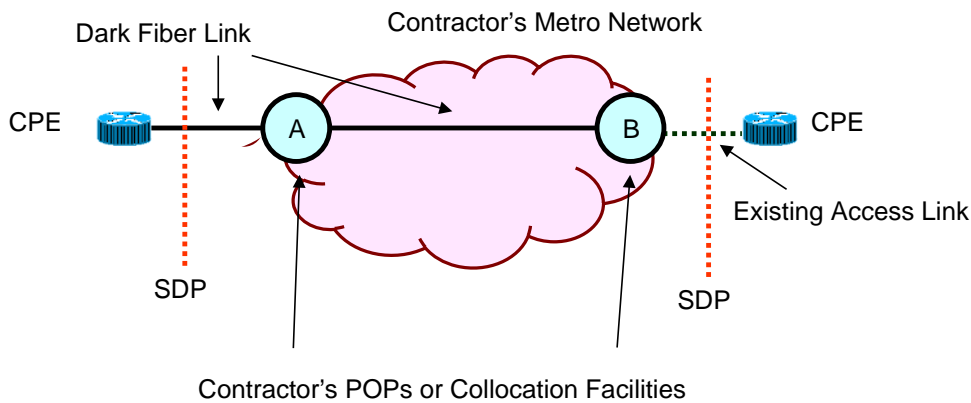
4. Redundant paths to support Agency's transport infrastructure, thereby enhancing service reliability.
5. The contractor shall terminate fiber(s) in the existing Fiber Distribution Panel (FDP) or the FDP specified by the Agency using connectors specified by industry's standards for:
  - a. Multi-tenant buildings
  - b. Single tenant buildings

#### **C.2.5.3.1.4 Technical Capabilities**

The following Dark Fiber Services capabilities are mandatory unless marked optional:

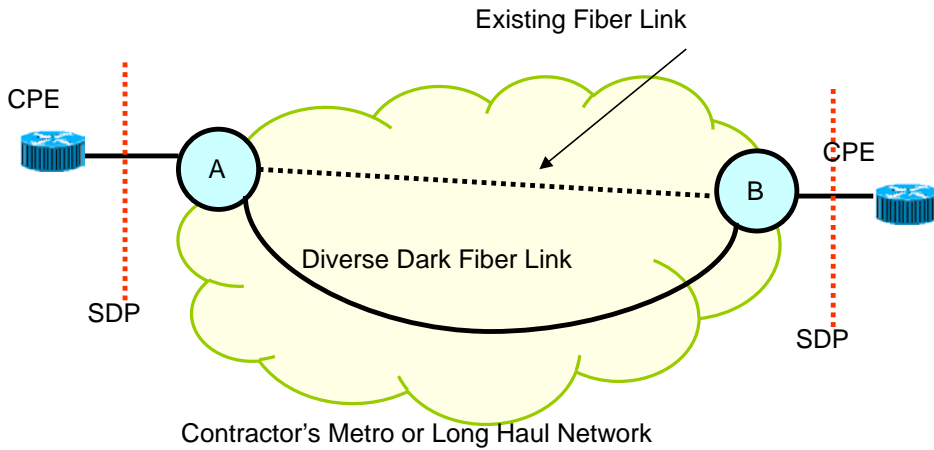
1. Facility Documentation. The contractor shall document its DFS facilities as follows:
  - a. [Optional] Non-domestic. The contractor shall provide and maintain a list of all the Countries/Jurisdictions where the contractor's dark fiber is available.
  - b. CONUS
    - i. Inter-city connectivity. The contractor shall specify the information outlined as follows, and shall update such information as the network is modified:
      1. Number of Inter-city route miles available in North America and listing of interconnected cities shall be included.
      2. Availability of regeneration locations and hut spacing shall be listed.
      3. Should amplification locations be available, type of fiber deployed and spacing between locations shall be included.
    - ii. Intra-city connectivity. The contractor shall specify the information outlined as follows, and shall update such information as the network is modified:
      1. The contractor shall list the available metro networks
      2. The contractor shall include the available connection options.
      3. Reserved
      4. List of Collocation facilities provided shall be provided as part of "on-net" facilities. If collocation facilities are not provided as part of "on-net" facilities, collocation facilities contracted with third parties shall be specified.
  - c. OCONUS
    - i. Inter-city connectivity. The contractor shall specify the information outlined as follows, and shall update such information as the network is modified:

1. Number of Intercity route miles available in OCONUS shall be included.
  2. Availability of regeneration locations and hut spacing shall be listed.
  3. Should amplification locations be available, type of fiber deployed and spacing between locations shall be included.
- ii. Intra-city connectivity. The contractor shall specify the information outlined as follows, and shall update such information as the network is modified:
1. The contractor shall list all available metro networks.
  2. Reserved
2. Configuration Options. The contractor shall support the network topologies outlined as follows.
- a. Point-to-point. This configuration connects any two points in the contractor's network. As an example, Figure C.2.5.3.1.4-1 depicts two Agency locations in a metro area connected by a dark fiber link from POP to POP.



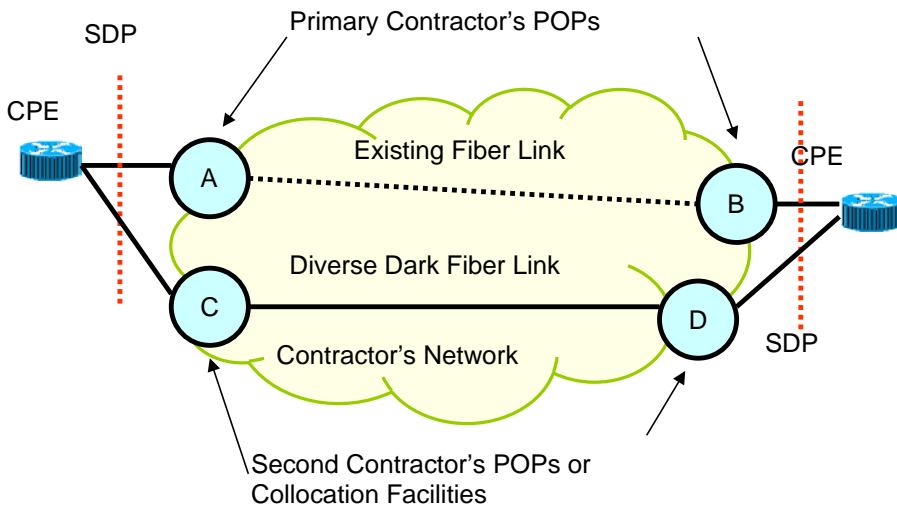
**Figure C.2.5.3.1.4-1 Point-to-point Dark Fiber Connection**

- b. Route Diversity Ring/Single Drops. This configuration is possible when the terminating equipment provides equipment and/or line protection schemes. As an example, Figure C.2.5.3.1.4-2 shows that two diverse paths are available on the network to prevent service interruptions if either fiber path is damaged.



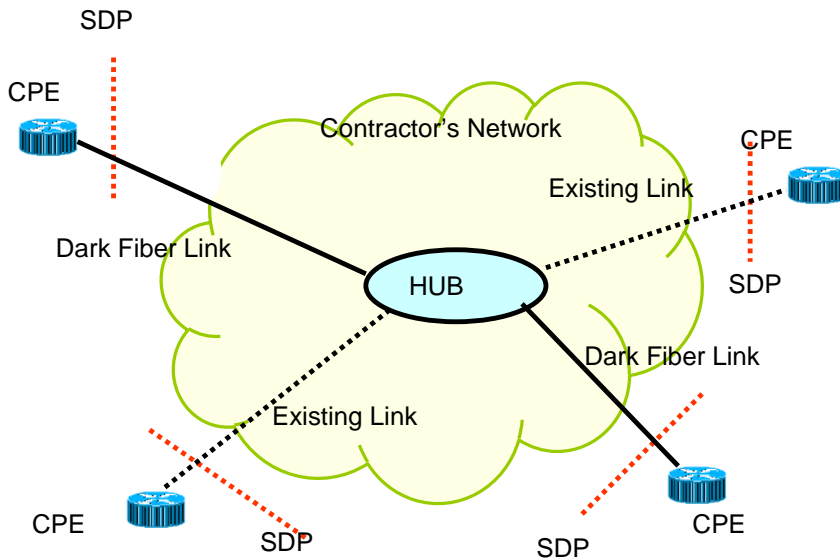
**Figure C.2.5.3.1.4-2 Route Diverse Dark Fiber Ring Connection with Single Drops**

c. Route Diversity Ring/Dual Drops. [Optional] This configuration is possible when two diverse paths are available end-to-end to prevent service interruptions caused by a failure in either in the contractor's network or at the drop's path. As an example, Figure C.2.5.3.1.4-3 shows that an Agency has built an alternate route for protection (path C-D) using a second contractor's POPs or collocation facilities where the Agency has placed its optronics.



**Figure C.2.5.3.1.4-3 Route Diverse Dark Fiber Ring Connection with Dual Drops**

- d. Star Configuration. [Optional] This configuration allows an Agency to have a single location that functions as a hub that provides connectivity to other Agency locations. As an example, Figure C.2.5.3.1.4-4 depicts a point-to-point configuration.



**Figure C.2.5.3.1.4-4 Dark Fiber Connections using Star configuration**

- e. Hybrid Configuration. The preceding four configurations can be combined to yield a custom-tailored solution.
3. Fiber Service Delivery Point (FSDP). The contractor shall support the SDP at either the fiber patch panel where the fibers terminate at a Government location or the collocation facility where the Agency has installed its optronics as required by the Agency. The contractor shall meet the following conditions when delivering DFS to an Agency:
- Optical Fiber. The fiber shall meet the standards specified in Section C.2.5.3.1.2.
  - Fiber Count. The contractor shall provide the number of fiber strands to be delivered at the FSDP as specified by the Agency.
  - Ducting. The contractor shall provide the number of ducts between connecting locations and the number of fiber strands running in each duct as specified by the Agency.
  - Future Growth. The contractor shall always include an additional duct running in parallel to the working duct(s) to provide room for future growth.
4. Channel Count.



- a. Deployed fibers shall be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1
  - b. Deployed fibers shall be capable of operating in the "C", and "L" bands. Support for the "S" band will also be required when commercially available.
5. Gateways. The contractor shall provide the ability to add and drop traffic via gateway locations (nodes A, B, C, and D in Figure C.2.5.3.1.4-1 through Figure C.2.5.3.1.4-3 are examples of gateways). The following requirements shall be fulfilled by the contractors and updates on improvements or expansions shall be provided throughout the life of the contract.
- a. Gateway locations shall be equipped with external back up generators or UPS systems.
  - b. If UPS systems are provided, they shall operate for at least 8 hours without interruption.
  - c. Lock cabinet spaces shall be provided.
  - d. 24x7 access to the gateway locations shall be provided.
  - e. Gateway locations shall be equipped with surveillance and highly secured systems.
  - f. The contractor shall indicate if gateway expansion is possible.
  - g. The contractor shall indicate if gateway locations are monitored remotely.
  - h. Environmental monitoring shall be supported
6. Amplification. Fiber available to Agencies shall work with the following types of In-Line Amplifier:
- a. Erbium-doped Fiber Amplifiers (EDFA).
  - b. Raman Amplifiers.
  - c. EDFA/Raman hybrid Amplifiers.
  - d. Semiconductor Optical Amplifiers (SOA).
7. Fiber Deployed. The contractor shall indicate which type of fiber is deployed, if a mixed of fiber types has been deployed, and where fiber has been deployed.
- a. The contractor shall make available single mode and multimode fiber.
  - b. The contractor shall indicate which of the fiber types have been deployed and where:
    - i. Non-zero dispersion shifted (NZDS) fiber to allow DWDM transmission
    - ii. Corning ELEAF
    - iii. Lucent True-Wave
    - iv. Lucent True-Wave RS
    - v. Lucent All-Wave
    - vi. SMF-28, limited to link segments below 60 km.

- 8. Required Optical Characteristics are identified in Section C.2.5.3.4.1.
- 9. Network Services Verification Criteria. The contractor shall comply with the following verification requirements.
  - a. Verification Testing shall be performed as follows:
    - i. On Single Mode Fibers, end-to-end attenuation measurements shall be tested in both directions of transmission at the 1310nm and 1550nm wavelengths using an industry-accepted laser source and power meter.
    - ii. On Multi Mode Fibers, end-to-end attenuation measurements shall be tested in both directions of transmission at the 850nm and 1300 nm wavelengths.
    - iii. Loss measurements shall be taken from both ends at applicable wavelengths as in i) and ii) and in compliance with OFSTP-7 and OFSTP-14 as applicable or EIA/TIA-568 B
    - iv. OTDR measurements shall be performed for each fiber for length, transmission anomalies, and end-to-end attenuation.
    - v. A written report shall be issued and delivered to the Government, for each cable and OTDR traces and other measurements shall be included for each fiber.
- 10. Service Components. DFS service components shall include the following.
  - a. Trunks. Trunks are main fiber cables that may carry hundreds of fiber strands which may be shared and owned by a variety of contractors, Government Agencies, universities, etc.
  - b. Laterals. Laterals are fiber cables from the Agency's premises to the nearest splice point on the cable trunk. They shall be funded by the Agency and their length may vary from a few meters to several kilometers.
    - i. The contractor shall indicate the minimum and maximum size of the lateral in fiber strands.
  - c. Building Entrances. Facilities within the Agency's premises for the termination of fibers, i.e., fiber panel terminations.

**C.2.5.3.2 Features**

The following Dark Fiber Services features in Section C.2.5.3.2.1 are mandatory unless marked optional:

**C.2.5.3.2.1 Dark Fiber Services (DFS) Features**

ID Number	Name of Feature	Description
1 (Optional)	Colocation Service	The contractor shall provide the ability to add/drop traffic (gateways) and to regenerate and amplify traffic where

ID Number	Name of Feature	Description
		needed.
2	Duct	The contractor shall support the number of ducts (conduits) as specified by the Agency that shall be included in the service.
3 (Optional)	Dark Fiber Local Loop	The contractor shall provide Dark Fiber connection between the Agency's location and the contractor's wire center or outside plant (hut or regeneration location).
4	Diverse Route Single Drop	The contractor shall ensure that two diverse paths are available on the network to prevent service interruptions if a fiber on either of two paths is damaged. A Single Add/drop location/network element shall be used in this arrangement with automatic protection switching capabilities
5	Diverse Route Dual Drop	The contractor shall provide two diverse paths end-to-end to prevent service interruptions caused by a failure either in the contractor's network or at the drop's path. Figure C.2.5.3.1.4-3 illustrates this concept. A second contractor shall provide the diverse route should the Agency requires full diversity for protection unless the working link provider is able to do so.
6	Intercity Connectivity	The contractor shall support a dark fiber connection between Agency's locations in metro areas in the Continental US as well as outside the Continental US.
7	Multiple Duct	The contractor shall be able to upgrade to multiple ducts (conduits).
8 (Optional)	Off-net laterals	The contractor shall provide fiber cables from the Agency's premises to the nearest splice point on the cable trunk. They shall be funded by the Agency and their length may vary from a few meters to several kilometers.

### C.2.5.3.3 Interface

The interfaces for this service are the fiber terminations at the FSDP. The contractor shall identify the fiber connectors that are supported.

### C.2.5.3.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Dark Fiber Services (DFS) in Section C.2.5.3.4.1 are mandatory unless marked optional:

### C.2.5.3.4.1 Dark Fiber Services (DFS) Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Attenuation Coefficient SMF (1550 nm)	Routine	0.25 dB/km	≤ 0.25 dB/ km at all times	See Note 1
Attenuation Coefficient SMF (1310 nm)	Routine	0.35 dB/km	≤ 0.35 dB/ km at all times	
Attenuation Coefficient MMF 850 nm (50/125 μm)	Routine	2.35 dB/km	≤ 2.35 dB/ km at all times	
Attenuation Coefficient MMF 1300 nm (50/125 μm)	Routine	0.35 dB/km	≤ 0.35 dB/ km at all times	
Polarization Mode Dispersion (PMD) at 1550 nm (Inter-City Networks)	Routine	0.1 ps/km <sup>1/2</sup>	≤ 0.1 ps/km <sup>1/2</sup> at all times	See Note 2
Polarization Mode Dispersion (PMD) (Intra-City Networks)	Routine	0.3 ps/km <sup>1/2</sup>	< 0.3 ps/km <sup>1/2</sup> at all times	
Chromatic Dispersion at 1550nm	Routine	2.0 ps/km nm	< 2.0 ps/ km nm at all times	See Note 3
Reflectance Events (all events)	Routine	Less than 40 dB	≤ 40 dB at all times	See Note 4
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	
<b>Connectors</b>				
Return Loss	Routine	Less than 50 dB	≤ 50 dB at all times	See Note 6
Insertion Loss	Routine	Less than 0.5 dB	≤ 0.5 dB at all times	See Note 7

Notes:

1. Attenuation coefficient is the attenuation per unit length with a maximum value at one or more wavelengths. In this case, wavelengths are from 1310 and 1550nm. The method used to test the attenuation coefficient of single-mode optical fiber is based on bidirectional backscattering measurements. For campus applications, MMF may be used and the attenuation coefficient per unit length is included for 850nm and 1300nm. The values listed in the Section C.2.5.3.4.1 reflect fiber only. Additional allowances will be made for splices and connectors.
2. Polarization Mode Dispersion (PMD) is the term that describes the relationship between polarization and group delay. PMD can limit the highest bit rate that is achievable in a fiber optic system. The following are the most popular methods of measuring PMD: Fixed Analyzer (also called wavelength scanning), Interferometry, Pointcare arc (also called SOP), Modulation phase shift, Pulse delay, and Baseband Curve fit. The major differences in testing setups among these methods are the type of light source, means of defining spectral width, and means of tuning the wavelength. Measurement data is collected while sweeping or stepping the wavelength of the source (or receiver, depending on the method used).
3. Chromatic dispersion measurements characterize how the velocity of propagation in fiber or components changes with wavelength. This measurement is obtained by analyzing the group delay through the fiber as a function of wavelength. A wavelength tunable optical source is intensity modulated and the phase of the detected modulation signal is compared to that of the transmitted modulation. The wavelength of the tunable source is then incremented and the phase comparison is made again. By calculating how the difference between the two measurements, the group delay of the fiber is measured.
4. Reflection measurements are done using an optical time-domain reflectometer (OTDR). The OTDR injects a pulsed signal into the optical fiber and a small amount of the injected signal is reflected back (Rayleigh Backscattering). By measuring the amount of backscattered signal in relation to time, signal loss in relation to fiber optic cable distance is determined.
5. See Section C.3.3.1.2.4 for definition and how to measure.
6. Return Loss – The most widely used method for return loss measurement is Optical Continuous Wave Reflectometry (OCWR). In this method, a continuous wavelength of light energy is passed through the connector, under test. The returned power is then measured and the return loss calculated. Using only a calibrated light source, coupler and an optical power meter, return loss measurements using the OCWR method can be accomplished with accuracy. OCWR test procedures are described in detail in FOTP-1071.
7. Insertion Loss - Insertion loss for a connector or splice is the difference in power that is seen by the insertion of the device into the system. This parameter is measured using an Optical Power Meter and a piece of fiber. Take a length of

fiber and measure the optical power through it, then cut the fiber in half, terminate the fibers and connect them, and re-measure the power. The difference between the first reading (P1) and the second (P2) is the insertion loss-the loss of optical power contributed by inserting the connector into the line - measured as follows:

$$IL \text{ (dB)} = 10 \log (P2 / P1)$$

#### **C.2.5.4 Optical Wavelength Services (OWS)**

Government Agencies require dedicated broadband, framing-independent transport networks to interconnect their offices in different regions of the United States and internationally. In offering OWS, the contractor always provides the optronics equipment and fiber connectivity that comprise the transport network. Management of the network, however, may be performed by either the providing contractor or the Government Agency. In the latter case, Agencies will manage their dedicated networks via a web portal or a remote User Interface (UI).

The two principal means of providing OWS use the following technologies:

- a. Wavelength Division Multiplexing (WDM)
- b. Automatic Switched Transport Network (ASTN)

Optical Wavelength Services (OWS) delivered over WDM provide high bandwidth solution without the capital and expense of owning and operating network infrastructure. OWS delivered over ASTN, also provides this benefit and will transport digital payloads of different bit rates and frame formats with operational efficiencies not expected from current WDM transport solutions alone. The ASTN is an emerging technology approach that will provide improved support for end-to-end provisioning, re-routing and restoration; new transport services such as bandwidth on demand, rapid service restoration for disaster recovery, and switched connections within a private network and support for a wide range of client signals such as SDH/SONET, IP, Ethernet, ATM, and Frame Relay. OWS employment of the WDM and ASTN technologies is specified in paragraphs C.2.5.4.1 and C.2.5.4.2.

##### **C.2.5.4.1 OWS over Wavelength Division Multiplexing (WDM)**

OWS is provided over Wavelength Division Multiplexing (WDM) equipment where several wavelengths, or lambdas, are multiplexed into a composite signal that is transported over a single fiber. The composite signal is then de-multiplexed at the receiver end and each wavelength is recovered.

###### **C.2.5.4.1.1 Service Description**

###### **C.2.5.4.1.1.1 Functional Definition**

Basic OWS is a point-to-point, bi-directional, single link service delivered over the WDM (It may also be delivered over the ASTN – see paragraph 2.5.4.2.1.1).

**C.2.5.4.1.1.2 Standards**

Optical Wavelength Services (OWS) over WDM shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed as follows:

1. International Telecommunications Union (ITU) Standards defining frequencies grid and physical layer parameters for DWDM are G.692 and G.694
2. ITU Standards defining frequencies grid for CWDM are G.694.2. Standards for physical layer parameters are still under development.
3. ITU Standards defining OTN architecture, interface formats, and physical layer interfaces are G.872, G.709, and G.959.1 respectively. [Optional]
4. Applicable ITU Standards defining submarine transmission functional requirements are G.971, G.972, G.973, G.974, G.975, G.976 and G.977.
5. Telcordia standards for metro and long haul protection are GR-253, GR-1400, and GR-1230.
6. Telcordia standard for reliability assurance is GR-418
7. Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009.
8. VSR4-01 (OC-192 Very Short Reach Interface, 12 fibers 850nm)  
OIF-VSR4-01.0 - Very Short Reach (VSR) OC-192 Interface for Parallel Optics. [Optional]
9. VSR4-02 (OC-192 Very Short Reach Interface, 1 fiber 1310nm)  
Note: VSR4-02 has been included as the 4dB link option in VSR4-05 below [Optional]
10. VSR4-03.1 (OC-192 Very Short Reach Interface, 4 fibers 850nm)  
OIF-VSR4-03.0 - Very Short Reach (VSR) OC-192 Four Fiber Interface Based on Parallel Optics. [Optional]
11. VSR4-04 (OC-192 Very Short Reach Interface, 1 fiber 850nm)  
OIF-VSR4-04.0 - Serial Shortwave Very Short Reach (VSR) OC-192 Interface for Multimode Fiber. [Optional]
12. VSR4-05 (OC-192 Very Short Reach Interface, OXC 1310nm)  
OIF-VSR4-05.0 - Very Short Reach (VSR) OC-192 Interface Using 1310 Wavelength and 4 and 11 dB Link Budgets. [Optional]
13. VSR5-01 (OC-768 Very Short Reach Interface) OIF-VSR5-01.0 - Very Short Reach Interface Level 5 (VSR-5): SONET/SDH OC-768 Interface for Very Short Reach (VSR) Applications. [Optional]

14. All new versions, amendments, and modifications to the above documents and standards when commercially available.

**C.2.5.4.1.1.3 Connectivity**

OWS shall be delivered at the Service Delivery Point (SDP) via User to Network Interfaces (UNIs) as specified in Section C.2.5.4.1.3.1.

Point-to-point, bi-directional, duplex services shall be connected from the SDP to the Optical Transport Network via a fiber pair.

The wavelengths ordered by the Agencies shall connect to and interoperate with:

- a. Contractor's metro and long networks
- b. Agency's Intranet
- c. Internet
- d. Other Agency networks.

**C.2.5.4.1.1.4 Technical Capabilities**

The following Optical Wavelength Services (OWS) capabilities are mandatory unless marked optional:

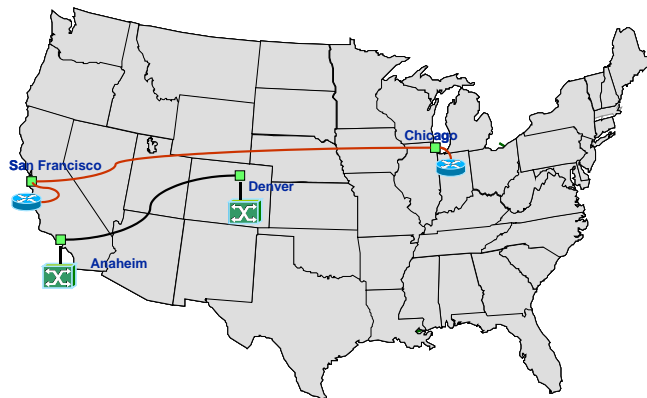
1. End to End Wavelength Termination - The contractor shall support wavelengths end-to-end regardless of where its terminations are located as follows:
  - a. [Optional] Transoceanic Wavelengths may be part of an end-to-end service or stand-alone connection through the ocean as illustrated in Figure C.2.5.4.1.1.4-1. The contractor shall drop and pick up traffic from and to cities in different continents, as required by an Agency.



**Figure C.2.5.4.1.1.4-1. OCONUS and Non-domestic Wavelength Services**



- i. [Optional] Backhaul services shall be available where necessary.
- ii. The basic wavelength service shall be a single point-to-point; bi-directional wavelength connecting two Agency sites located in different countries.
- b. CONUS Wavelengths. The contractor shall support wavelengths over the long-haul network. This is applicable for inter-city connectivity within the United States as illustrated in Figure C.2.5.4.1.1.4-2.
  - i. The basic service shall be a single point-to-point, bi-directional wavelength connecting two Agency sites located in different states.



**Figure C.2.5.4.1.1.4-2 – CONUS Wavelength Service**

- c. Metro Wavelength Services. The contractor shall support the provisioning of wavelengths over its metro networks.
  - i. Single point-to-point, bi-directional wavelengths connecting two Agency sites in the same city shall be supported.
- 2. Reserved
- 3. Reserved
- 4. Transmission Rates. Wavelengths shall be supported at 2.5 Gbps and 10 Gbps. Following the implementation of Networkx, the contractor may support optional rates beyond than 10 Gbps, e.g., 40 Gbps and greater.
- 5. Clock Transparency. The contractor’s networks shall support the following levels of clock transparency:
  - a. Asynchronous transport, where the contractor’s network shall not apply clocking to Agency’s traffic.
  - b. The contractor’s network shall provide Synchronous Status Messaging (SSM) byte transparency

6. Protocol Transparency - Metro. The contractor shall support Metro wavelengths that are rate and protocol independent.
7. Protocol Transparency – CONUS and Non-Domestic. The contractor shall support CONUS and Non-Domestic Wavelengths that are rate and protocol independent. [Optional]
8. Byte Transparency. The support to framed wavelengths shall include byte transparency where the overhead bytes are passed through without being overwritten (i.e. non-intrusive Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) processing of the signals).
  - a. Transparency of Transport Overhead (TOH) bytes shall be provided, with the exception of A1 and A2 bytes. A1 and A2 are framing bytes which monitor the framing integrity of the incoming Synchronous Transport Signal Level-N (STS-N, where N=1, 3, 12, 48, 192) and Optical Carrier Level-N (OC-N, where N=1, 3, 12, 48, 192) signals. The framing bytes can be terminated and the wavelength is then transparent.
  - b. If the framed wavelengths supported are not fully transparent, the contractor shall indicate the level of transparency offered for wavelengths at 2.5 Gbps and 10 Gbps.
  - c. Fully transparent wavelengths shall be supported at 10 Gbps. This applies to Non-domestic, CONUS, and metro wavelengths.
9. Concatenation. For framed wavelengths, the contractor shall support standard and virtual concatenation.
10. Channelization. For framed wavelengths, the contractor shall support channelized User-to-Network Interfaces (UNIs) as per Section C.2.5.4.1.3
11. Wavelength Delivery. Hand-off at the SDP shall be accomplished using two fibers over two ports when delivering bidirectional wavelength services, with one fiber for each direction. Patch panel and fiber terminations shall be based on Agency needs.
12. Access Methods – The contractor shall provide access methods to the ordered wavelength service for an end-to-end offering.
  - a. If the contractor is not able to provide access on his network, it shall indicate what alternatives exist to enable the service end-to-end.
  - b. Each end of the wavelength shall be delivered using different access methods if required by the Agency.

- c. When Agency access is provided via the backbone of the Long Haul (LH) DWDM systems and is not collocated, the contractor shall specify the appropriate reach of the optical interface to be used. If the distance is too long for interfaces such as FICON, Fiber Channel, etc., the mediation devices or gateways needed shall be specified in order to compensate for distance limitations.

13. Customer Premises Equipment (CPE) Support – The contractor shall provide multi-vendor interoperability support to the CPE owned or leased by the Agency by completing connectivity using the appropriate UNIs in the following cases:

- a. Should the CPE and the metro WDM system be collocated at the Agency’s office, connectivity between them shall be established using Short Reach (SR) interfaces (1310 nm) or Very Short Reach (VSR).
- b. Should the CPE and the metro WDM systems be not collocated; the metro WDM shall be located in a telehouse or collocation hotel. In this case, the contractor shall interface with the CPE using the appropriate optical interface that shall reach the distance between the Agency’s office and the collocation site.
- c. Reserved
- d. The wavelength service shall be able to support different kinds of traffic depending on the type of CPE (i.e., Fiber Connectivity (FICON), Enterprise System Connection (ESCON), and Fiber Channel for a Storage Area Network (SAN)).

14. Efficient Transport. The contractor shall ensure that a single wavelength is capable of transporting different types of traffic without the need to use a separate physical wavelength to run ATM, Frame Relay (FR), IP, Ethernet, etc.

**C.2.5.4.1.2 Features for OWS over WDM**

The following Optical Wavelength Services (OWS) over WDM features in Section C.2.5.4.1.2.1 are mandatory unless marked optional:

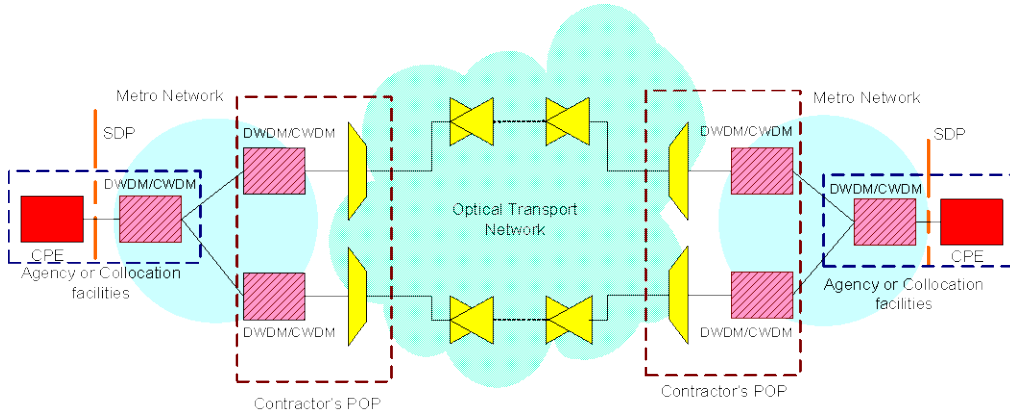
**C.2.5.4.1.2.1 Optical Wavelength Services (OWS) over WDM Features**

ID Number	Name of Feature	Description
1 [Optional]	Customer Network Management (CNM) – Level 1	The contractor shall provide monitoring capabilities only via this feature. Agency personnel shall be able to monitor wavelength(s) via alarm messages from the Optical Transport Network into a software user interface (UI). The UI shall be a website or a Java application available via a remote application.

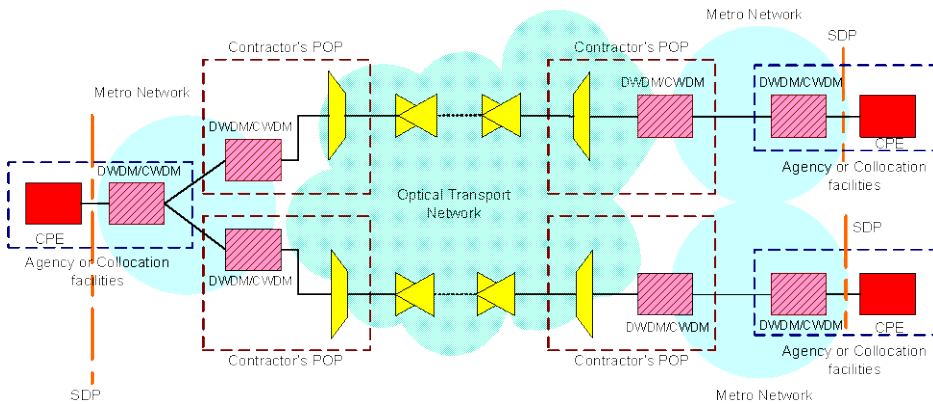
ID Number	Name of Feature	Description
2 [Optional]	Customer Network Management (CNM) – Level 2	The contractor shall provide management and monitoring capabilities. These shall be included support to alarm messages visibility and execution of control commands that shall be sent into the wavelength(s). Operations available shall include set up, modification and tearing-down connections. The CNM can be a website or a UI that is available via remote application.
3	Equipment Protection 1:1 - CPE	The contractor shall provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.
4	Equipment Protection 1+1 - CPE	The contractor shall provide protection to the User to Network Interfaces to the SDP, where the protection channel is permanently bridged to the working channel. Protection switching is faster than 1:1.
5	Equipment protection – Network Side	The contractor shall support two channels facing the network for full redundancy and equipment protection at the SDPs.
6	Geographical Diversity – Non-Domestic and CONUS Wavelengths	The contractor shall support geographically diverse wavelengths to be used by the Agency as a hard protection against fiber failures. When delivering CONUS wavelength services, the contractor shall maintain diversity through the metro and deliver the wavelength to two Agency SDPs. Physical interfaces facing the contractor's network that are required to provide geographically diverse wavelengths originating at the contractor's POP shall not impact the number of UNI's ordered by the Agency.
7	Geographical Diversity – Metro Wavelengths	The contractor shall support geographical diverse wavelengths in the metro area by delivering wavelengths in the metro area., The contractor shall maintain diversity through the metro and deliver the wavelength to two Agency SDPs.
8	Geographic Diverse Wavelength – single site delivery	The contractor shall provide two geographically diverse delivery channels from SDP1 to SDP2. This is the minimum configuration supported and shall consist of two fiber links traveling in different fiber conduits that traverse different geographies but end at the same SDP, as indicated in <b>Figure C.2.5.4.1.2.1-1</b> . In this illustration is assumed that the Agency and the contractor's metro WDM are collocated.
9 [Optional]	Geographic Diverse Wavelength – dual site delivery	The contractor shall provide two geographically diverse delivery channels from SDP1 to SDP3 and SDP2 to SDP4. The contractor shall provide the ability to support two wavelengths originating at a common SDP but ending at two different SDPs. As indicated in <b>Figure C.2.5.4.1.2.1-2</b> , in this illustration it is assumed that the Agency's

ID Number	Name of Feature	Description
		equipment is collocated with the contractor's metro WDM.
10	Geographic Diverse Wavelength – single metro hub	The contractor shall allow CONUS or Non-Domestic wavelength services to transport the wavelengths through the metro network via single metro hub as depicted in <b>Figure C.2.5.4.1.2.1-3</b>
11 [Optional]	Geographic Diverse Wavelength – dual metro hub	The contractor shall support CONUS or Non-Domestic wavelength services to transport the wavelengths through the metro network via a dual metro hub.
12 [Optional]	Protected Non-Domestic Wavelength	The contractor shall support protected Non-Domestic Wavelengths and they shall be architected using submarine transmission protocols such as Bidirectional Path Switched Ring (BPSR) or equivalent. The contractor shall ensure protection switching in the submarine transmission networks to be less than 4 seconds for a single failure.
13 [Optional]	Protected CONUS Wavelength	The contractor shall support protected CONUS Wavelengths using transmission protocols to provide resiliency. Protection switching in the nationwide transmission networks shall be less than 300 ms for a single failure.
14	Protected Metro Wavelength	The contractor shall provide protection on a per-wavelength basis when delivering services in the metro areas, such as Unidirectional Path Switched Ring (UPSR). Restoration times for protected wavelengths in the metro area shall be below 60 ms for a single failure. When delivering protected wavelengths in the metro area, the Agency and the contractor shall agree on whether equipment protection is required facing the CPE. If so, the contractor shall provide protection at the SDP and multiple UNIs shall be ordered, the number of which shall depend on the protection method selected by the Agency. The contractor shall supply its own physical UNIs.

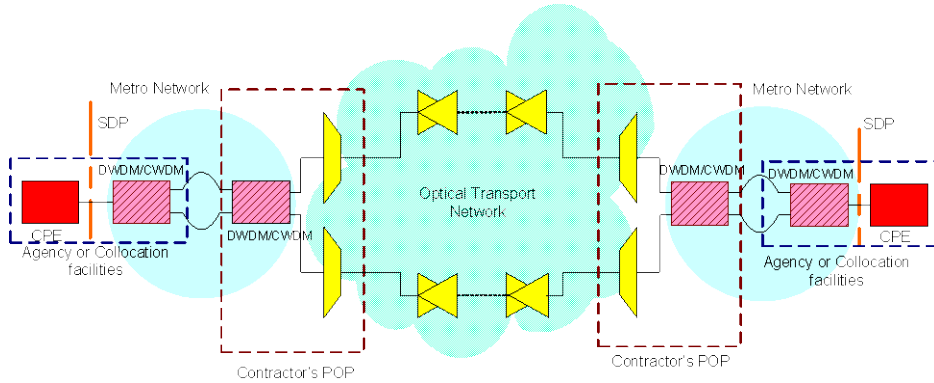
The following are supporting illustrations for some of the Features.



**Figure C.2.5.4.1.2.1-1 – Geographically Diverse Wavelengths Ending at the Same SDP**



**Figure C.2.5.4.1.2.1-2- Geographically Diverse Wavelengths Being Delivered at Two Customer's Sites**



**Figure C.2.5.4.1.2.1-3 – Delivery of Geographically Diverse Wavelengths via a Single Metro Hub.**

**C.2.5.4.1.3 Interfaces for OWS over WDM**

The User-To-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.5.4.1.3.1, are mandatory unless marked optional:

**C.2.5.4.1.3.1 Optical Wavelength Services (OWS) over WDM Interfaces**

UNI Type	Interface Type	Standard	Frequency of Operation	Payload Data Rate or Bandwidth	Signaling or Protocol Type
1	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gbps	SONET or SDH
2	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gbps	SONET or SDH Concatenated
3	Optical	GR-253, ITU-T G.707	1310 nm	10Gbps	SONET or SDH
4 [Optional]	Optical (over 12 fibers)	OIF-VSR4-01.0	850 nm	10 Gbps	SONET or SDH
5 [Optional]	Optical (over 1 fiber)	OIF VSR4-02	1310nm	10 Gbps	SONET or SDH
6 [Optional]	Optical (over 4 fibers)	OIF-VSR4-03.0	850nm	10 Gbps	SONET or SDH
7 [Optional]	Optical (over 1 fiber)	OIF-VSR4-04.0	850 nm	10 Gbps	SONET or SDH

**C.2.5.4.1.4 Performance Metrics for OWS over WDM**

1. Framed Wavelength Performance – Wavelengths based on SONET framing shall comply with performance requirements as stated in Section C.2.5.2.1.4 (7) through (8)
2. Transparent Wavelength Performance – If applicable, the contractor shall describe the methods by which fully transparent wavelengths (i.e. based on all optical gear, G.709 based) will be monitored and how Acceptable Quality Level (AQLs) will be met.
3. The contractor shall support In-Service Monitoring (ISM) and shall not rely on performance observed and measured at higher layers of the network.

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Optical Wavelength Services (OWS) over WDM in Section C.2.5.4.1.4.1 are mandatory unless marked optional:

**C.2.5.4.1.4.1 Optical Wavelength Services (OWS) over WDM Performance Metrics**

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
<b>Av(OWS over WDM)</b>	Routine	99.9%	> 99.9%	In-Service Monitoring See Note 1
	Critical (Optional)	99.999%	≥ 99.999%	
<b>Time To Restore (TTR)</b>	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	
<b>Grade of Service (Restoration Time)</b>	Routine	100 ms	≤ 100 ms	In-Service Monitoring See Note 3
	Critical (Optional)	60 ms	≤ 60 ms	
<b>Bit Error Rate(BER)</b>	Routine	10 <sup>-12</sup>	≤10 <sup>-12</sup>	Out-of-Service Monitoring See Note 4

Notes:

1. OWS over WDM availability shall be measured in service on an end-to-end basis. COT(HR) shall be calculated based on ES and/or SES as defined by GR-253, G.826 through G.829 and shall be expressed in Hours. Availability is computed by the standard formula:



$$A_v(OWS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Refer to Section C.3.3.1.2.4 for definitions and how to measure.
3. Restoration time is the time taken to reroute the traffic over a redundant path before the failure is repaired.

For critical user traffic, the redundant path should be a geographically diverse wavelength in a 1+1 configuration where the time accounted for includes the switching time and the propagation time in the fiber. Proactive monitoring using element management systems should be used to measure restoration time in real time. Simulation tools are also available and used by contractors. Calculated based on an 8000 km ring using the following formula: T= Detect time + Time in fiber + Time in Nodes + Time to bridge and switch + Traffic delay time. Domestic networks are usually ring based on the backbone. For 1+1 protection based on APS, GR-253 compliance includes 10 ms for detection and 50 ms for the actual switching.

4. Bit Error Rate (BER)- this KPI shall be measured out-of-service (OOS) at service turn-up or when requested by the subscribing Agency (i.e. after a failure). Both directions of the wavelength shall be tested. The duration of the BER test shall be determined using criteria included in recommendations such as ITU-T M.2100 and service acceptance testing criteria as included in Section E.2.

#### **C.2.5.4.2 OWS over the Automatic Switched Transport Network (ASTN) [Optional]**

The ASTN is an emerging technology for providing OWS.

##### **C.2.5.4.2.1 Service Description**

###### **C.2.5.4.2.1.1 Functional Description**

Basic OWS is a point-to-point, bi-directional service that can be delivered over the WDM or ASTN. OWS over ASTN, however, further enables Agencies to contract multi-point to multi-point connections in different configurations and classes of service options.

###### **C.2.5.4.2.1.2 Standards**

Optical Wavelength Services (OWS) over ASTN shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed as follows:

1. International Telecommunications Union (ITU) Standards defining frequencies grid and physical layer parameters for DWDM are G.692 and G.694

2. ITU Standards defining frequencies grid for CWDM are G.694.2. Standards for physical layer parameter still under development.
3. ITU Standards defining OTN architecture, interface formats and physical layer interfaces are G.872, G.709, and G.959.1 respectively. [Optional]
4. ITU Standard defining the Automatic Switched Transport Network (ASTN) is G.807
5. ITU Standards defining the Automatic Switched Optical Network (ASON) and their associated functions are G.808, G.7712.X, G.7713.X, G.7714.X, G.7715.X, G.7716.X, G.7717.X
6. ITU Standards defining frequencies grid and physical layer parameters for DWDM are G.692 and G.694
7. ITU Standards defining frequencies grid for CWDM are G.694.2. Standards for physical layer parameters are still under development.
8. ITU Standards defining OTN architecture, interface formats and physical layer interfaces are G.872, G.709, and G.959.1 respectively.
9. Applicable ITU Standards defining submarine transmission functional requirements are G.971, G.972, G.973, G.974, G.975, G.976 and G.977.
10. Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009.
11. Telcordia standards for metro protection are GR-253, GR-1400, and GR-1230.
12. Optical Internetworking Forum (OIF), User to Network Interface version 1.0, OIF-UNI-01.0
13. OIF-TL-01.1 - Implementation Agreement for Common Software Protocol, Control Syntax, and Physical (Electrical and Mechanical) Interfaces for Tunable Laser Modules.
14. OIF-TLMSA-01.0 - Multi-Source Agreement for CW Tunable Lasers.
15. OIF-ITLA-MSA-01.0 - Integratable Tunable Laser Assembly Multi-Source Agreement.
16. UNI 1.0 Signaling Specification, Release 2
  - a. OIF-UNI-01.0-R2-Common - User Network Interface (UNI) 1.0 Signaling Specification, Release 2: Common Part

- b. OIF-UNI-01.0-R2-RSVP - RSVP Extensions for User Network Interface (UNI) 1.0 Signaling, Release 2
- 17. CDR-01  
OIF-CDR-01.0 - Call Detail Records for OIF UNI 1.0 Billing.
- 18. SEP-01.1  
OIF-SEP-01.1 - Security Extension for UNI and NNI
- 19. SMI-01.0  
OIF-SMI-01.0 - Security Management Interfaces to Network Elements
- 20. E-NNI-01.0  
OIF-E-NNI-Sig-01.0 - Intra-Carrier E-NNI Signaling Specification
- 21. [Optional] VSR4-01 (OC-192 Very Short Reach Interface, 12 fibers 850nm)  
OIF-VSR4-01.0 - Very Short Reach (VSR) OC-192 Interface for Parallel Optics.
- 22. [Optional] VSR4-02 (OC-192 Very Short Reach Interface, 1 fiber 1310nm)  
Note: VSR4-02 has been included as the 4dB link option in VSR4-05 below
- 23. [Optional] VSR4-03.1 (OC-192 Very Short Reach Interface, 4 fibers 850nm)  
OIF-VSR4-03.0 - Very Short Reach (VSR) OC-192 Four Fiber Interface Based on Parallel Optics.
- 24. [Optional] VSR4-04 (OC-192 Very Short Reach Interface, 1 fiber 850nm)  
OIF-VSR4-04.0 - Serial Shortwave Very Short Reach (VSR) OC-192 Interface for Multimode Fiber.
- 25. [Optional] VSR4-05 (OC-192 Very Short Reach Interface, OXC 1310nm)  
OIF-VSR4-05.0 - Very Short Reach (VSR) OC-192 Interface Using 1310 Wavelength and 4 and 11 dB Link Budgets.
- 26. [Optional] VSR5-01 (OC-768 Very Short Reach Interface) OIF-VSR5-01.0  
Very Short Reach Interface Level 5 (VSR-5): SONET/SDH OC-768 Interface for Very Short Reach (VSR) Applications.
- 27. Tele Management Forum (TMF) 814.
- 28. All new versions, amendments, and modifications to the above documents and standards when commercially available.

#### **C.2.5.4.2.1.3 Connectivity**

The Optical Wavelength services over ASTN shall be delivered at the Service Delivery Point (SDP) via User to Network Interfaces (UNIs) as specified in Section C.2.5.2.3.1, Interfaces.

Optical Wavelength Services (OWS) over ASTN shall connect to and interoperate with:

1. Point-to-point, bi-directional, duplex services shall be connected from the SDP to the Optical Network via a fiber pair.
2. Inter-Agency connectivity shall be provided as the Agency may need to exchange information with another Agency's optical network in a secure manner.
3. OWS over ASTN may be provided by contractor-sponsored optical network that supplies a pool of bandwidth shared by different members. Consequently, OWS shall interoperate in a multi-contractor, multi-vendor, multi-user environment. Network-to-Network (NNI) interfaces shall be included in the subscription fees. NNI are basically the same physical interfaces as specified in Section C.2.5.4.2.3.

#### **C.2.5.4.2.1.4 Technical Capabilities**

The following Optical Wavelength Services (OWS) over ASTN capabilities are mandatory unless marked optional:

1. End-to-End Wavelength Termination - Same as specified in section C.2.5.4.1.1.4.
2. Reserved
3. Reserved
4. The contractor shall support the following connection types as defined by the ITU:
  - a. The contractor shall support Permanent Connections (PC) that are provisioned using traditional Element Management systems and are reserved for a period specified by the Agency.
  - b. The contractor shall support Soft Permanent Connections (SPC). The connection request for SPFs are initiated via the Element Management Systems via its management agent.
  - c. The contractor shall support Switched Connections (SC). The connection request for SCs shall be originated by the Agency clients via the User to Network Interface (UNI).
5. The contractor shall adhere to one of the following paradigms.
  - a. Overlay Model, as supported by the OIF and the ITU (ASON) – The contractor shall ensure that its network's architecture includes two separate control planes. One to control the Optical domain and the other one to control the IP domain. The IP domain shall be a client to the Optical domain and shall signal into the optical domain via a User to Network Interface (UNI) in order to utilize the optical network resources (i.e. to setup connections, increase/decrease bandwidth, etc.). The topology of the Optical domain shall not be visible to the clients.

- b. Peer-to-peer Model, as supported by the IETF – The contractor shall ensure that a single integrated control plane is used to control both the optical and the IP domains. In such arrangement, clients such as routers and optical network elements are peers allowing the optical topology to be visible to the clients.
6. Transmission Rates – The contractor shall support sub-wavelength and wavelength rates ranging from 2.5 Gbps and 10 Gbps. Following the implementation of Networx, the contractor may support optional rates beyond than 10 Gbps, e.g., 40 Gbps and greater.
7. Transparency. Same as specified in section C.2.5.4.1.1.4.
8. Delivery methods. Same as specified in section C.2.5.4.1.1.4.
9. Concatenation. The contractor shall support standard and non-standard concatenated signals in accordance with the standards established by the ITU and ATIS.
10. Control Plane – The contractor shall support the following:
  - a. Logical Interfaces. The contractor shall be able to support Logical Interfaces such as OIF/ITU UNI and NNI. These interfaces are identified in Section C.2.5.4.1.2.1 as UNI 1.0 and UNI 2.0.

They are logical entities that enable the following functionality.

    - i. UNI Functionality shall be supported
      1. Connection establishment
      2. Connection deletion
      3. Status change inquiry
      4. Auto discovery
      5. Non-disruptive modification of bandwidth
      6. Service Discovery
      7. Traffic exchange
    - ii. NNI Functionality shall be supported by the contractor's Control Plane.
  - b. Routing and signaling protocols shall be supported
  - c. Different Classes of Service shall be supported
  - d. Quality of Service (QoS) shall be supported
11. The following functions shall be supported by the contractor's Management Plane
  - a. Point-and-Click Provisioning

- b. Wavelength management. The contractor shall ensure that the management of the contracted wavelengths can be managed by the contractor or the Agency contractor

12. Efficient Transport – The contractor shall comply with this requirements as specified in Section C.2.5.4.1.1.4 # 14

13. The contractor shall ensure interoperability between its network and the Agency’s networks, even if they are built using multi-vendors equipment.

14. The contractor’s network shall support Virtual Rings in order to take advantage of the predictable and reliable resilience of such architectures while minimizing capital expenditures.

15. The contractor shall support Optical Virtual Private Networks (OVPNs). The following functions shall be supported as a minimum.

- a. Addressing
- b. Registration Service
- c. OVPN Identifier
- d. Inter-domain OVPN

16. The contractor’s network shall ensure scalability in order to support Agency’s traffic growth without sacrificing Agency’s performance requirements

**C.2.5.4.2.2 Features for OWS over ASTN**

The following Optical Wavelength Services (OWS) over ASTN features in Section C.2.5.4.2.2.1 are mandatory unless marked optional:

**C.2.5.4.2.2.1 Optical Wavelength Services (OWS) over ASTN Features**

ID Number	Name of Feature	Description
1	Customer Network Management (CNM) – Level 1	The contractor shall provide monitoring capabilities only via this feature. Agency personnel shall be able to monitor wavelength(s) via alarm messages from the Optical Transport Network into a software user interface (UI). The UI shall be a website or a Java application available via a remote application.
2	Customer Network Management (CNM) – Level 2	The contractor shall provide management and monitoring capabilities. These shall be included support to alarm messages visibility and execution of control commands that shall be sent into the wavelength(s). Operations available shall include set up, modification and tearing-down connections. The CNM can be a website or a UI that is available via remote application.
3	Equipment Protection 1:1 - CPE	The contractor shall provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.
4	Equipment Protection 1+1 - CPE	The contractor shall provide protection to the User to Network Interfaces to the SDP, where the protection channel is permanently bridged to the working channel.

ID Number	Name of Feature	Description
		Protection switching is faster than 1:1.
5	Equipment protection – Network Side	The contractor shall provide two channels for full redundancy and equipment protection from SDP1 in country 1 to SDP2 in country 2. This protection shall be provided on a 1:1-like protection method.
6	Geographic Wavelength – Diverse Single Delivery	The contractor shall provide two geographically diverse delivery channels from SDP1 to SDP2.
7	Geographic Wavelength – Diverse Dual Delivery	The contractor shall provide two geographically diverse delivery channels from SDP1 and SDP 2 to SDP3 and SDP4.
8	Multi-tiered protection	The contractor shall ensure that multi-tiered protection is supported such that the initial protection method selected defaults to different levels of protection with lesser priority. This shall take place when the network is not able to provide the original protection scheme selected. Mesh Protection shall be final and default protection level.
9	Optical Virtual Private Network (OVPN)	The contractor shall support point-to-point, multi-point-to-multi-point resources from the contractor's network to be used by the Agency. This service shall allow the Agency to access ports, links and bandwidth from the contractor's optical network. 5.
10	Planning Tools Support	The contractor shall support Planning Tools in order for the user to plan in advance network resources contracted by the Agency. The Planning Tools shall include the following functions as a minimum: <ol style="list-style-type: none"> <li>1. Connection management</li> <li>2. Off-line Routing</li> <li>3. Capacity Planning</li> <li>4. Failure simulation</li> <li>5. Forecasting</li> <li>6. Trend Analyses</li> </ol>
11	Reserved bandwidth	The contractor shall support the reservation of fixed bandwidths and routes as specified by the Agency.
12	Shared protection	The contractor shall allow the Agency to choose protection bandwidth allocated in a pool of bandwidth shared by different customers in the network
13	Subscription to a multi-user optical network	The contractor shall support the Agency in the subscription for the usage of bandwidth available in a pool of bandwidth via tele-houses or CO-hotels. Such pools of bandwidth shall be managed by the collocation company where the Agency contracts additional wavelengths on-demand from the collocation company or subscription manager.
14	UNI 1.0	The contractor shall support UNI 1.0 at the SDP compliant to OIF-UNI-01.00
15	UNI 1.0, Release 2	The contractor shall support UNI 1.0 Release 2.0 at the SDP compliant to OIF-UNI-01.00 Release 2.0
16	UNI 2.0	The contractor shall support UNI 2.0 at the SDP compliant to OIF-UNI-02.00 when available commercially

### C.2.5.4.2.3 Interfaces for OWS over ASTN

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.5.4.2.3.1, are mandatory unless marked optional:

#### C.2.5.4.2.3.1 Optical Wavelength Services (OWS) over ASTN Interfaces

UNI Type	Interface Type	Standard	Frequency of Operation	Payload Data Rate or Bandwidth	Signaling or Protocol Type
1	Optical	GR-253, ITU-T G.707	1310 nm	2.5 Gbps	SONET or SDH
2	Optical	GR-253, ITU-T G.707	1310 nm	2.5 Gbps	SONET or SDH Concatenated
3	Optical	GR-253, ITU-T G.707	1310 nm	10 Gbps	SONET or SDH
4 [Optional]	Optical (over 12 fibers)	OIF-VSR4-01.0	850 nm	10 Gbps	SONET or SDH
5 [Optional]	Optical (over 1 fiber)	OIF VSR4-02	1310nm	10 Gbps	SONET or SDH
6 [Optional]	Optical (over 4 fibers)	OIF-VSR4-03.0	850nm	10 Gbps	SONET or SDH
7 [Optional]	Optical (over 1 fiber)	OIF-VSR4-04.0	850 nm	10 Gbps	SONET or SDH
8 [Optional]	Optical	OIF-VSR4-05.0	1310nm	10 Gbps	SONET or SDH
9 [Optional]	Optical	OIF-VSR5-01.0	850nm	40 Gbps	SONET or SDH

#### C.2.5.4.2.4 Performance for OWS over ASTN

1. Framed Wavelength Performance – Wavelength based on SONET framing shall comply with performance requirements as stated in Section C.2.5.2.1.4 (7) through (8)
2. Transparent Wavelength Performance – If applicable, the contractor shall describe the methods by which fully transparent wavelengths (i.e. based on all optical gear, G.709 based) will be monitored and how Acceptable Quality Level (AQLS) will be met
3. The contractor shall support In-Service Monitoring (ISM) and shall not rely on performance observed and measured at higher layers of the network.



The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Optical Wavelength Services (OWS) over (ASTN in Section C.2.5.4.2.4.1 are mandatory unless marked optional

#### C.2.5.4.2.4.1 Optical Wavelength Services (OWS) over ASTN Performance Metrics

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(OWS over ASTN)	Routine	99.9%	$\geq 99.9\%$	In-Service Monitoring See Note 1
	Critical (Optional)	99.999%	$\geq 99.999\%$	
Time To Restore (TTR)	Without Dispatch	4 hours	$\leq 4$ hours	See Note 2
	With Dispatch	8 hours	$\leq 8$ hours	
Grade of Service (Restoration Time) Non-Domestic	Routine	4 seconds	$\leq 4$ seconds	In-Service Monitoring See Notes 3, 4 and 5
	Critical (Optional)	1 second	$\leq 1$ second	
Grade of Service (Restoration Time) CONUS	Routine	300 ms	$\leq 300$ ms	
	Critical (Optional)	60 ms	$\leq 60$ ms	
Grade of Service (Restoration Time) Metro	Routine	100 ms	$\leq 100$ ms	
	Critical (Optional)	60 ms	$\leq 60$ ms	
Bit Error Ratio (BER)	Routine	$10^{-12}$	$\leq 10^{-12}$	Out of-Service Monitoring See Note 6
Latency (Delay)	Routine	400 ms	$\leq 400$ ms	In-Service Monitoring

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Non-Domestic	Critical (Optional)	200 ms	≤ 200 ms	
Latency (Delay) CONUS	Routine	100ms	≤ 100 ms	In-Service Monitoring

Notes:

1. OWS over WDM availability shall be measured in service on an end-to-end basis. COT(HR) shall be calculated based on ES and/or SES as defined by GR-253, G.826 through G.829 and shall be expressed in Hours. Availability is computed by the standard formula:

$$Av(OWS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for definition and how to measure.
3. Restoration time is the time taken to reroute the traffic over a redundant path before the failure is repaired. For critical user traffic, the redundant path should be a geographically diverse wavelength in a 1+1 configuration where the time accounted for includes the switching time and the propagation time in the fiber. Due to the length of transoceanic distances, 1 second is more than sufficient to move the critical traffic to an alternate, redundant path. In the case of Routine users, restoration time should be longer as restoration should be used. Proactive monitoring using element management systems should be used to measure restoration time in real time. Simulation tools shall also be available and used by contractors.
4. For CONUS, Routine Traffic, Restoration time is calculated based on an 8000 km ring using the following formula: T= Detect time + Time in fiber + Time in Nodes + Time to bridge and switch + Traffic delay time. Domestic networks are usually ring based on the backbone.
5. Assuming 1+1 protection for Mission Critical traffic, based on APS, GR-253 compliance which includes 10 ms for detection and 50 ms for the actual switching.
6. Bit Error Rate (BER) - This KPI shall be measured out-of-service (OOS) at service turn-up or when requested by the subscribing Agency (i.e. after a failure). Both directions of the wavelength shall be tested. The duration of the BER test shall be determined using criteria included in recommendations such as ITU-T

M.2100 and service acceptance testing criteria as included in Section E.2.  
Combined Services

### **C.2.5.5 Combined Services (CS)**

Combined Services (CS) is a collection of separate telecommunications services packaged into a single service offering from a contractor. Agencies may utilize a Combined Services package to provide a core telecommunications service that suits their fundamental business needs.

#### **C.2.5.5.1 Service Description**

##### **C.2.5.5.1.1 Functional Definition**

Combined Services provides local, regional toll, and domestic (CONUS and OCONUS) long distance service in a CS core package to enable Agencies to procure voice telecommunications service from a single source. Additional optional features and optional services may be made available to offer Agencies flexible service plans to support their requirements.

##### **C.2.5.5.1.2 Standards**

Combined Services shall comply with the following standards and the required standards of the individual services being combined as applicable. The contractor shall refer to the appropriate section for a description of the technical standards for each respective optional service included with the CS package as described in Section C.2.6.1.2.1. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. ANSI T1.101
2. ANSI ISDN
3. ANSI SS7 standards
4. Telcordia Notes on the Networks, currently Issue 4, October 2000 SR-2275
5. Telcordia LATA Switching Systems Generic Requirements (LSSGR) FR-64
6. ITU-T E.164 as interpreted by the Industry Number Committee of ATIS
7. All applicable Telcordia, ANSI, and ITU Standards
8. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

**C.2.5.5.1.3 Connectivity**

Combined Services shall comply with the connectivity requirements for the individual services being combined. The contractor shall refer to Section C.2.2.1.1.3 Voice Services, for the connectivity requirements associated with the core CS service package. Refer to the following sections, under Connectivity, for the appropriate requirements for optional services:

1. C.2.2.3 Toll Free Services (TFS)
2. C.2.4.1 Internet Protocol Service (IPS)
3. C.2.14.1 Cellular / Personal Communications Service (CPCS)

**C.2.5.5.1.4 Technical Capabilities**

The following Combined Services capabilities are mandatory unless indicated otherwise:

1. The contractor shall provide local, regional toll, and domestic long distance (CONUS and OCONUS) calling capabilities with unlimited usage as the core service in a single combined service package.
2. The CS core service can also offer a portfolio of optional features with unlimited usage. Feature ID's 1 through 9 in Table C.2.6.1.2-1 provide a description of the optional features that the contractor can include with the CS core service.
3. The contractor shall have the flexibility to supplement the core CS service with additional optional service offerings such as non-domestic calling, wireless, toll free service, and Internet services. Refer to feature ID numbers 10 through 14 in Table C.2.6.1.2-1 for a description of service offering options that can be made available for the CS package.
4. The contractor shall provide a single invoice for all services included in their proposed CS offering.
5. The contractor shall comply with all applicable local and FCC regulatory requirements including Local Number Portability (LNP), directory assistance, and emergency services (911 or E911) requirements to identify the location of an originating station and route them to the appropriate Public Safety Answering Point (PSAP).
6. The contractor shall allow non-domestic dialing for CS. It should be noted that non-domestic calling from the CS contractor is an optional feature. Agencies may choose any provider, independent of the CS contractor, for non-domestic calling. The contractor shall restrict non-domestic calling if requested by the subscribing Agency.

### C.2.5.5.2 Features

The following Combined Services features in Section C.2.6.1.2.1 are optional.

#### C.2.5.5.2.1 Combined Services Features

ID Number	Name of Feature	Description
1	Call Forwarding (All, Busy, No Answer)  (Optional)	The contractor shall provide the capability to allow a station user to choose to reroute incoming calls to another specified telephone number. <ol style="list-style-type: none"> <li>1. The contractor shall offer call forwarding on a busy, no answer, or all calls basis.</li> <li>2. The Agency will have the option to limit call forwarding to local and/or long distance numbers</li> <li>3. Outgoing calling capability shall be allowed when call forwarding is activated</li> <li>4. It shall be possible for the station user to activate or cancel this feature.</li> <li>5. This feature capability shall be administered on a station basis.</li> </ol>
2	Call Transfer  (Optional)	The contractor shall provide the capability to allow a station user to transfer any call in progress to another telephone number without the assistance of the attendant. This feature capability shall be administered on a station basis according to the subscribing Agencies needs.
3	Call Waiting  (Optional)	The contractor shall provide the capability that allows a call to a busy station line to be held waiting while a tone signal is directed towards the busy station user. (Only the called station user shall hear this tone). The contractor shall offer the capability for the subscriber to disable the service, temporarily on a per call basis. This feature capability shall be administered on a station basis.
4	Caller ID  (Optional)	The contractor shall provide the Automatic Number Identification number (full ten digit number or non-domestic equivalent), when available, to the terminating station.
5	Caller ID Block  (Optional)	The contractor shall provide, the Agency with the option to activate or deactivate Caller ID transmission from an originating station on a permanent or per call basis.
6	Remote Access to Call Forwarding  (Optional)	The contractor shall provide the capability for subscribers to remotely activate or de-activate the call forwarding feature. This feature capability shall be administered on a station basis.
7	Speed Dial  (Optional)	The contractor shall provide abbreviated single digit dialing capability on a per station basis. <ol style="list-style-type: none"> <li>1. The service shall enable a station user to reach any of a pre selected group of stations by dialing single-digit codes.</li> <li>2. A minimum of eight programmable speed dial codes should be available.</li> <li>3. Feature capability shall be administered on a station basis.</li> </ol>

ID Number	Name of Feature	Description
8	Three Way Calling (Optional)	The contractor shall provide the capability that allows a station user to establish a multiparty conference connection of up to a minimum of three conferees including themselves, without attendant assistance. This feature capability shall be administered on a station basis.
9	Voice Mail (Optional)	<p>The contractor shall provide voice mail capability that includes voice messaging transmission, reception, and storage for 24x7 except for periodic scheduled maintenance. The contractor shall provide the following minimum capabilities:</p> <ol style="list-style-type: none"> <li>1. At least thirty minutes of storage time (or 15 messages)</li> <li>2. Ability to remotely access voice mail services</li> <li>3. Secure access to voice mail via a password or PIN</li> <li>4. Automatic notification when a message is received. The contractor shall provide options for notification (a) message waiting indication or (b) an outcall to a pager/cell phone.</li> <li>5. Minimum message length of two minutes</li> <li>6. Capability to record custom voice mail greetings</li> </ol> <p>This feature capability shall be administered on a station basis.</p>
10	Calling Card Service (Optional)	The contractor shall provide the capability for calling card services to be included as an option for the CS package. Refer to Section C.2.2.1.2 for a technical description of Calling cards (authorization code).
11	Internet Service (Optional)	The contractor shall provide the capability for Internet access services to be included as an option for the CS package. Internet access shall be provided by (a) DSL service (where available) or (b) via dedicated or switched dial up access service. Refer to Section C.2.4.1 for a technical description of Internet Protocol Service.
12	Non-Domestic Calling Service (Optional)	The contractor shall provide the capability for non-domestic long distance service from the contractor to be included as an option for the CS package. The contractor shall provide the capability to selectively block this feature by station and country code at Agency request. Refer to Section C.2.2.1 for a technical description of non-domestic long distance service.
13	Toll Free Calling Service (Optional)	<p>The contractor shall provide the capability for basic incoming toll free services to be included as an option for the CS package. The contractor shall provide the following toll free features</p> <ol style="list-style-type: none"> <li>1. Alternate Routing</li> <li>2. ANI</li> <li>3. Announcements</li> </ol>

ID Number	Name of Feature	Description
		4. Day of Week Routing 5. Day of Year Routing (Holiday Routing) 6. Dialed Number Identification Service (DNIS) 7. Make Busy Arrangement 8. NPA/NXX Routing 9. Service Assurance 10. Terminating Announcements 11. Time of Day routing  Refer to Section C.2.2.3 for a technical description of Toll Free Service features.
14	Wireless Service (Optional)	The contractor shall provide the capability for wireless service plans to be included as an option for the CS package. Refer to Section C.2.14.1 for a technical description of Cellular / Personal Communications Service.

**C.2.5.5.3 Interfaces**

**C.2.5.5.3.1 Network Interface**

The contractor shall support user-to-network interfaces (UNIs) at the SDP for each individual service offered under CS as described in this contract. There are no additional CS specific interface requirements. The contractor shall refer to Section C.2.2.1 Voice Services, for the interface requirements associated with the core CS service package. Refer to the following sections for the appropriate network interface requirements for CS optional services:

1. C.2.2.3 Toll Free Service (TFS)
2. C.2.4.1 Internet Protocol Services (IPS)
3. C.2.14.1 Cellular / Personal Communications Services (CPCS)

**C.2.5.5.4 Performance Metrics**

The performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for the local voice service component of the core Combined Services package shall be measured and monitored as defined in Section C.2.6.1.4.1 below.

**C.2.5.5.4.1 Combined Services Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (SDP-to-SDP)	Routine	99.5%	≥ 99.5%	See Note 1
	Critical	99.95%	≥ 99.95%	

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
	(Optional)			
Grade of Service (Call Blockage) (SDP-to-SDP)	Routine	0.07	≤ 0.07	See Note 2
	Critical (Optional)	0.01	≤ 0.01	
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

The optional services presented in Section C.2.6.1.2.1 shall comply with the performance metrics for each individual service offering as described in this contract. The contractor shall refer to the appropriate contract section for the performance metrics associated with each optional service:

1. C.2.2.3 Toll Free Service (TFS)
2. C.2.4.1 Internet Protocol Service (IPS),
3. C.2.14.1 Cellular / Personal Communications Service (CPCS)

Notes:

1. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the CS is operationally available to the Agency. Availability is computed by the standard formula:  

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
2. Call Blockage is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements. For example, 0.01 indicates that 1% of the calls are not being completed successfully (e.g. 1 out of 100 calls).
3. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.6 Virtual Private Network Services**

**C.2.6.1 Ethernet Services (EthS)**

Ethernet Services allow Agencies to interconnect their LANs seamlessly over the Metro Area Networks (MAN) or the Wide Area Networks (WAN) regardless of the geographical location of their sites. Ethernet Services enable Intra and Extranet services, as well as Intra and Inter-Agency communications.

**C.2.6.1.1 Service Description**



#### C.2.6.1.1.1 Functional Definition

Ethernet Services are offered over point-to-point connections and multi-point to multi-point connections, as described in Section C.2.7.1.1.34. Ethernet Services exploit Ethernet's flexibility, cost effectiveness, and differentiation of service capabilities while providing end-to-end transport to data traffic with minimal protocol conversion. The technology components and implementation details for delivering Ethernet Services are left to contractor's discretion; however, the following services shall be supported:

1. **Ethernet Private Line (E-LINE).** Point-to-point service in which bandwidth is reserved and used for mission critical traffic. This service resembles traditional Time Division Multiplexing (TDM) private line service. Some applications include router interconnect, business continuity, and disaster recovery. E-LINE service can be offered over the MAN and/or WAN.
2. **Ethernet Private LAN (E-LAN).** Multi-point to multi-point service in which disparate LAN segments are connected into a single virtual LAN. Applications include Inter and Intra-city LAN connectivity, router interconnect and server consolidation. It can be offered over the MAN and/or WAN.

#### C.2.6.1.1.2 Standards

Ethernet Services shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed as follows:

1. Metro Ethernet Forum (MEF)
  - a. Ethernet Services Model, Phase 1. Technical Specification, MEF 1, November 10, 2003.
  - b. Requirements and Framework for Ethernet Service Protection in Metro Ethernet Networks. Technical Specification, MEF 2, February 8, 2004.
  - c. Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks. Technical Specification, MEF 3, April 13, 2004.
2. Internet Engineering Task Force (IETF)
  - a. RFC 3069
3. International Telecommunications Union (ITU)
  - a. G.8011.1/Y.1307.1, (g.epls, g.eota) Ethernet Private Line, in progress
  - b. G.8011/Y.1307, (g.ethsrv), Ethernet over Transport – Ethernet services framework, in progress
  - c. G.8012/Y.1308 (g.eint), Ethernet UNI and Ethernet over Transport NNI, in progress
  - d. G.nni, Ethernet over transport network node interface, approval targeted for May 2004
4. Institute of Electrical and Electronics Engineers, Inc. (IEEE)

- a. IEEE 802.3, 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY
- b. IEEE 802.3ae, 10Gbit Ethernet 802.17, Resilient Packet Rings (RPR) – In progress
- c. 802.1ah, Ethernet First Mile – In progress
- d. IEEE 802.1p
- e. IEEE 802.1q

5. Ethernet in the First Mile Alliance – EFM standards for providing a single approach for transmitting Ethernet over copper, fiber optic point-to-point networks and fiber optic point-to-multi-point networks are in progress, in conjunction with the IEEE.

6. 10 Gigabit Ethernet Alliance

7. All new versions, amendments, and modifications to the above documents and standards when commercially available.

#### **C.2.6.1.1.3 Connectivity**

Ethernet Services shall connect to and interoperate with:

**1. Intra-Agency LAN-LAN Connectivity.** Ethernet services provide connectivity for an Agency's LANs located in the same city or different cities, thereby extending the LAN to the MAN and WAN. This is achieved by connecting the Agency's SDP(s) in one location to another SDP(s) in one or more locations. Interconnection shall be possible over transoceanic links, if required.

**2. Inter-Agency LAN-LAN Connectivity.** Different Agencies may share resources to connect to the contractor's metro or long haul network. This is achieved by connecting from one Agency's SDP(s) to other Agencies SDP(s).

**3. Internet Connectivity.** Internet connectivity is for Intra-net and internet services. Ethernet connection shall be provided from the Agency's SDP(s) to one or more Internet Service Provider(s) (ISPs) over the metro, the WAN, or transoceanic links.

#### **C.2.6.1.1.4 Technical Capabilities**

The following Ethernet Services (EthS) capabilities are mandatory unless marked optional:

1. End-to-End Ethernet Delivery - A seamless end-to-end service shall be provided from the SDP Customer Premise Equipment (CPE) traversing the contractor's network (Metro Access/Core and the Long Haul) in order to minimize conversion of protocols. The contractor shall indicate if protocol conversions are required and how they impact the delay when delivering services end-to-end. The following Ethernet service shall be provided:
  - a. Intra-City Ethernet Service – the contractor shall provide Ethernet connections to Agency sites located in the same city.

- b. Inter-City Ethernet Service –The contractor shall provide Ethernet connections to Agency sites located in different cities. [Optional]
2. The contractor shall support Ethernet UNI (User-to-Network-Interface) to support Layer 2 and Layer 3 clients. Layer 3 clients are Agency devices which support Layer 3 protocol packets such as IPv4, IPv6. [Optional]
  3. The contractor shall support Ethernet Virtual Connections (EVC), which are used to define the association of two or more User-to-Network Interfaces (UNIs).
  4. The contractor shall support delivery of the EthS at the Agency's Service Delivery Point (SDP) via a User-to-Network Interface (UNI).
  5. The contractor shall support circuit emulation services for FR, ATM and TDM services. [Optional]
  6. The contractor shall support point-to-point, multi-point-to-multi-point, and point-to-multi-point EVCs.
  7. EVC multiplexing shall be supported in order to build more sophisticated services while minimizing the hardware UNIs required.
  8. The contractor shall describe the Ingress/Egress bandwidth profiles supported per UNI. This applies to electrical as well as optical ports.
  9. The contractor shall support rate-limited throughput access links, i.e., 1000 Mbps or 1Gbps port rate limited in 100 Mbps increments.
  10. The contractor shall support rate-limiting at the Agency's SDP and at the individual VLAN ingress and egress.
  11. The contractor shall describe the Ingress/Egress bandwidth profiles per EVC. For example, for a 10Mbps service, the bandwidth profiles available may be 5 and 10 Mbps. For 100 Mbps, the bandwidth profiles may be available in increments of 10 Mbps. For 1 Gbps, the bandwidth profiles may be available in increments of 100 Mbps.
  12. Privacy and security similar to a Frame Relay or ATM Permanent Virtual Circuit (PVC) shall be supported.
  13. The contractor shall support the following service attributes:
    - a. Physical Interface shall be supported as listed in Section C.2.7.1.3.

- b. The following traffic profiles shall be supported:
    - i. Committed Information Rate (CIR) - minimum amount of bandwidth guaranteed for an Ethernet service.
    - ii. Committed Burst Size (CBS) – the size up to which subscriber traffic is allowed to burst and still be in-profile and not discarded or shaped.
    - iii. Peak Information Rate (PIR) – specifies the rate above the CIR that traffic is allowed into the network for a given burst interval defined by the MBS.
    - iv. Maximum Burst Size (MBS)
  - c. Performance parameters shall be supported to conform to the ones outlined in Section C.2.7.1.4.
  - d. Service Frame Delivery options supported shall include:
    - i. Unicast Frame Delivery
    - ii. Multicast Frame Delivery, as per RFC 1112
    - iii. Broadcast Frame Delivery as per IEEE 802.3
  - e. VLAN tag supported shall include:
    - i. VLAN tag preservation
    - ii. VLAN tag translation
    - iii. VLAN tag stacking
    - iv. VLAN aggregation across a common physical connection(Optional)
  - f. Service multiplexing shall be supported to include multiple EVCs connected via a single UNI.
  - g. Bundling shall be supported to enable two or more VLAN IDs to be mapped into a single EVC at a UNI.
  - h. Security Filters shall be supported. [Optional]
14. The contractor shall indicate what proactive Performance Monitoring (PM) capabilities are supported. It is desirable that at least one of the items in the following list be supported.
- a. Signal failure
  - b. Signal degradation
  - c. Connectivity or Loss of connectivity
  - d. Frame loss
  - e. Errored frames
  - f. Looping
  - g. Denial of service (DoS)
  - h. Misinserted frames
  - i. Maintenance parameters

15. The contractor shall support at least one of the following maintenance functions:
  - a. Alarm suppression
  - b. Loopbacks (intrusive and non-intrusive)
  - c. Protection switching, restoration, etc.
16. Delivery of Ethernet services in the First/Last Mile shall be accomplished over the following physical media: [Optional]
  - a. Copper
  - b. Fiber
  - c. Passive Optical Networks (E-PON)
  - d. Coaxial Cable
17. The contractor shall support a wide range of access methods as required by the Agencies; they are outlined in Section C.2.1.5, additional to those they shall include: [Optional]
  - a. Terrestrial microwave access (LMDS)
  - b. Satellite Access Services
  - c. Free Space Optics (FSO)
18. The contractor shall support the following network topologies:
  - a. Point-to-point
  - b. Point-to-Multi-point (i.e., hub-and-spoke)
  - c. Multi-point-to-Multi-point (i.e., mesh)
  - d. Rings[Optional]
19. The contractor shall support geographical diversity to provide added reliability. An Agency may buy a geographical diverse route from the same or a different contractor to serve as a protection path.
20. Bridging shall be supported in compliance with IEEE 802.1X
21. The contractor shall indicate the Virtual Connection Sizes supported by its network. As a minimum, the following shall be supported:
  - a. For point-to-point Ethernet connections – up to 1 Gbps, and 10 Gbps as optional
  - b. For multi-point-to-multi-point connections – up to 1 Gbps, and 10 Gbps as optional
22. The contractor shall notify the Network PMO when it updates the Protection Mechanisms for this service.
23. The contractor shall indicate whether the Ethernet services enabled by its networks use any of the following transport methods and Protocol Interworking:

- a. Ethernet over CWDM/DWDM – The contractor shall indicate limitations, if any, when transporting native Ethernet over WDM gear.
  - b. Ethernet over SONET/SDH, ASTN/OTN – The contractor shall indicate limitations, if any, when using Generic Framing Procedure (GFP), LCAS and Virtual Concatenation Technologies
  - c. Ethernet over ATM
  - d. Ethernet over FR
  - e. Ethernet over MPLS – The contractor shall indicate whether “c” and “d” are supported over the MPLS infrastructure and the approach for implementation.
24. Quality of Service (QoS) [Optional] – The contractor shall support traffic prioritization that enables higher priority traffic to be transmitted first.
25. The contractor shall support traffic reconfiguration that supports the ability of the Agency to modify a specific service connection subsequent to the establishment of the connection. Changes to an established connection may include upgrade/downgrade of speeds that do not result in physical equipment changes.

**C.2.6.1.2 Features**

The following Ethernet Services (EthS) features in Section C.2.7.1.2.1 are mandatory unless marked optional:

**C.2.6.1.2.1 Ethernet Services Features**

ID Number	Name of Feature	Description
1	Bandwidth-on-Demand (BoD)	The contractor shall support bandwidth increments and decrements on demand, as agreed between the contractor and the Agency. The contractor shall indicate what increments are available to modify the contracted bandwidth in near real time. Options for incremental/reduction steps shall include at least 1 Mbps, 5 Mbps, and 10 Mbps. Provisioning time for this feature shall not exceed 30 min per instance unless otherwise agreed by the Agency and contractor on a case by case basis.
2	Reserved Protection Bandwidth	The contractor shall allow the Agency to specify the amount of bandwidth to be reserved with the desired constraints, i.e., geographical routing to minimize cost of the connection. The bandwidth reserved shall only be used for Agency requirements.
3	Shared Protection Bandwidth	The contractor shall allow the Agency to specify the amount of bandwidth required for protection with no constraints on how the protection channels shall be routed.

**C.2.6.1.3 Interfaces**

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.7.1.3.1, are mandatory unless marked optional:

## C.2.6.1.3.1 Ethernet Services Interfaces

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
1	Optical	IEEE 802.3z	1310 nm	1.25 Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1.25 Gbps	Gigabit Ethernet
3	Optical	IEEE 802.3	1310 nm	125 Mbps	Fast Ethernet
4 (Optional)	Optical	IEEE 802.3ae	1310 nm	10 Gbps	10GBASE-SR (65 meters)
5 (Optional)	Optical	IEEE 802.3ae	850nm	10 Gbps	10GBASE-SW
6 (Optional)	Optical	IEEE 802.3ae	1550 nm	10 Gbps	10GBASE-ER
7 (Optional)	Optical	IEEE 802.3ae	1310 nm	10 Gbps	10GBASE-LR
8 (Optional)	Optical	IEEE 802.3ae	1550 nm	10 Gbps	10GBASE-LW
9 (Optional)	Optical	IEEE 802.3ae	1310 nm Multimode	10 Gbps	CWDM 10GBASE-LX4 (300 meters)
10 (Optional)	Optical	IEEE 802.3ae	1310 nm Single Mode	10 Gbps	CWDM 10GBASE-LX4 (10,000 meters)
11 (Optional)	Optical	IEEE 802.3ae	1310 nm Single Mode	10 Gbps	10GBASE-LW (10,000 meters)
12 (Optional)	Optical	IEEE 802.3ae	1550 nm Single Mode	10 Gbps	10GBASE-EW (40,000 meters)
13 (Optional)	Electrical	IEEE 802.3	N/A	10 Mbps	10Base
14	Electrical	IEEE 802.3	N/A	100 Mbps	100 Base
15	Optical	IEEE 802.3		1 Gbps	1000Base
16 (Optional)	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
17 (Optional)	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c
18	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-LX
19	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-SX
20 (Optional)	Electrical (Copper)	IEEE 802.3z	N/A	1 Gbps	1000BASE-CX
21 (Optional)	Electrical (Twisted pair)	IEEE 802.ab	N/A	1 Gbps	1000BASE-T
22 (Optional)	Optical	GR-253, ITU-T G.707	1310 nm	10 Gbps	SONET or SDH

#### C.2.6.1.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Ethernet Services (EthS) in Section C.2.7.1.4.1 are mandatory unless marked optional:

##### C.2.6.1.4.1 Ethernet Services Performance Metrics

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(EthS)	Routine (Single Connection)	99.5%	$\geq 99.5\%$	See Note 1
	Critical (Double Connection) (Optional)	99.99%	$\geq 99.99\%$	
Latency (EthS)	CONUS	100 ms	$\leq 100$ ms	See Note 2
	OCONUS	200 ms	$\leq 200$ ms	
Jitter(Packet)	Routine	10 ms	$\leq 10$ ms	See Note 3
Grade of Service (Packet Delivery Rate)	Routine	99.95%	$\geq 99.95\%$ at all times	See Note 4
	Critical (Optional)	99.99%	$\geq 99.99\%$ at all times	
Time To Repair(TTR)	Without Dispatch	4 hours	$\leq 4$ hours	See Note 5
	With Dispatch	8 hours	$\leq 8$ hours	
Grade of Service (Fail Over Time)	Routine	1 minute	1 minute	See Note 6
	Critical (Optional)	100 ms	$\leq 100$ ms	See Note 7



## Notes:

1. EthS availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the EthS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(EthS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the round trip delay experienced by an end-user across the contractor's network to other Agency's sites. It is the average time for packets to travel over the core network. The Internet Control Message Protocol (ICMP) test can be used to calculate packet delivery and latency. The ICMP test consists of sending, every five minutes, a series of five test packets between originating Agency's SDPs and the delivery SDPs. The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. Contractor shall meet or exceed standards set by RFC 1242 and RFC 2285. It can be determined by the following formula:

(Distance/(0.6\*c)+hops\*delay), where c is the velocity of light and 0.6 is the multiplier recommended by the ITU (G.144) in ms/km plus the delay in each hop caused by the routers times the number of hops.

3. Measurement of packet jitter are performed by injecting packets at regular intervals into the network and measuring the variability in the arrival time. Relevant standard is RFC 2679.
4. Network devices, such as switches and routers, sometimes have to hold data packets in buffered queues when a link gets congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost. Relevant standards are RFC 1242 and RFC 2285.
5. Refer to Section C.3.3.1.2.4 for definitions and how to measure.
6. Restoration for links transported over the Ethernet infrastructure (i.e., Ethernet switches) is achieved by the use of protocols such as Spanning Tree (IEEE 802.1d), which converge slower than SONET. Therefore, Ethernet Services for critical users shall be delivered over a carrier class infrastructure.
7. Local restoration for critical users shall be achieved in less than 100 milliseconds.

### C.2.6.2 Premises-based IP VPN Services (PBIP-VPNS)

Premises-based IP Virtual Private Networks (VPN) are typically IPsec tunnel-based, with customer edge (CE) devices encrypting and decrypting traffic before it enters and leaves the contractor's network. Because security is provided on an end-to-end basis, the contractor has no visibility into the IP tunnel. A Layer 3 IP VPN provides any-to-any connectivity because it relies on IP routing to build paths, which facilitates the creation of fully or partially meshed networks the contractor's cloud.

#### C.2.6.2.1 Service Description

### C.2.6.2.1.1 Functional Definition

The contractor manages VPN gateways, i.e., Customer Premises Equipment (CPE), at Agency locations and provides connectivity to the contractor's IP network. The CPE provides secure, end-to-end encrypted tunnels to carry an Agency's traffic between its locations. The CPE may either be furnished by an Agency or by the contractor as part of a managed service.

Premises-based IP VPNs provides three basic solutions:

1. Intranet — which provides IPSec-based tunnels between remote sites utilizing broadband or dedicated access.
2. Extranet — which enables trusted business partners to gain access to corporate information via IPSec tunnels utilizing broadband or dedicated access.
3. Remote Access — which enables mobile/remote workers to access secure corporate information via IPSec tunnels utilizing dial or broadband access.

### C.2.6.2.1.2 Standards

Premises-based VPNs shall comply with the following standards, as applicable, and when commercially available. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards.

1. Internet Engineering Task Force (IETF) RFCs
  - a. For secure VPNs
    - i. General IPSec
    - ii. ESP and AH
    - iii. Key exchange
    - iv. Cryptographic algorithms
    - v. IPSec policy handling
    - vi. IPSec MIBs
    - vii. Remote access
    - viii. Certificate Authorities
  - b. For trusted VPNs
    - i. General MPLS
2. IP Security Working Group
3. IP Security Policy Working Group
4. MPLS Working Group
5. Layer 3 Virtual Private Network (L3VPN) Working Group
6. Pseudo Wire Emulation Edge to Edge (pwe3) Working Group
7. IETF-TLS Working Group
8. SSL Protocol Specification compliant with FIPS 140-2

9. IETF RFCs for IPv6 when offered commercially by the contractor
10. All new versions, amendments, and modifications made to the above listed documents and standards, when offered commercially.

#### **C.2.6.2.1.3 Connectivity**

Premises-based IP VPNs shall connect Government locations and trusted business partners via dial-up, broadband, or leased line for site-to-site or remote access.

#### **C.2.6.2.1.4 Technical Capabilities**

The following premises-based IP VPNs capabilities are mandatory unless marked optional:

1. The contractor shall provide multiple tunneling standards, as required by an Agency. Examples include L2TP, GRE, IPSec, and SSL/TLS.
2. The contractor shall provide various encryption levels, as required by an Agency. Examples include 3DES, RC4 (optional), and AES, in accordance with the appropriate FIPS publications and modules.
3. The contractor shall provide authentication services as required by an Agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
4. Reserved
5. The contractor shall provide access flexibility by supporting various access methods including dedicated access and at least one of the following:
  - a. DSL
  - b. Local ISPs
  - c. Cable high speed access
6. The contractor shall provide fast dial access connectivity at either of the following speeds:
  - a. 56 kbps
  - b. 128 kbps.
7. The contractor shall provide layered security architecture to ensure that attackers will not find a single point of entry and instead will be challenged with multiple levels of security.
8. The contractor shall provide proactive, around-the-clock management of the premises-based IP VPN. The contractor shall also provide Agencies with administrative tools to view the topology, operational state, order status, and other parameters associated with each VPN.
9. The contractor shall provide network design and engineering service to provide bandwidth and CPE design as part of the standard service. The total solution shall be engineered and integrated into the Agency's premises network infrastructure.
10. The contractor shall provide secure routing services to provide full routing capability on the VPN platform with secure, centralized policy across the VPN.

11. The contractor shall provide traffic management service to allow an Agency's VPN administrators to classify some packets for preferential treatment or QoS.

#### C.2.6.2.2 Features

The Premises-based IP VPN features delineated in Section C.2.7.2.2.1 are mandatory unless marked optional.

##### C.2.6.2.2.1 Premises-based IP VPN Features

ID Number	Name of Feature	Description
1	High availability options for CPE	The contractor shall provide the high availability options: <ol style="list-style-type: none"> <li>1. Fault tolerance</li> <li>2. Load sharing</li> <li>3. Fail-over protection</li> <li>4. Diverse access points to service provider's POP(s).</li> </ol>
2	Internet Gateway Service	The contractor shall provide controlled and monitored connections between the IP-VPN service and the Internet via a hardened trusted gateway.
3	Interworking services	If the following services are offered, the contractor shall provide interworking services for an Agency's IP VPN to transparently access Agency locations that use the following: <ol style="list-style-type: none"> <li>1. The contractor's ATMS</li> <li>2. The contractor's FRS</li> <li>3. The contractor's Ethernet Service (Optional)</li> <li>4. The contractor's IPS.</li> </ol>
4	Key Management	The contractor shall provide the capability to set up VPN meshes and manage encryption keys owned by the following: <ol style="list-style-type: none"> <li>1. Contractor</li> <li>2. Government Agency</li> </ol> Key management can be defined as the generation, distribution, storage, and security of keys. An Agency may decide to be responsible for the key generation and outsource the rest of the key management task.
5	Security services	The contractor shall provide the following capabilities, as required: <ol style="list-style-type: none"> <li>1. Managed stateful firewall services</li> <li>2. Network scanning service</li> <li>3. Managed Intrusion Detection service</li> <li>4. Denial of Service (DoS) protection</li> <li>5. Network Address Translation</li> <li>6. Port Address Translation</li> </ol> Defenses should be inherent to product design rather than software upgrades to a non-secure platform.

### C.2.6.2.3 Interfaces

The User-to-Network-Interfaces (UNI) at the SDP, as defined in Section C.2.7.2.3.1 for Intranet and Extranet VPNs are mandatory, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage unless marked optional.

#### C.2.6.2.3.1 Interface for Intranet and Extranet Premises-based IP VPNs

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Ethernet Interface	1. 1 Mbps up to 1 GbE (Gigabit Ethernet) 2. 10 GbE (Optional)	IPv4/v6 over Ethernet

Notes:

1. IPv6 shall be supported when offered commercially by the contractor.
2. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

The User-to-Network-Interfaces (UNI) at the SDP, as defined in Section C.2.7.2.3.2 for Remote Access VPNs are mandatory, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage, unless marked optional.

#### C.2.6.2.3.2 Interface for Remote Access Premises-based IP VPNs

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Voice Service	Analog dialup at 56 Kbps	Point-to-Point Protocol, IPv4/v6
2	DSL Service	xDSL access at 1.5 to 6 Mbps downlink, and 384 Kbps to 1.5 Mbps uplink	Point-to-Point Protocol, IPv4/v6
3	Cable high speed access	320 kbps up to 10 Mbps	Point-to-Point Protocol, IPv4/v6
4 (Optional)	Multimode/Wireless LAN Service	See Section C.2.14.3.3.1 MWLANS User-to-Network Interfaces	
5 (Optional)	Wireless Access	See Section C.2.16.2.3.3.1 Wireless Access Arrangement Interfaces	
6 (Optional)	Satellite Access	See Section C.2.16.2.4.3.1 Satellite Access Arrangement Interfaces	
7	Circuit Switched Data Service	1. ISDN at 64 Kbps 2. ISDN at 128 Kbps 3. ISDN dial backup at 64 Kbps 4. ISDN dial backup at 128 Kbps	Point-to-Point Protocol, IPv4/v6

Notes:

1. IPv6 shall be supported when offered commercially by the contractor.

- Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

**C.2.6.2.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Premises-based IP VPNs in Section C.2.7.2.4.1 are mandatory unless marked optional.

**C.2.6.2.4.1 Performance Metrics for Premises-based IP VPNs**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(VPN)	Routine	99.9%	≥ 99.9%	See Note 1
Latency (CONUS)	Routine	120 ms	≤ 120 ms	See Note 2
Latency (OCONUS)	Routine	300 ms	≤ 300 ms	See Note 3
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

- VPN availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the VPN is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(VPN) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

- Latency value is the average round trip transmission between Agency premise routers for an IP VPN with all of its CONUS sites. Latency metric does not apply for the access methods (UNI Types 1-7) in C.2.7.2.3.2.. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the Government more cost effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
- Latency value is the average round trip transmission between Agency premise routers for an IP VPN with its CONUS and OCONUS sites. Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the Government more cost effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
- See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.6.3 Network-based IP VPN Services (NBIP-VPNS)**

The contractor's Network-based IP VPN provides secure, reliable transport of Agency applications across the provider's high-speed unified multiservice IP-enabled backbone infrastructure.

Verizon's Independent and Embedded Analog and ISDN Dial-up Services referenced under the Functional Definition, Connectivity, Technical Capabilities, and Interface sections of C.2.7.3 were previously offered under Networx, but are now discontinued effective 07/31/2013, in accordance with Networx Contract Section C.2.1.1.

### **C.2.6.3.1 Service Description**

#### **C.2.6.3.1.1 Functional Definition**

The main characteristic of a Network-based VPN is that all devices involved in building the VPN are systems owned by the contractor and located at the edge of the contractor's backbone. Tunnels usually will terminate at the contractor's edge-router. The contractor utilizes its backbone to establish three basic solutions for Network-based IP VPNs:

1. Intranet – which provides secure tunnels between remote sites, utilizing broadband or dedicated access.
2. Extranet – which enables trusted business partners to gain access to corporate information via secure/encrypted tunnels, utilizing broadband or dedicated access.
3. Remote Access – which enables mobile/remote workers to gain access to secure corporate information via secure encrypted tunnels, utilizing dial, broadband, or dedicated access.

#### **C.2.6.3.1.2 Standards**

Network-based VPNs shall comply with the following standards, as applicable, and when commercially available. After award, the contractor may propose alternative at no additional cost to the Government that meet or exceed the provisions of the listed standards.

1. Internet Engineering Task Force (IETF) RFCs
  - a. For secure VPNs
    - i. General IPsec
    - ii. ESP and AH
    - iii. Key exchange
    - iv. Cryptographic algorithms
    - v. IPsec policy handling
    - vi. IPsec MIBs
    - vii. Remote access
    - viii. Certificate Authorities
  - b. For trusted VPNs
    - i. General MPLS
2. IP Security Working Group

3. IP Security Policy Working Group
4. MPLS Working Group
5. Layer 3 Virtual Private Network (L3VPN) Working Group
6. Pseudo Wire Emulation Edge to Edge (pwe3) Working Group
7. Use of PE-PE GRE or IP in RFC2547 VPNs
  - a. draft-ietf-l3vpn-gre-ip-2547-00.txt
8. Reserved
9. IETF-TLS Working Group
10. SSLv3 Protocol Specification
11. IETF RFCs for IPv6 when offered commercially by the contractor
12. All new versions, amendments, and modifications to the above documents and standards commercially available.

#### **C.2.6.3.1.3 Connectivity**

Network-based IP VPNs shall connect Government locations and trusted business partners via leased lines for site-to-site access or via dial or broadband for remote access to provide direct connectivity between all sites as a partial or fully meshed WAN.

#### **C.2.6.3.1.4 Technical Capabilities**

The following network-based IP VPN capabilities are mandatory, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage, unless marked optional:

1. The contractor shall provide multiple tunneling standards, as required by an Agency. Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and SSL/TLS.
2. The contractor shall provide various encryption levels, as required by an Agency. Examples include 3DES, RC4 (optional), and AES in accordance with the appropriate FIPS publications and modules.
3. The contractor shall provide authentication services as required by an Agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
4. Reserved.
5. The contractor shall support IPv4 as both the encapsulating and encapsulated protocol.
6. The contractor shall support IPv6 as both the encapsulating and encapsulated protocol, when offered commercially by the contractor.
7. The contractor shall support QoS in one or more of the following standardized mode



- a. Best effort
  - b. Aggregate Customer Edge (CE) Interface level QoS (“hose” level)
  - c. Site-to-site level QoS (“pipe” level)
  - d. Intserv (RSVP) signaled
  - e. Diffserv marked.
8. Reserved.
9. The contractor shall support QoS across a subset of the access networks as listed below, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage.
- a. ATM Virtual Connections (VCs)
  - b. Frame Relay Data Link Connection Identifiers (DLCIs)
  - c. 802.1p Prioritized Ethernet
  - d. MPLS-based access
  - e. Multilink Multiclass PPP
  - f. QoS-enabled wireless
    - i. LMDS
    - ii. MMDS
  - g. Cable high speed access (DOCSIS 1.1) (Optional)
  - h. QoS-enabled Digital Subscriber Line (DSL) (Optional)
  - i. QoS-enabled Satellite Broadcast Access (Optional)
10. The contractor shall support one or more of the following application level QoS objectives, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage:
- a. Intserv model for selected individual flows
  - b. Diffserv model for aggregated flows.
11. The contractor shall provide access flexibility by supporting various access methods, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage, including but not limited to:
- a. DSL
  - b. Local ISPs
  - c. Cable high speed access (Optional)
  - d. Dedicated
  - e. Satellite broadband (Optional)
12. The contractor shall support fast dial access connectivity at either of the following
- a. 56 Kbps
  - b. 128 Kbps.
13. Reserved

14. The contractor shall provide isolation of traffic and routing service that isolates the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN.
15. The contractor shall provide layered security architecture to ensure that attackers will not find a single point of entry but will be faced with multiple levels of security.
16. The contractor shall provide proactive, around-the-clock management of the network-based IP VPN. The contractor shall also provide Agencies with administrative tools to view the topology, operational state, order status, and other parameters associated with each VPN.
17. The contractor shall provide mobile user support via client or other devices as follows:
  - a. The contractor shall allow mobile users to move within a VPN site.
  - b. Mobile users may also temporarily connect to another VPN site within the same VPN.
  - c. Authentication shall be provided for both of these cases.
18. The contractor shall support multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies.
19. The contractor shall provide network design and engineering service to provide bandwidth and CPE design as part of the standard service. The total solution is engineered and integrated into an Agency's premises network infrastructure.
20. (Optional) The contractor's network shall provide near real-time response to dynamic requests from the customer, for changes to adjust allocated bandwidth.
21. The contractor shall provide secure routing services to provide full routing capability on the VPN platform with secure, centralized policy across the VPN.
22. The contractor shall support the inclusion of encryption, decryption, and key management profiles as part of the security management system.
23. The contractor shall support an Agency deploying their own internal security mechanisms in addition to those deployed by the contractor, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.
24. The contractor shall allow an Agency to choose from alternatives for authentication of temporary access users. Authentication server choices include
  - a. Contractor provided
  - b. Third party
  - c. Agency provided

#### **C.2.6.3.2 Features**

The Network-based IP VPN features delineated in Section C.2.7.3.2.1 are mandatory unless marked optional:

### C.2.6.3.2.1 Network-based IP VPN Features

ID Number	Name of Feature	Description
1	Class of Service (CoS)	<p>The contractor shall accommodate and optimize an Agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies.</p> <p>The Classes of Service or prioritization levels may be categorized as:</p> <ol style="list-style-type: none"> <li>1. Premium – for time-critical traffic such as voice and video</li> <li>2. Enhanced – for business-critical traffic such as transactions</li> <li>3. Standard – for non-critical traffic such as email.</li> </ol>
2	High availability options for CPE	<p>The contractor shall provide the following high availability options:</p> <ol style="list-style-type: none"> <li>1. Fault tolerance</li> <li>2. Load sharing</li> <li>3. Fail-over protection</li> <li>4. Diverse access points to service provider's POP(s).</li> </ol>
3	Internet Gateway Service	<p>The contractor shall provide controlled and monitored connections between the IP-VPN service and the Internet via a hardened trusted gateway.</p>
4	Interworking services	<p>If the following services are offered, the contractor shall provide interworking services for an Agency's IP VPN to transparently access Agency locations that use the following:</p> <ol style="list-style-type: none"> <li>1. The contractor's ATMS</li> <li>2. The contractor's FRS</li> <li>3. The contractor's Ethernet Service (Optional)</li> <li>4. The contractor's IPS.</li> </ol>
5	Key Management	<p>The contractor shall provide the capability to set up VPN meshes and manage encryption keys owned by the following:</p> <ol style="list-style-type: none"> <li>1. Contractor</li> <li>2. Government Agency.</li> </ol> <p>Key management can be defined as the generation, distribution, storage, and security of keys. An Agency may decide to be responsible for the key generation and outsource the rest of the key management task.</p>
6 (Optional)	Non-peered Private IP Network	<p>The contractor shall provide the capability to run an Agency's VPN service over transport that is not connected to the public Internet and allows separation of Agency traffic from any other Agency's traffic. This network shall enforce physical and logical separation of an Agency's traffic.</p>

ID Number	Name of Feature	Description
7	Security services	<p>The contractor shall provide the following capabilities, as required:</p> <ol style="list-style-type: none"> <li>1. Carrier grade managed stateful firewall services</li> <li>2. Network scanning service</li> <li>3. Managed Intrusion Detection service</li> <li>4. Denial of Service (DoS) protection</li> <li>5. Network Address Translation</li> <li>6. Port Address Translation</li> <li>7. Edge-to-edge encryption</li> <li>8. Replay attack protection</li> </ol> <p>Defenses should be inherent to product design rather than software upgrades to a non-secure platform.</p>

### C.2.6.3.3 Interfaces

The User-to-Network-Interfaces (UNI) at the SDP, as defined in Section C.2.7.3.3.1 for Intranet and Extranet VPNs are mandatory unless marked optional.

#### C.2.6.3.3.1 Interface for Intranet and Extranet Network-based IP VPNs

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 2)
1	Ethernet Interface	<ol style="list-style-type: none"> <li>1. 1 Mbps up to 1 GbE (Gigabit Ethernet)</li> <li>2. 10 GbE (Optional)</li> </ol>	IPv4/v6 over Ethernet
2	Private Line Service	<ol style="list-style-type: none"> <li>1. DS0</li> <li>2. Fractional T1</li> <li>3. T1</li> <li>4. T3</li> <li>5. Fractional T3</li> <li>6. OC-3c (Optional)</li> <li>7. OC-12c (Optional)</li> <li>8. OC-48c (Optional)</li> <li>9. OC-192c (Optional)</li> </ol>	IPv4/v6 over PLS
3	IP over SONET Service (Optional)	<ol style="list-style-type: none"> <li>1. OC-3c</li> <li>2. OC-12c</li> <li>3. OC-48c</li> <li>4. OC-192c</li> </ol>	IP/PPP over SONET

#### Notes:

1. Reserved
2. IPv6 shall be supported when offered commercially by the contractor.
3. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

The contractor shall provide at least one of the User-to-Network-Interfaces (UNI) at the SDP, as defined in Section C.2.7.3.3.2 below for Remote Access VPNs, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage, unless marked optional.

#### C.2.6.3.3.2 Interface for Remote Access Network-based IP VPNs

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Voice Service	Analog dialup at 56 kbps	Point-to-Point Protocol, IPv4/v6
2	DSL Service	xDSL access at 1.5 to 6 Mbps downlink, and 384 Kbps to 1.5 Mbps uplink	Point-to-Point Protocol, IPv4/v6
3	Cable high speed access	320 Kbps up to 10 Mbps	Point-to-Point Protocol, IPv4/v6
4 (Optional)	Multimode/Wireless LAN Service	See Section C.2.14.3.3.1 MWLANs User-to-Network Interfaces	
5 (Optional)	Wireless Access	See Section C.2.16.2.3.3.1 Wireless Access Arrangement Interfaces	
6 (Optional)	Satellite Access	See Section C.2.16.2.4.3.1 Satellite Access Arrangement Interfaces	
7	Circuit Switched Data Service	<ol style="list-style-type: none"> <li>1. ISDN at 64 Kbps</li> <li>2. ISDN at 128 Kbps</li> <li>3. ISDN dial backup at 64 Kbps</li> <li>4. ISDN dial backup at 128 Kbps</li> </ol>	Point-to-Point Protocol, IPv4/v6

Notes:

1. IPv6 shall be supported when offered commercially by the contractor.
2. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

#### C.2.6.3.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for Network-based IP VPNs in C.2.7.3.4.1 below are mandatory unless marked optional.

##### C.2.6.3.4.1 Performance Metrics for Network-based IP VPNs

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Latency (CONUS)	Routine	70 ms	≤ 70 ms	See Note 1
Latency (OCONUS)	Routine	150 ms	≤ 150 ms	See Note 2

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(VPN)	Routine	99.9%	≥ 99.9%	See Note 3
	Critical (Optional)	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Latency value is the average round trip transmission between Agency premise routers for an IP VPN with all of its CONUS sites. Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the Government more cost effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
2. Latency value is the average round trip transmission between Agency premise routers for an IP VPN with its CONUS and OCONUS sites. Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the Government more cost effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
3. VPN availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the VPN is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(VPN) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

4. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.6.4 Managed Tiered Security Services (MTSS)**

The General Services Administration (GSA) Federal Technology Service (FTS) has identified the requirement to increase security in the services being delivered to customer Agencies. The Multi Tier Security Profiles (MTSP) initiative was developed to meet this requirement. MTSP provides four baseline levels (Tier 1 through Tier 4) of embedded security, which can be tailored to individual customer needs contingent on the respective levels of mission criticality and information sensitivity. Figure C.2.7.4-1 illustrates the MTSP architecture. The performance level of the basic transport and/or service being contracted by the Government Agency shall not be degraded by the MTSP enhancements.

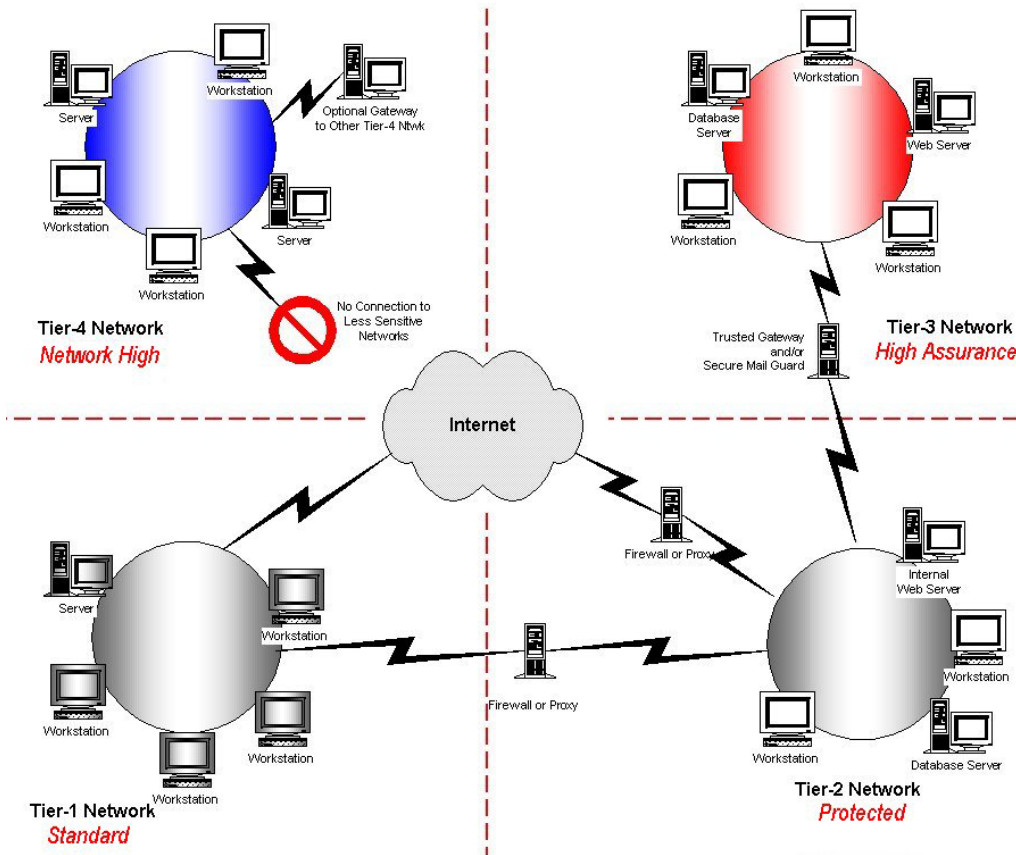


Figure C.2.7.4-1. MTSP Notional Architecture

**C.2.6.4.1 Service Description**

The combined Security Profiles under MTSS can facilitate the purchasing of standard baseline or customized security services across multiple tiers.

**C.2.6.4.1.1 Functional Definition**

MTSS provides Agencies with any of the four security levels, or tiers, of embedded security in the MTSP architecture. A functional description of each of the four tiers is provided. For all tiers, the help desk service includes the human resources required to perform all required functions.

**C.2.6.4.1.1.1 MTSP Tier 1 – Standard Service**

MTSP Tier 1 – Standard service supports basic Internet connectivity and is appropriate for non-mission critical functions or non-sensitive communications. The Agency will identify and implement all security features. The contractor shall provide Agency

dedicated help desk capabilities on a 24 hour/7 day basis for all issues concerning service delivery.

#### **C.2.6.4.1.1.2 MTSP Tier 2 – Protected Service**

MTSP Tier 2 – Protected service shall include all the security components of Tier 1. Protected service shall provide security enhancements to the subscribing Agency with additional protection from unauthorized activities and the proliferation of malicious code. Protected service shall also mitigate the potential for Denial of Service (DOS) attacks. Security enhancements include a combination of firewall, premises-based virtual private network (encrypted tunnels), filtering router, proxy server, and boundary anti-virus detection technologies configurable to the subscribing Agency's security policy(s) and specifications.

Tier 2 is tailored to Sensitive but Unclassified (SBU) mission functions and information. It employs both technical and network management components appropriate to the respective mission and/or information sensitivity.

#### **C.2.6.4.1.1.3 MTSP Tier 3 – High Assurance Service [Optional]**

MTSP Tier 3 – High Assurance service shall include all the security enhancements of Tier 2 and is tailored to protect extremely sensitive information up to and including National Security Information (NSI) that has been classified pursuant to Executive Order 12958 or its successor such as *Secret* mission functions and information. Typical users include Federal law enforcement Agencies, counter-terrorism practitioners, cyber incident response teams, inter-Agency collaborators and special communities of interest.

A Tier 3 enclave shall not connect to the Internet except via a Tier 2 enclave and its associated security enhancements. Connection to a Tier 2 enclave shall only be made via a National Security Agency (NSA) approved trusted gateway, secure mail guard technologies, or other NSA approved multilevel security solution.

#### **C.2.6.4.1.1.4 MTSP Tier 4 – Network High Service [Optional]**

MTSP Tier 4 – Network High service is for unique and highly sensitive telecommunication requirements typically categorized as "Special Category." This service is ideally suited to protect critical functions while ensuring the highest levels of performance, survivability, and resistance to external compromise.

Tier 4 services are tailored to meet general and national level guidance for the processing of NSI classified functions such as Top Secret, Sensitive Compartmented Information (SCI) and Single Integrated Operational Plan – Extremely Sensitive Information (SIOP-ESI). A Tier 4 enclave shall not connect to a lesser sensitive enclave and shall be completely isolated from publicly accessible networks such as the Internet.

#### **C.2.6.4.1.2 Standards**

MTSS shall comply with the following standards and government guidelines, as applicable, and when commercially available. After award, the contractor may propose



alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards.

1. NIST Federal Information Processing Standards Publication (FIPS) PUB 140 - 2 — Security Requirements for Cryptographic Modules
2. NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems (Pre-Publication Final)
3. NIST Special Publications (SP) 800-12 — An Introduction to Computer Security: The NIST Handbook
4. NIST SP 800-14 — Generally Accepted Principles and Practices for Securing Information Technology Systems
5. NIST SP 800-18 Revision 1— Guide for Developing Security Plans for Information Technology Systems
6. NIST SP 800-23 — Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
7. NIST FIPS PUB 200, NIST SP 800-53 Revision 3 and NIST SP 800-53A
8. NIST SP 800-30 — Risk Management Guide for Information Technology Systems
9. NIST SP 800-94 – Guide to Intrusion Detection and Prevention Systems (IDPS).
10. NIST SP 800-34 Revision 1– Contingency Planning Guide for Federal Information Systems
11. NIST SP 800-35 — Guide to Information Technology Security Services
12. NIST SP 800-36 — Guide to Selecting Information Technology Security Products
13. NIST SP 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach .
14. NIST SP 800-40 — Creating a Patch and Vulnerability Management Program
15. NIST SP 800-41 — Guidelines on Firewalls and Firewall Policy
16. NIST SP 800-115 – Technical Guide for Information Security Testing and Assessment
17. NIST SP 800-45 — Guidelines on Electronic Mail Security
18. NIST SP 800-46— Security for Telecommuting and Broadband Communications
19. NIST SP 800-47 — Security Guide for Interconnecting Information Technology Systems
20. NIST SP 800-48 — Guide to Securing Legacy IEEE 802-11 Wireless Networks
21. NIST SP 800-50 — Building an Information Technology Security Awareness and Training Program
22. NIST SP 800-51 — Guide to Using Vulnerability Naming Schemes

23. NIST SP 800-53 — Revision 3 – Recommended Security Controls for Federal Information Systems and Organizations
24. NIST SP 800-55 — Performance Measurement Guide for Information Security
25. NIST SP 800-61 – Computer Security Incident Handling Guide
26. NIST SP 800-61 — Draft Computer Security Incident Handling Guide
27. NIST SP 800-64 — Security Considerations in the Information System Development Life Cycle
28. NSA Standards for handling of information classified NSI
29. NIACAP (NSTISSI 1000) — National Information Assurance Certification and Accreditation Process
30. DIACAP (DoDI 8510.01) Defense Information Assurance Certification and Accreditation Process
31. E-Government Act of 2002. Title III (Federal Information Security Management Act (FISMA))
32. T1.276-2003 American National Standard for Telecommunications — Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane
33. All commercially available standards for any applicable underlying access and transport services
34. All new versions, amendments, and modifications made to the above listed documents and standards, when applicable and offered commercially.

#### **C.2.6.4.1.3 Connectivity**

##### **C.2.6.4.1.3.1 MTSP Tier 1 – Standard Service**

MTSP Tier 1 – Standard service shall apply to Agency locations and network services that are connected directly to the Internet (via Agency installed security mechanisms).

**C.2.6.4.1.3.2 MTSP Tier 2 – Protected Service**

MTSP Tier 2 – Protected service shall apply to Agency locations that include Agency LANs/MANs/WANs with various underlying access, transport, and network services and which are connected to the Internet or Tier 1 networks via the security enhancements delineated in Section C.2.7.4.1.1.2 MTSP Tier 2 – Protected Service

**C.2.6.4.1.3.3 MTSP Tier 3 – High Assurance Service [Optional]**

MTSP Tier 3 – High Assurance service shall apply to Agency and Agency specified LANs/MANs/WANs with various underlying access, transport, and network services that operate in a “quasi-closed” network environment. Connectivity to Tier 2 enclaves shall only be made via NSA approved trusted gateways, secure mail guard technologies, or other NSA approved multilevel security solution. A Tier 3 enclave shall not have a direct connection to the Internet.

**C.2.6.4.1.3.4 MTSP Tier 4 – Network High Service [Optional]**

MTSP Tier 4 – Network High service shall apply to Agency and Agency specified LANs/MANs/WANs with various underlying access, transport, and network services that operate in a closed and isolated network environment. This service may provide connectivity among other Tier 4 enclaves within a community of interest.

**C.2.6.4.1.4 MTSP Security Enhancement Matrix**

The security enhancement services that are identified by checkmarks for the different MTSP Tiers as listed in Section C.2.7.4.1.4.1 below are mandatory unless marked optional. MTSP Tiers 3 and 4 are optional.

**C.2.6.4.1.4.1 MTSP Security Profile Technical Capabilities Matrix**

Security Enhancement Services	TIER			
	1	2	3	4
Agency Sponsored Type 1 Encryption			✓	✓
Anti-virus		✓	✓	✓
Firewall		✓	✓	✓
Agency Dedicated Help Desk	✓	✓	✓	✓
Intrusion Detection/Prevention		✓	✓	✓
Incident Response		✓	✓	✓
Network Isolation (Air Gap)				✓
NSA Approved Multilevel Security Solution			✓	✓
Packet Filtering		✓	✓	✓
Premises-based Virtual Private Network (VPN)		✓	✓	✓
Proxy Server		✓	✓	
Secure Managed Email		✓	✓	✓
Security Certification Support		✓	✓	✓
Security Maintenance		✓	✓	✓
Vulnerability Scanning		✓	✓	✓

The security enhancement services are specified in Section C.2.7.4.1.5.

**C.2.6.4.1.5 Technical Capabilities**

MTSS shall support the following capabilities as they apply to the matrix in Section C.2.7.4.1.4.1:

1. Agency Sponsored Type 1 Encryption Service [Optional]
  - a. The contractor shall provide and manage NSA approved Type 1 (hardware) encryption devices, through Agency sponsorship.
  - b. The contractor shall limit the end-to-end path latency to ensure that cryptographic equipment synchronization is maintained.
  - c. The contractor shall provide key management.
2. Anti-virus Service
  - a. The contractor shall provide Anti-virus Service. See Section C.2.10.4 Anti Virus Management Service (AVMS).
3. Firewall Service
  - a. The contractor shall provide Firewall Service. See Section C.2.10.1 Managed Firewall Service (MFS).
4. Agency Dedicated Help Desk Service
  - a. The contractor shall establish a single point-of-presence help desk capability for all issues concerning service delivery 24x7.
  - b. The contractor shall maintain a trouble detection and reporting system allowing the diagnosis and resolution of service delivery problems.
  - c. The contractor shall proactively detect problems and open trouble tickets.
  - d. The contractor shall provide notification of events including alarms, network troubles, and service interruptions via email, pager, fax, telephone, as directed by the Agency's notification procedures.
  - e. The contractor shall provide the Agency secure Web Portal access to realtime network management information for visibility into service delivery activities.
  - f. The contractor shall provide access to reports as directed by the Government Contracting Officer's Representative (COR).
  - g. The contractor shall retain log files and reports as required by the user Agency.
5. Intrusion Detection/Prevention Service
  - a. The contractor shall provide Intrusion Detection and Prevention Service. See Section C.2.10.2 Intrusion Detection and Prevention Service (IDPS).
6. Incident Response Service [Optional]
  - a. The contractor shall provide Incident Response Service. See Section C.2.10.5 Incident Response Service (INRS).

7. Network Isolation (Air Gap) — Air Gap requirements vary in concert with the mission application and information sensitivity [Optional]
  - a. The contractor shall provide absolute physical isolation from lesser sensitive networks.
8. NSA Approved Multilevel Security Solution, which includes, but is not limited to the following services. [Optional]
  - a. The contractor shall provide NSA Approved Secure Mail Guard Service
    - i. The contractor's solution shall provide the filters and logic to ensure the e-mail messages are approved for transfer between the security enclaves.
    - ii. The filters shall be configurable based on the security policy of the Tier 3 enclaves.
    - iii. The filters shall include the following:
      1. Sender/Recipient Address — Source and destination address of the Simple Mail Transfer Protocol (SMTP) message shall be included in a database of approved addresses
      2. Classification Label — The sender shall include text indicating the security classification of the message content(s)
      3. Attachment Type — Any attachments to the message shall be of a type approved by the filter
      4. Attachment Review — Verifies that attached files include a special tag and checksum indicating that the attachment was reviewed and approved
      5. Digital Signature — Verifies that the body of the message is formatted correctly and is signed using a digital signature and that the signature belongs to the authorized sender
      6. Encryption — Verifies that the body of the message is formatted correctly and is encrypted.
    - iv. Each e-mail and attachment shall successfully traverse all configured filters before the message is delivered to the destination recipient.
    - v. All improperly formatted e-mail shall be disallowed for transfer.
    - vi. The contractor's solution shall support enforcement of the Department of Defense (DoD) Mandatory Access Control (MAC) policy by limiting flows at different security levels to those that are consistent with the overall system policy.

- b. The contractor shall provide NSA Approved Trusted Gateway Service
    - i. The contractor's solution shall provide a secure one-way transfer of data from one network to another higher classification network.
    - ii. The contractor shall provide a DoD level of absolute information assurance incorporating auditing, authentication, non-repudiation, and forensics.
9. Packet Filtering Service
- a. The contractor shall provide routers to restrict packets to specific ports based on protocol specific criteria.
10. Premises-based VPN Service
- a. See Section C.2.7.2 Premises-based IP VPN Services (PBIP-VPNS).
11. Proxy Server Service [Optional]
- a. The contractor shall provide secure web proxy servers to shield a sensitive network enclave from an enclave of lesser sensitivity. Users on the more sensitive network, with the appropriate access levels, shall be able to securely browse the lesser sensitive domain (e.g. Internet).
12. Secure Managed Email Service [Optional]
- a. See Section C.2.10.8 Secure Managed Email Service (SMEMS).
13. Security Assessment and Authorization Support Service
- a. The contractor shall support the certification of all network systems and services provided to government Agencies in accordance with the following prescribed activities:
    - i. OMB Circular A-130 Appendix III — Management of Federal Information Resources
    - ii. NIACAP (NSTISSI 1000) — National Information Assurance Certification and Accreditation Process
    - iii. NIST SP 800-37 — Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    - iv. DIACAP (DoDI 8510.01) Defense Information Assurance Certification and Accreditation Process
    - v. Agency specific requirements for Security Assessment and Authorization
  - b. The contractor shall assist Agencies in the development and preparation of the following security documents:
    - i. Configuration Management (CM) Plan
    - ii. Risk Assessment (RA)

- iii. System Security Plan (SSP)
  - iv. Contingency Plan
  - v. Security Test & Evaluation (ST&E)
- c. The security assessment and authorization deliverables shall comply with all applicable federal laws, regulations, policies, guidelines, and standards.
14. Security Maintenance Service
- a. The contractor shall advise the Agency concerning control and elimination of the identified vulnerabilities.
  - b. The contractor shall provide post alarm support including analysis and interpretation of attack data.
  - c. The contractor shall perform configuration changes as initiated and prioritized by the Agency.
  - d. The contractor shall maintain all security systems, performing the necessary hardware/software upgrades, updates, and replacements.
  - e. The contractor shall deploy the latest patches and bug fixes as soon as they become available in order to ensure optimal performance of the service.
  - f. The contractor shall regularly perform off-site backups to ensure the availability of recent configurations for restoration purposes.
  - g. The contractor shall perform periodic security scans capable of revealing known vulnerabilities of the security system.
  - h. The contractor shall document the results of the scans, and the fixes applicable to the identified vulnerabilities.
  - i. The contractor shall support networks of varying complexity, in terms of size, bandwidth, and access speeds.
  - j. Log Review
    - i. The contractor shall review logs on a regular basis as defined by the Agency.
    - ii. The contractor shall analyze logs when related to specific security incidents and advise the Agency on appropriate actions to prevent subsequent incidents.
  - k. The contractor shall report computer security related incidents or suspicious activity to the United States Computer Emergency Readiness Team (US-CERT) per FISMA.
15. Vulnerability Scanning Service [Optional]
- a. See Section C.2.10.3 Vulnerability Scanning Service (VSS).

**C.2.6.4.2 Features**

**C.2.6.4.2.1 MTSP Feature Matrix**

The MTSS Features identified by checkmarks for the different MTSP Tiers listed in Section C.2.7.4.2.1.1 are mandatory unless marked optional.

**C.2.6.4.2.1.1 MTSP Security Profile Feature Matrix**

MTSS Features	TIER			
	1	2	3	4
On-site management and monitoring 24x7		✓	✓	✓
On-site installation		✓	✓	✓

The MTSS Features are specified in Section C.2.7.4.2.2

**C.2.6.4.2.2 MTSS Features**

ID Number	Name of Feature	Description
1	On-site Management and monitoring 24x7	The contractor shall provide proactive, around-the-clock management and monitoring of the service delivery functions. Agency shall be able to view the topology, operational state, order status, and other parameters associated with each contracted service.
2	On-site installation	The contractor shall provide on-site installation services as required by the Agency.

**C.2.6.4.3 Interfaces**

MTSS shall support the User-to-Network Interfaces (UNIs) defined in the following Sections, as applicable:

- a. C.2.3.1 Frame Relay Service (FRS) (Optional)
- b. C.2.3.2 Asynchronous Transfer Mode Service (ATMS) (Optional)
- c. C.2.4.1 Internet Protocol Services (IPS)
- d. C.2.5.1 Private Line Services (PLS) (Optional)
- e. C.2.5.2 Synchronous Optical Network Services (SONETS) (Optional)
- f. C.2.7.1 Ethernet Services (Eths) (Optional)
- g. C.2.7.2 Premises-based IP-VPN Services (PBIP-VPNs) (Optional)
- h. C.2.7.3 Network-based IP-VPN Services (NBIP-VPNS)

**C.2.6.4.3.1 Reserved**

**C.2.6.4.3.2 Reserved**



#### C.2.6.4.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for MTSS in Section C.2.7.4.4.1 below are mandatory unless marked optional, and are applicable to the specific Tier.

##### C.2.6.4.4.1 Performance Metrics for MTSS

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
<b>Grade of Service (GOS) (Configuration / Rule Change)</b>	Routine	Within 5 hours for Normal priority change	≤ 5 hours	See Note 1
		Within 2 hours for an Urgent priority change	≤ 2 hour	
<b>Event Notification</b>	Routine	Within 2 hours of a low category event	≤ 2 hours	See Note 2
		Within 5 minutes of a high category event	≤ 5 minutes	
<b>Av(Firewall)</b>	Routine	99.5% of the time	≥ 99.5%	See Note 3
<b>HELPER DESK</b> <b>EN(Outage Notification to Customer)</b>	Routine	Within 2 hours of a low category event	≤ 2 hours	See Note 4
		Within 5 minutes of a high category event	≤ 5 minutes	
<b>GOS(Percentage of Calls Abandoned)</b>	Routine	3%	≤ 3%	See Note 5
<b>Response Time</b>	Routine	All incoming calls to the Help Desk shall be answered on or before the fifth ring	≤ 5 rings	See Note 6
<b>Av(Multilevel Security Solution) NSA Approved</b>	Routine	100% of the time	100%	See Note 7
<b>Av(Type 1 Encryption)</b>	Routine	99.99% of the time	99.99%	See Note 8
<b>Av(Web Portal)</b>	Routine	99.7% of the time	≥ 99.7%	See Note 9
<b>EN(Security Incident Reporting)</b>	Routine	Near real time	≤ 1 hour	See Note 10

Notes:

1. The GOS(Configuration/Rule Change) value represents the elapsed time between the change request and the change completion. The value is measured by logs/reporting. The changes are initiated and prioritized by the Agency. Changes are categorized as Normal and Urgent (Emergency).
2. The Event Notification value is measured via event/reporting logs. It represents the elapsed time between the detection of the problem and the Agency's notification.
  - a. Low — Events in the Low category do not severely impact service. They include security incidents that do not significantly affect network security. They also include minor hardware, software and configuration problems. They are incorporated in reports available to the Agency.
  - b. High — Events in the High category represent security violations that seriously impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software, and configuration problems, and are immediately reported via email, pager, telephone, etc., as specified by the Agency.

3. Firewall availability is calculated as a percentage of the total reporting interval time that the firewall is operationally available to the Agency. Availability is

$$Av(\text{Firewall}) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

computed by the standard formula:

4. The contractor shall notify key Agency contacts of any service related issue that the Agency may experience.
5. This measurement is the percentage of calls in which the caller disconnects before an analyst or an automated answering system picks up. The measurement is a monthly aggregate and average by site of the percentage of abandoned calls at the Help Desk.
6. Response time is the number of rings before connection to a technician or an automatic answer to voice menus. The measurement is an aggregate of the response time via phone at the Help Desk. The utilized Help Desk software shall permit monitoring of the time between initial ring and call pickup.
7. NSA Approved Multilevel Security Solution availability is calculated as a percentage of the total reporting interval time that the MLSS is operationally available to the Agency. Availability is computed by the standard formula:  
$$Av(\text{Multilevel Security Solution}) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
8. Type 1 Encryption availability is calculated as a percentage of the total reporting interval time that the Type 1 Encryption device is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(\text{Type1 Encryption}) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

9. Web Portal availability is calculated as a percentage of the total reporting interval time that the web portal is operationally available to the Agency. Availability is

$$Av(\text{Web Portal}) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

computed by the standard formula:

10. Security incident reporting to US-CERT must be performed in near real time, from the time of detection not to exceed 1 hour.

#### **C.2.6.5 Reserved**

#### **C.2.6.6 Reserved**

#### **C.2.6.7 Reserved**

#### **C.2.6.8 Voice Over Internet Protocol Transport Services (VOIPTS)**

Voice over Internet Protocol Transport Service (VOIPTS) provides real time transmission of voice communications as data packets on the contractor's managed Internet Protocol (IP) network.

The following sections provide the requirements for VOIPTS.

##### **C.2.6.8.1 Service Description**

###### **C.2.6.8.1.1 Functional Definition**

Voice over Internet Protocol Transport Service provides real time transport of Agency voice communications over the contractor's IP network and interoperates with the PSTN. VOIPTS shall allow voice calls, originating from on-net locations to be connected to on-net and off-net locations by direct dialing.

###### **C.2.6.8.1.2 Standards**

Voice over Internet Protocol Transport Service shall conform to the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Internet Engineering Task Force (IETF) RFC's 3761 (ENUM), 3966
2. Internet Protocol (IP) IPv4. IPv6 when and where offered commercially by the contractor
3. IETF RFC 2474,2475 DiffServ
4. ITU-T E.164 as interpreted by the Industry Number Committee of Alliance for Telecommunications Industry Solutions (ATIS)
5. ITU-T G.711

6. ITU-T G.723.x [Optional], G.726 [Optional], G.728 [Optional], or G.729.x [Optional]
7. ITU-T H.248.1 (MEGACO), H.323, H.350 when and where offered commercially by the contractor
8. ITU-T P.800 series of standards for telephone transmission quality
9. ITU-T T.30, T.37 and T.38, Group III fax
10. Media Gateway Control Protocol (MGCP) IETF RFC 3435 when and where offered commercially by the contractor
11. IETF RFC 3550 Real-Time Transport Protocol (RTP)
12. IETF RFC 2205 Resource Reservation Protocol (RSVP)
13. IETF RFC 3261 SIP (Session Initiation Protocol) when and where offered commercially by the contractor
14. IETF RFC 768 User Datagram Protocol (UDP)
15. Reserved
16. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

#### **C.2.6.8.1.3 Connectivity**

Voice over Internet Protocol Transport Service shall connect to and interoperate with the Public Switched Telephone Network (PSTN) including both wireline and wireless networks, in domestic and non-domestic locations.

#### **C.2.6.8.1.4 Technical Capabilities**

The following Voice over Internet Protocol Transport Service capabilities are mandatory:

1. The contractor's VOIPTS shall enable Agency subscribers to successfully establish and receive telephone calls between on net locations and originate calls to off-net locations.
2. The contractor shall enable a routing prioritization scheme or class of service to distinguish between IP services. Time sensitive VOIPTS packets shall be assigned a higher priority than non-time sensitive services to mitigate potential call quality issues.
3. The contractor shall provide the following minimum capabilities:
  - a. The contractor shall provide real time transport of voice, facsimile, and TDD traffic.
  - b. The contractor shall provide real time transport and delivery of caller ID (ANI) when provided from the originating calling party's service provider.
  - c. The contractor's VOIPTS shall interoperate with public network dial plans.

- d. The contractor's VOIPTS shall interoperate with private Agency network dial plans.
4. A VOIPTS gateway enables interworking between voice over IP packet switched networks and non-IP networks and devices. The contractor shall provide gateways for interoperability with the contractors VOIPTS and the PSTN or Agency UNI's. The specific gateway will depend upon the subscribing Agency's UNI requirements. The gateways and functionality are described below:
  - b. Access Gateway – Provides transparent access to Agency's Local Wide Area Network (WAN) connection. It shall provide an Ethernet UNI port to connect with Agency equipment.
  - c. Trunking Gateway – Provides transparent access and interoperability between the IP network and Agency's Time Division Multiplexing (TDM) based equipment (PBX's, etc). It shall provide both analog and digital trunk UNI's to the Agency's TDM equipment.
  - d. PSTN Gateway – Provides transparent access to and interwork with the domestic and international Public Switched Telephone Network (PSTN).
5. The contractor shall provide a transparent, flexible alternate routing capability (overflow and failover routing) to allow calls to route off-net ("hop off") from the VOIPTS network to the PSTN if the VOIPTS is unavailable.
6. The contractor's VOIPTS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.
7. The contractor shall provide a secure web site to access both historical and real time VOIPTS performance and management reports.
8. The contractor shall state the minimum and optimal requirements for Agency owned voice equipment (such as PBX's or other voice systems) to be compatible and interoperate with the contractor's VOIPTS.
9. The contractor shall meet a minimum quality level equivalent to or better than a Mean Opinion Score (MOS) of 4.0 as defined in ITU-T specification P.800 series when using the G.711 CODEC.
10. The contractor shall provide a call routing capability between phone numbers and IP addresses or URLs.
11. The contractor shall ensure security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized

access. This includes SIP-specific gateway security for SIP firewalls, where applicable. The contractor shall ensure security practices and policies are updated and audited regularly. Listed below are the general areas of security to be addressed:

- a. Denial of service – The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate VOIPTS users and subscribers from accessing VOIPTS.
- b. Intrusion – The contractor shall provide safeguards to mitigate attempts to illegitimately use VOIPTS service.
- c. Invasion of Privacy – The contractor shall ensure VOIPTS is private and that unauthorized third parties cannot eavesdrop or intercept VOIPTS communications.

#### C.2.6.8.2 Features

None.

#### C.2.6.8.3 Interfaces

##### C.2.6.8.3.1 Network Interface

The User-to-Network Interfaces (UNI's) at the SDP, as defined in the Section C.2.7.8.3.2, are mandatory unless indicated otherwise.

##### C.2.6.8.3.2 Voice Over Internet Protocol Transport Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP, H.323, MGCP, or SCCP [Optional]
2	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Loop Signaling (loop start and ground start)
3	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	E&M Wink Start Signaling
4	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
5	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
6 OCONUS / non-domestic (Optional)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling

#### C.2.6.8.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of key performance indicators (KPI's) for Voice over Internet Protocol Transport Service in Section C.2.7.8.4.1 below are mandatory:

**C.2.6.8.4.1 Voice over Internet Protocol Transport Service Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Latency	Routine	200 ms	≤ 200 ms	See Note 1
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	See Note 2
Availability	Routine	99.6%	≥ 99.6%	See Note 3
	Critical (Optional)	99.9%	≥ 99.9%	
Jitter	Routine	10 ms	≤ 10 ms	See Note 4
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	

Note:

1. Latency is the average time (round trip) for a packet to travel from source SDP to destination SDP. This applies to CONUS.
2. Grade of Service (Packet Loss) is defined as the percentage of packets that are sent by the source SDP but never arrive at the destination SDP (the percentage of packets that are dropped). The packet loss can be measured with an ICMP test. This applies to CONUS.
3. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the VOIPTS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

4. Jitter is the average variation or difference in the delay between received packets of an IP packet data stream from SDP to SDP. Relevant standard: IETF RFC 1889. This applies to CONUS.
5. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.6.9 Internet Protocol Video Transport Services (IPVTS)**

Agencies are seeking services to provide reliable, high quality transport of video traffic over a managed Internet Protocol (IP) network. Internet Protocol Video Transport Services (IPVTS) can offer video conferencing capabilities using the contractor's IP network. Agency video conferencing systems and devices may include studio, fixed, desktop, and portable systems operating at different transmission rates and protocols.

The following sections provide the requirements for Internet Protocol Video Transport Service.

### **C.2.6.9.1 Service Description**

#### **C.2.6.9.1.1 Functional Definition**

Internet Protocol Video Transport Service will transport Agency video traffic over the contractor's IP network with guaranteed service levels. This includes, but is not limited to, transport of point to point, multi-point, and uni-cast/multi-cast IP video communications operating at a variety of data rates. IPVTS will offer a gateway service to allow access outside of the contractors IP network and bridging services for multi-point conferences.

#### **C.2.6.9.1.2 Standards**

Internet Protocol Video Transport Service shall comply with the following standards (and recommendations) as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Federal Telecommunications Recommendations (FTR) 1080B - 2002 (hereafter referred to as FTR-1080) issued by the Technology and Standards Division of the National Communication System (NCS).
2. FTR 1080 encompasses the specifications for video teleconferencing and video telephony primarily based on the following standards:
  - a. ITU-T series H.323 recommendations for packet based multi-media conferencing
  - b. ITU-T series T.120 recommendations for multimedia document conferencing
  - c. ITU-T series H.320 recommendations for narrow band video conferencing

Refer to [http://www.ncs.gov/library/fed\\_rec/FTR%201080B-2002%208-15.pdf](http://www.ncs.gov/library/fed_rec/FTR%201080B-2002%208-15.pdf) for a copy of the FTR 1080 document.

3. IETF RFC 3216 Session Initiation Protocol (SIP) when and where available commercially
4. IETF RFC 3376 Internet Group Management Protocol (IGMP)
5. ISO/IEC Moving Picture Experts Group (MPEG) digital video standards.
6. ITU-T H.350
7. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.



The Internet Protocol Video Transport Service shall comply with the appropriate standards for the underlying IP network services as described in sections C.2.4.1 (IPS), C.2.7.2 (PBIP-VPNS), and C.2.7.3 (NB-IPVPNS).

#### **C.2.6.9.1.3 Connectivity**

Internet Protocol Video Transport Service shall connect to and interoperate with:

1. Internet
2. IP Networks and IP VPN's
3. Public Switched Telephone Network (PSTN)

#### **C.2.6.9.1.4 Technical Capabilities**

The following Internet Protocol Video Transport Service capabilities are mandatory marked optional:

1. The contractor's IPVTS shall allow participants at different physical locations to simulate in person meetings and conduct interactive dialogue using point-to-point and point-to-multi-point video teleconferencing arrangements.
  - a. A point-to-point conference is a single video connection between two endpoints that provides simultaneous two way or one way transmission of digital signals.
  - b. A multipoint conference is a single video conference between three or more endpoints that provides simultaneous two way or one way transmission of digital signals.
2. The contractor shall support two way video, one way video with interactive voice, and/or the interactive viewing, editing or transfer of various types of documents/data files among IPVTS participants as an adjunct to the IP video transport session.
3. The contractor shall support point-to-point connection arrangements with full-duplex video, audio, and ancillary data transmission between participating locations on demand without a reservation.
4. The contractor shall supply IPVTS gateways, gatekeepers, or other interfaces to enable conference capability between Agency IPVTS endpoints and dissimilar or non IPVTS endpoints.
5. The contractor shall provide a routing prioritization scheme or class of service to distinguish services.
6. Time sensitive IPVTS IP packets shall be assigned a higher priority than non time sensitive services to mitigate potential quality and latency issues. [Optional]
7. The contractor shall support streaming video applications utilizing multi-cast and/or uni-cast transmission of data packets.

8. The contractor's IPVTS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.
9. The contractor shall provide an IPVTS central reservation capability to permit authorized video teleconference users to schedule and establish video teleconferences when a gateway, provided by the contractor, is required to establish connectivity between dissimilar networks, rate adaptation, or coding conversion. Reservations shall be required only when contractor provided coding conversion, rate adaptation, or gateway service is requested by the subscribing Agency.
10. The contractor shall provide access via a secure web site to the reservation service. The reservation service shall provide the ability to electronically schedule reservations and obtain Agency IPVTS reports via a secure Internet connection. The reservation service shall provide the ability for authorized IPVTS users to schedule one or more conferences within at least one year in advance of the conference. Scheduling can be by time and day of the week either as a single event or recurring event on a daily, weekly, monthly, or other periodic basis. The reservation service shall provide the ability to add participants to a conference.
11. The contractor shall provide a reservation service with the capability to provide an e-mail notification with a meeting invitation and RSVP option to IPVTS participants. The service shall also provide the capability to provide cancellation notices to IPVTS participants. The reservation system shall capture the following minimum information:
  - a. Name of the person scheduling an IPVTS conference.
  - b. Organization of the person scheduling an IPVTS conference.
  - c. Telephone number and email address of the person scheduling IPVTS.
  - d. Name, telephone number, and email address of the contact person at participating locations.
  - e. IP addresses of the participant end points in an IPVTS conference.
  - f. Date and time of an IPVTS conference.
  - g. Scheduled duration of an IPVTS conference.
12. The contractor shall provide IPVTS reservation users with the following capabilities:
  - a. Schedule a non-recurring multi-point or point-to-point video teleconference within 30 minutes of the reservation request.
  - b. Permit IPVTS users to cancel a reservation before the scheduled start time of the video teleconference.

- c. Enable IPVTS end points operating at different (disparate) data rates/speeds to interconnect and conference at their preferred rate.
13. The contractor's IPVTS multi-point conference arrangements shall be supported in conjunction with the reservation service upon the subscribing Agency's request. The multi-point conference arrangement shall have the capability of providing service to users of a different contractor's network or public or private networks. The following multi-point conference arrangements shall be supported:
  - a. Voice Activation - The video signal transmitted to all locations is automatically switched, by voice activation, after the speaker's audio signal from a location exceeds a preset level for a specified amount of time.
  - b. Chairperson Activated - The person in control of the video teleconference sends his or her own video and selects a return video from one of the participating locations.
  - c. Continuous Presence - This option allows multiple sites to be viewed simultaneously on the same screen. The contractor shall support at a minimum of four split screens with this option.
  - d. Lecture Control (Broadcast Video with Audio Return) – The video from the lecturer's location is transmitted to all VTS participants. Audio, but no video, may be returned to the lecturer's location from all other participating locations.
14. The contractor shall detail video teleconferencing activity used by the reservation service in a monthly report. At a minimum, the report shall include the date and starting time of each conference, whether it was successfully completed, conference duration, participating locations, and the data rate used between each participating location.
15. The contractor shall maintain lip synchronization between the audio and video signals within  $\pm 2$  video frames to the extent possible with the video frame rate employed in the video teleconference.
16. The contractor shall support transport of unclassified and non sensitive video conferencing information that is unencrypted as part of the standard service. Section C.2.7.9.2.1, Features, provides a description of higher security requirements that shall be available.
17. The contractor shall provide the capability for users to request real-time assistance to resolve service issues.
18. The contractor shall ensure security practices and safeguards are provided to minimize susceptibility to unauthorized access. Listed below are the general areas of security to be addressed:

- a. Denial of service – the contractor shall provide safeguards to prevent hackers, worms or viruses from denying legitimate IPVTS users and subscribers from accessing IPVTS.
- b. Intrusion – the contractor shall provide safeguards to mitigate attempts to illegitimately use IPVTS service.
- c. Invasion of Privacy – the contractor shall ensure IPVTS is private and that unauthorized third parties cannot eavesdrop or intercept IPVTS communications.

Features

The following Internet Protocol Video Transport Service features in section C.2.7.9.2.1 are mandatory unless marked optional:

**C.2.6.9.1.5 Internet Protocol Video Transport Service Features**

ID Number	Name of Feature	Description
1.	Certification	The contractor shall provide pre-testing, registration and certification that Agency video teleconferencing equipment is compatible and can conduct IPVTS calls over the contractors IPVTS network. In the event that the equipment is not certified, the contractor will notify the Agency of the deficiency and required changes to be operable with IPVTS.
2.	Coding Conversion (Transcoding)	<ol style="list-style-type: none"> <li>1. The contractor shall provide transcoding that is compliant with FTR 1080 formats.</li> <li>2. [Optional] The contractor shall provide a coding conversion capability that permits operation between Codecs, all of which use the National Television Standards Committee (NTSC) video format, but none of which support the FTR 1080 standard and none of which use the same encoding/decoding algorithm(s). At a minimum, the contractor shall support the following compression algorithms as needed by the Agency: SG3/SG4, CTX, and CTX+.</li> <li>3. [Optional] The contractor shall provide a coding conversion capability that permits operation between Codecs, all of which use the NTSC video format, in which one or more of the codec's support the FTR 1080 and in which one or more of the codec's do not support the FTR 1080. At a minimum, the contractor shall support the following compression algorithms as needed by the Agency: SG3/SG4, CTX, and CTX+.</li> </ol>
3.	Gateway Service	<p>The contractor shall provide an IP gateway service to provide transparent connectivity between the contractors IPVTS network endpoints and external network endpoints.</p> <p>At a minimum, the contractor's gateway service shall provide interoperability and transcoding between end point devices utilizing different protocols such as (1) H.320, (2) H.323, or (3) SIP (when available commercially) based upon the subscribing Agency's needs.</p> <p>The gateway service shall be capable, at a minimum, of operating at the following data transmission rates:</p> <ol style="list-style-type: none"> <li>1) 128 Kbps</li> </ol>

ID Number	Name of Feature	Description
		2) 256 Kbps 3) 320 Kbps 4) 336 Kbps 5) 384 Kbps 6) 448 Kbps 7) 512 Kbps 8) 768 Kbps 9) 1.544 Mbps [Optional] 10) 1.92 Mbps [Optional]
ID Number	Name of Feature	Description
4.	Rate Adaptation	The contractor shall provide a data rate adaptation capability to ensure that all IPVTS locations participating in a video teleconference at different data rate can interconnect with each other. The rate adaptation feature shall be used in conjunction with the reservation feature.
5.	Security – Sensitive But Unclassified.	The contractor shall support and provide transparent and secure IPVTS communications paths that do not corrupt Agency encrypted video conference data. This includes transport of video information that is categorized as sensitive but unclassified. The security capabilities are described in the FTR 1080 recommendation.
6.	Security – Classified [Optional]	The contractor shall support and provide transparent and secure IPVTS communications paths that do not corrupt Agency encrypted video conference data. This includes transport of video information that is categorized as classified (National Security Agency type 1 encryption). The security capabilities are described in the FTR 1080 recommendation.

### C.2.6.9.2 Interfaces

#### C.2.6.9.2.1 Network Interface

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.7.9.3.1.1, are mandatory:

##### C.2.6.9.2.1.1 Internet Protocol Video Transport Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	All IEEE 802.3 cable and connector types	Up to 1.92 Mbps per IPVTS end point	IEEE 802.3. IPv4. [IPv6 when available]

### C.2.6.9.3 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI's) for Internet Protocol Video Transport Service shall be measured and monitored as defined in Section C.2.7.9.4.1

#### C.2.6.9.3.1 Internet Protocol Video Transport Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.6%	≥ 99.6%	See Note 1
Latency	Routine	120 ms	≤ 120 ms	See Note 2
Jitter	Routine	10 ms	≤ 10 ms	See Note 3
Grade of Service (Packet Loss)	Routine	0.4 %	≤ 0.4 %	See Note 4
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	

**Notes:**

1. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that IPVTS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the average time (round trip) for a packet to travel across the contractor's IPVTS service. This applies to CONUS only.
3. Jitter is the average variation or difference in the delay between received packets of an IP packet data stream from SDP to SDP. Relevant standard: IETF RFC 1889. This applies to CONUS only.
4. Grade of Service (Packet Loss) is defined as the percentage of RTP packets that are sent by the source SDP but never arrive at the destination SDP. This applies to CONUS only.
5. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.6.10 Internet Protocol Telephony Service (IPTelS)**

Internet Protocol Telephony Service (IPTelS) provides voice communications service and telephony features to the subscribing Agency using the Voice over Internet Protocol over a managed IP network.

The following sections provide the requirements for Internet Protocol Telephony Service.

**C.2.6.10.1 Service Description**

#### **C.2.6.10.1.1 Functional Definition**

Internet Protocol Telephony Service provides a network based telephone service over a contractor provided IP network with a set of telephony features using the Voice over Internet Protocol (VoIP). IP Telephony service allows subscribers to be reached by direct dialing.

#### **C.2.6.10.1.2 Standards**

Internet Protocol Telephony Service shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. IEEE 802.1p/q, 802.3x
2. Internet Engineering Task Force (IETF) RFC 2132 for Dynamic Host Configuration Protocol (DHCP)
3. IETF RFCs 3761 (ENUM), 3966
4. IETF RFCs for Internet Protocol (IP) IPv4. IPv6 when and where offered commercially by the contractor.
5. ITU RFC 2474,2475 DiffServ
6. ITU-T E.164 as interpreted by the Industry Number Committee of Alliance for Telecommunications Industry Solutions (ATIS).
7. ITU-T G.107
8. ITU-T G.711
9. ITU-T G.723.x [Optional], G.726 [Optional], G.728 [Optional], or G.729.x [Optional]
10. ITU-T H.248.1 (MEGACO), H.323, H.350 when and where offered commercially by the contractor.
11. ITU-T Q.700 series recommendations for Signaling System No. 7
12. ITU-T T.30, T.37, and T.38
13. Lightweight Directory Access Protocol (LDAP)
14. Media Gateway Control Protocol (MGCP) IETF RFC 3435 when and where offered commercially by the contractor.
15. Real-Time Transport Protocol (RTP) IETF RFC 3550
16. Session Initiation Protocol (SIP) IETF RFC 3261 when and where offered commercially by the contractor.
17. Transmission Control Protocol (TCP) IETF RFC 793
18. User Datagram Protocol (UDP) IETF RFC 768
19. Reserved

20. FCC Orders as issued

21. The contractor shall comply with new versions, amendments, and modifications made to the above documents and standards when offered commercially.

#### **C.2.6.10.1.3 Connectivity**

Internet Protocol Telephony Service shall connect to and interoperate with:

1. Public Switched Telephone Network (PSTN)
2. Internet
3. Agency LAN's

IPTelS requires a connection to the contractor's IP network.

#### **C.2.6.10.1.4 Technical Capabilities**

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:

1. The contractor shall provide capabilities that shall enable IPTelS subscribers to successfully establish and receive telephone calls between both on- net locations and the PSTN.
2. The contractor shall provide the following minimum capabilities:
  - a. The contractor shall provide real time transport of voice, facsimile, and TTY communications.
  - b. The contractor shall provide real time delivery of caller ID (ANI) information (when provided from the originating party).
  - c. The contractor's IPTelS shall interoperate with public network dial plans (ITU-T E.164, North American Numbering Plan) and Direct Inward Dialing (DID) service.
  - d. The contractor's IPTelS shall interoperate with private network dial plans and support direct station to station dialing.
  - e. The contractor's IPTelS shall interoperate with non commercial, Agency specific 700 numbers
  - f. The contractor shall provide access to public directory and operator assistance services.
  - g. The contractor shall provide the capability to identify the originating number of a caller, on a per call basis, and dial back to the originating number (call return).
  - h. The contractor shall support multi-point conferencing
3. A gateway enables interworking between the voice over IP packet switched network and non-IP networks and devices. The contractor shall provide gateway's for interoperability with IPTelS and the PSTN, or with Agency UNI's.



The specific gateway will depend upon the subscribing Agencies UNI requirements. The gateways and functionality are described below:

- a. Subscriber Gateway – The contractor shall provide interoperability for traditional “non-IP” telephone devices. The contractor shall provide non-proprietary telephony station UNI’s including (a) analog station and (b) ISDN BRI station [Optional] interfaces.
  - b. PSTN Gateway. The contractor shall provide transparent access to and interwork with the domestic and non-domestic Public Switched Telephone Networks (PSTN’s).
4. The contractor shall provide a transparent alternate routing capability (overflow and failover routing) to allow calls to route off net (or “hop off”) from the contractors IPTeIS network to the PSTN when necessary.
  5. The contractor shall provide a routing prioritization scheme or class of service. Time sensitive IP Telephony packets shall be assigned a higher priority than non real time sensitive services to mitigate potential call quality issues.
  6. The contractor shall provide the capability to support station mobility. Station mobility enables an IPTeIS subscriber to dynamically move their IP phone within the Agencies enterprise wide network and access IPTeIS services.
  7. The contractor shall fully comply with emergency service requirements, including 911 and E911 services, and identify the location of an originating station and route them to the appropriate Public Safety Answering Point (PSAP).
  8. The contractor’s IPTeIS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewall is compatible with the contractors’ service.
  9. The contractor’s IPTeIS shall meet a minimum quality level equivalent to or better than a Mean Opinion Score (MOS) of 4.0 as specified in ITU-T specification P.800 series when using the G.711 CODEC.
  10. The contractor’s IPTeIS shall comply with the Federal Communications Commission (FCC) Local Number Portability (LNP) requirements.
  11. The contractor shall ensure security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. This includes SIP-specific gateway security for SIP firewalls, where applicable. The contractor shall ensure security practices and policies are updated and audited regularly. Listed below are the general areas of security to be addressed:
    - a. Denial of service – provide safeguards to prevent hackers, worms, or viruses from denying legitimate IPTeIS users and subscribers from accessing IPTeIS.
    - b. Intrusion – provide safeguards to mitigate attempts to illegitimately use IPTeIS service.

- c. Invasion of Privacy – ensure IPTeIS is private and that unauthorized third parties cannot eavesdrop or intercept IPTeIS communications
12. The contractor shall provide a call routing capability between phone numbers and IP addresses or URL's.
13. The contractor shall provide a secure web site for IPTeIS subscribers and system administrator to view reports, administer personal calling preferences, retrieve messages, and perform configuration management for IPTeIS.
14. The contractor shall provide a telephone number with the following telephone features as part of the basic IPTeIS service:
- a. Call Forward - All Calls. Provide the capability that allows a station user to choose to reroute all incoming calls to another specified telephone number. The feature shall have the capability to restrict call forwarding to internal, local or long distance numbers. It shall be possible for the station user to activate or cancel this feature. Outgoing calling capability shall be allowed when call forwarding is activated. This capability can be administered on a station basis according to the subscribing Agencies needs.
  - b. Call Forward – Busy/Don't Answer. Provide the capability that allows a station user to choose to reroute incoming calls to another specified telephone number on a busy or ring-no-answer condition within a pre-determined interval. The feature shall have the capability to restrict call forwarding to internal, local or long distance numbers. It shall be possible for the station user to activate or cancel this feature. Outgoing calling capability shall be allowed when call forwarding is activated. This capability can be administered on a station basis.
  - c. Call Hold. The contractor shall provide the ability to put a caller on hold and retrieve them from the hold state. The contractor shall provide music for the caller when they are in the hold state (music on hold).
  - d. Call Park. The contractor shall allow a call to be parked at a subscriber's number for retrieval by another subscriber line. This capability can be administered on a station basis according to the subscribing Agencies needs.
  - e. Call Pickup. The contractor shall allow a subscriber to answer any calls directed to another station line within his or her own (a) predefined call pickup group or via (b) direct call pickup by dialing the telephone number of the ringing target extension. This capability can be administered on a station basis according to the subscribing Agencies needs.
  - f. Call Transfer. The contractor shall provide the capability that allows a station user to transfer any call in progress to another telephone number without the

assistance of the operator. Both unsupervised (blind) and supervised call transfer capabilities shall be provided.

- g. Call Waiting. The contractor shall allow a call to a busy station to be held waiting while a tone signal is directed towards the busy station user (only the called station user shall hear this tone). The contractor shall offer the capability for the subscriber to disable the service, temporarily on a per call basis.
- h. Calling Number Suppression. The contractor shall provide the originating subscriber the capability to suppress the origination station number from being received by the terminating station. It shall be possible to enable this function either on a (a) per-call basis or (b) as a permanent attribute of the station.
- i. Class of Service (COS) Restrictions. The contractor shall allow privileges assigned to a particular station. The COS can be used to restrict calling privileges and access to designated features.
- j. Conference Calling. The contractor shall allow a voice station user to establish a multiparty conference connection of a minimum of three conferees including themselves, without attendant assistance.
- k. Directory. The contractor shall provide a directory function to view and store frequently called numbers. The directory shall also track, at a minimum, the five most recent missed calls, received calls and originated calls.
- l. Distinctive Ringing. The contractor shall provide a unique ringing or alert that distinguishes between internal and external calls.
- m. Do Not Disturb (DND). The contractor shall provide the ability to temporarily block calls to a station number. The feature can be activated and de-activated by the subscriber. Outgoing calling capability shall be allowed when the DND state is activated. This capability can be administered on a station basis according to the subscribing Agencies needs.
- n. Hotline. The contractor shall provide an automatic ring down to a pre-defined endpoint when the originator initiates a call from the hotline station.
- o. Hunt Groups. The contractor shall provide the capability to route incoming calls to a predetermined sequence of telephone numbers until it is answered. The contractor shall offer different hunting options including (a) circular and (b) pilot (sequential) hunt groups.
- p. Last Number Dialed (LND). The contractor shall offer last number dialed capability on a per station basis. The service shall enable a station user to

automatically originate a call to the last number dialed from the station user's phone (re-dial).

- q. Multi Line Appearance. The contractor shall support the ability for multiple line appearances to operate on a subscriber's phone.
- r. Specific Call Rejection. The contractor shall allow subscribers to screen incoming calls by creating a list of phone numbers (or URLs) from which to reject calls. Calls originated from numbers contained on the rejection list shall be routed to an alternative destination such as an announcement.
- s. Speed Dial. The contractor shall offer abbreviated digit dialing capability on a per station basis.

**C.2.6.10.2 Features**

The following Internet Protocol Telephony Service features in Section C.2.7.10.2.1 below are mandatory:

**C.2.6.10.2.1 Internet Protocol Telephony Service Features**

ID Number	Name of Feature	Description
1	Find Me Follow Me Routing	The contractor shall provide Find me, Follow me with the capability to route incoming calls, at a minimum, to five alternate numbers with options for sequential or parallel routing to destination phone numbers (i.e. ring simultaneous phone numbers), or route to voice mail. The subscriber will be able to manage a "find me list" and select any combination of different phone numbers in a user defined search order to ensure delivery of important calls.
2	IP Telephony Manager (Subscriber)	The contractor shall provide secure browser based access, with authentication, for subscribers to manage their personal calling preferences, messages, and view call status. IP Telephony Manager shall enable IPTelS subscribers to change personal calling preferences in real time, control user telephony functions, screen and route calls, and provide the following minimum capabilities:  <ol style="list-style-type: none"> <li>1. Blocking of selected numbers</li> <li>2. Activate and de-activate call forwarding state</li> <li>3. Change ringing preferences</li> <li>4. View call history log</li> <li>5. Manage personal directory / address book</li> <li>6. Manage abbreviated dialing lists</li> <li>7. Select display format</li> <li>8. Manage subscriber password(s)</li> <li>9. View the status of the subscriber line (In use, Idle, etc.)</li> <li>10. Manage routing of incoming calls and messages</li> <li>11. View caller ID information</li> <li>12. Manage voice mail messages</li> <li>13. Provide message waiting indications</li> </ol>

ID Number	Name of Feature	Description
3	IP Telephony Manager (Administrator)	<p>The contractor shall provide secure browser based access, with authentication, to perform basic IPTeLS administration capabilities, configuration management, and retrieve management reports. The IP Telephony Manager shall enable an Agency to make administrative changes (real time and scheduled) and provide the following minimum capabilities:</p> <ol style="list-style-type: none"> <li>1. Administer and change station class of service</li> <li>2. Blocking of selected numbers</li> <li>3. View the status of a subscriber line (In use, Idle, etc.) or groups of lines</li> <li>4. Retrieve IPTeLS reports (real time or historical)</li> <li>5. Activate and de-activate call forwarding state</li> <li>6. Administer dial plans</li> <li>7. Perform directory updates</li> <li>8. Manage account passwords</li> </ol>
4	Voice Mail Box	<p>The contractor shall offer voice mail capability that includes voice messaging transmission, reception, and storage for 24x7 except for periodic scheduled maintenance. The contractor provided voice mailbox shall meet the following <i>minimum</i> requirements:</p> <ol style="list-style-type: none"> <li>1. At least sixty minutes of storage time (or 30 messages)</li> <li>2. Ability to remotely access voice mail services</li> <li>3. Secure access to voice mail via a password or PIN</li> <li>4. Automatic notification when a message is received</li> <li>5. Minimum message length of two minutes</li> <li>6. Capability to record custom voice mail greetings</li> </ol> <p>This capability can be administered on a station basis according to the subscribing Agencies needs.</p>
5	LAN Management	<p>The contractor shall provide and manage LAN networking hardware components (e.g., switches) to extend IPTeLS service to the terminating subscriber device (e.g. handset).</p> <p>The contractor shall specify the following LAN management activities:</p> <ol style="list-style-type: none"> <li>1. Configuration management</li> <li>2. Moves, Adds, Changes, Disconnects (MACDs)</li> <li>3. Service/Alarm monitoring and fault management</li> <li>4. Ticket creation</li> <li>5. Proactive notification</li> <li>6. Trouble isolation and resolution</li> </ol>

### C.2.6.10.3 Interfaces

#### C.2.6.10.3.1 Network Interface

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.7.10.3.2 are mandatory unless indicated otherwise. Internet Protocol Telephony Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP, H.323, MGCP, or SCCP [Optional]
2	Analog Line: Two- Wire (Std: Telcordia SR- TSV-002275)	4 kHz Bandwidth	Line - Loop Signaling
3 (Optional)	Digital Line: ISDN BRI S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 Kbps (2x64 kbps)	ITU-TSS Q.931

The contractor's IPTeS shall be capable of interfacing with non-proprietary telephone instruments and fax machines. IPTeS should, at a minimum, support the following subscriber devices:

1. Analog phones
2. Facsimile devices
3. IP phones
4. ISDN phones [Optional]
5. PC client soft phones

#### C.2.6.10.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI's) for Internet Protocol Telephony Service in Section C.2.7.10.4.1 are mandatory unless marked optional.

##### C.2.6.10.4.1 Protocol Telephony Services Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Latency	Routine	200 ms	≤ 200 ms	See Note 1
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	See Note 2
Availability	Routine	99.6%	≥ 99.6%	See Note 3
	Critical [Optional]	99.9%	≥ 99.9%	
Jitter	Routine	10 ms	≤ 10 ms	See Note 4

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	

**Notes:**

Note 1: Latency is the average round trip time for a packet to travel from source SDP to destination SDP. This applies to CONUS.

Note 2: Grade of Service (Packet Loss) is defined as the percentage of packets that are sent by the source SDP but never arrive at the destination SDP (the percentage of packets that are dropped). The packet loss can be measured with an ICMP test. This applies to CONUS.

Note 3: Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the IPTeS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

Note 4: Jitter is the average variation or difference in the delay between received packets of an IP packet data stream from SDP to SDP. Relevant standard: IETF RFC 1889.

Note 5: See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.6.11 Converged IP Services (CIPS)**

Converged IP Services is the integration of voice, video, and data transported over a common network infrastructure. Various technologies, media, and protocols which provide traffic prioritization are enabling convergence. These include, but are not limited to, broadband core networks and the availability of high speed network access including DSL, cable service, and fiber connections to the core network. Agencies recognize the benefits of a converged Internet Protocol (IP) network with multi-services to facilitate information sharing, minimize maintenance and administration, maximize utilization of available bandwidth, optimize network services, and increase productivity.

The following sections provide the requirements for CIPS.

### **C.2.6.11.1 Service Description**

#### **C.2.6.11.1.1 Functional Definition**

Converged IP Services will provide secure, converged voice, data, and video communications services over a common IP network connection to the subscribing Agency.

#### **C.2.6.11.1.2 Standards**

Converged IP Services shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Federal Telecommunications Recommendation (FTR) 1080B-2002
2. ITU-T H.248.1 (MEGACO), H.323 when and where offered commercially by the contractor.
3. IETF RFC 1771, 1772 Border Gateway Protocol (BGP), Real-Time Transport Protocol (RTP) and Open Shortest Path First [Optional] (OSPF).
4. IETF RFC 3261 Session Initiation Protocol (SIP), RFC 3761 (ENUM), and RFC 3966 when and where offered commercially by the contractor.
5. IP Security Protocol Working Group
6. ITU-T T.30, T.37, T.38, and E.164 ITU-T G.711
7. ITU-T G.723x [Optional], G.726 [Optional], G.728 [Optional], or G.729.x [Optional]
8. Media Gateway Control Protocol (MGCP) IETF RFC 3435 when and where offered commercially by the contractor.
9. Motion Pictures Expert Group (MPEG) MP2, MP3
10. Multi Protocol Label Switching (MPLS) Working Group standards
11. Transmission Control Protocol/Internet Protocol (TCP/IP) suite
12. Reserved
13. FCC Orders
14. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

#### **C.2.6.11.1.3 Connectivity**

Converged IP Services shall connect to and interoperate with:

1. Public Switched Telephone Network.



2. Internet.
3. Agency LANs.

#### **C.2.6.11.1.4 Technical Capabilities**

The following Converged IP Services capabilities are mandatory unless marked optional:

1. The contractor shall deliver the following converged IP services:
  - a. Data communications.
  - b. Video communications.
  - c. Voice communications.
2. The contractor shall provide a routing prioritization scheme or class of service to distinguish between applications that require real-time (or high priority) treatment over near, or non real-time applications.
3. The contractor shall ensure time sensitive IP packets are assigned a higher priority than non time sensitive services to mitigate potential quality and latency issues
4. The Agency will have the option to determine the prioritization of applications [Optional].
5. The contractor shall provide gateways and/or service enabling devices, where required, (a) for protocol conversions, (b) to interface with the contractor's CIPS network or (c) for access to external networks. External networks shall include the Public Switched Telephone Network (PSTN) and Internet.
6. The contractor shall ensure adequate network capacity to deliver CIPS service for the subscribing Agency.
7. The contractor shall support dynamic IP address, single or multiple static IP address schemes.
8. The contractor shall provide a secure web site with access to near real-time and historical CIPS network management information. This shall include but is not limited to:
  - a. Network statistics including availability, delay, packet loss, and jitter.
  - b. Utilization statistics.
9. For voice services, the contractor shall provide the following minimum telephony capabilities:
  - a. Call Transfer
  - b. Call Conferencing
  - c. Call Forwarding or Find Me/Follow Me Forwarding
  - d. Caller ID and Caller ID Blocking

- e. Do Not Disturb
  - f. Incoming/Outgoing Call Logs
  - g. Speed dialing
  - h. Voice Mail
  - i. Provide the capability to identify the originating number of a caller, on a per call basis, and dial back to the originating number (call return)
10. For voice services, the contractor shall provide directory assistance and operator services.
11. For voice services, the contractor shall fully comply with local number portability and emergency service requirements including 911 and E911 services to identify the location of an originating station and route the call to the appropriate Public Safety Answering Point (PSAP).
12. The contractor shall provide the CIPS SED's such as IP phones, and video teleconferencing terminals if requested by the Agency.
13. The contractor's CIPS shall be compatible and interoperate with Agency provided Active Directory services.
14. The contractor's CIPS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.
15. The contractor shall ensure security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. This includes SIP-specific gateway security for SIP firewalls, where applicable. The contractor shall ensure security practices and policies are updated and audited regularly. Listed below are the general areas of security to be addressed:
- a. Denial of service – provide safeguards to prevent hackers, worms, or viruses from denying legitimate CIPS users and subscribers from accessing CIPS.
  - b. Intrusion – provide safeguards to mitigate attempts to illegitimately use CIPS service.
  - c. Invasion of Privacy – ensure CIPS is private and that unauthorized third parties cannot eavesdrop or intercept CIPS communications.
  - d. Encryption and secure tunneling (VPN) at the Sensitive but Unclassified (SBU) through National Security Information (NSI) levels available under section C.2.10 Security Services and C.2.7.4 Managed Tier Security Services.

**C.2.6.11.2 Features**

None.

**C.2.6.11.3 Interfaces**

### C.2.6.11.3.1 Network Interface

The User-to-Network Interfaces (UNI's) at the SDP, as defined in the Section C.2.7.11.3.2 below, are mandatory unless marked optional:

### C.2.6.11.3.2 Converged IP Services Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	All 802.3 cable and connector types	10/100/1000 Mbps	IPv4 (v6 when and where available commercially by the contractor) over Ethernet
2 (Optional)	All 802.3 cable and connector types	10 GbE (Gigabit Ethernet)	IPv4 (v6 when and where available commercially by the contractor) over Ethernet

### C.2.6.11.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of key performance indicators (KPI's) for Converged IP Services in Section C.2.7.11.4.1 are mandatory:

#### C.2.6.11.4.1 Converged IP Services Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.6%	≥ 99.6%	See Note 1
Latency	Routine	200 ms	≤ 200 ms	See Note 2
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	See Note 3
Jitter	Routine	10 ms	≤ 10 ms	See Note 4
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	

#### Notes:

1. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the CIPS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the average round trip time for a packet to travel from source SDP to destination SDP. This applies to CONUS.
3. Grade of Service (Packet Loss) is defined as the percentage of packets that are sent by the source SDP but never arrive at the destination SDP (the percentage of packets that are dropped). The packet loss can be measured with the ICMP test. This applies to CONUS.
4. Jitter is defined as the average variation or difference in the delay between received packets of an IP packet data stream from SDP to SDP. Relevant standard: IETF RFC 1889. This applies to CONUS.
5. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

#### **C.2.6.12 Layer 2 Virtual Private Network Services (L2VPNS)**

Layer 2 Virtual Private Network Services (L2VPNS) allow Government Agencies to connect multiple sites in a single bridged domain over a contractor's network. The layer 2 handoff will be Ethernet. The contractor will provide TDM, FR and ATM service via the L2VPNS using a contractor-chosen implementation. This any-to-any service interworking enables Agency's sites to be interconnected regardless of the access network type. It also allows the Agencies to contract services delivered transparently to the network where interworking functions are required.

##### **C.2.6.12.1 Service Description**

###### **C.2.6.12.1.1 Functional Definition**

Agencies will be able to acquire point-to-point, point-to-multipoint and multi-point-to-multi-point services over a contracted common infrastructure. The contractor may fulfill requirements for L2VPNS by providing one or both of the following Layer 2 Virtual Private Network Services (L2VPNS) basic services:

1. Virtual Private LAN Service (VPLS) [Optional] – allows Agencies to extend their Ethernet or any other local area network (LAN) throughout the entire wide area network (WAN) in a secure manner. The offering provides fully meshed Layer 2 Multipoint connectivity across a contractor's network to the customer no matter where they are located and independent of the Agency's network access.
2. Virtual Private Wire Service (VPWS) [Optional] – Layer 2 Service that provides point-to-point connectivity (e.g. Frame Relay Data Link Connection Identifier (DLCI), ATM Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI)) across a contractor's network.

###### **C.2.6.12.1.2 Connectivity**

Layer 2 Virtual Private Network Services (L2VPNS) shall connect to and interoperate with:

1. The Agencies' Networks. L2VPNS shall provide connectivity for multiple LANs to extend them into the Metropolitan Area Networks (MAN) and Wide Area Networks (WAN). This enables the connection of Agency SDP(s) in one location to another SDP(s) in one or more locations.

### C.2.6.12.1.3 Standards

Layer 2 Virtual Private Network Services (L2VPNS) shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. Internet Engineering Task Force (IETF)
  - a. RFC 2684 - "Multi-protocol Encapsulation over ATM Adaptation Layer 5", September 1999
  - b. RFC 2427 - "Multi-protocol Interconnect over Frame Relay", September 1998
  - c. RFC3809, "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)", A. Nagarajan, Ed., June 2004
  - d. "Framework for Layer 2 Virtual Private Networks (L2VPNs)", draft-ietf-l2vpn-l2-framework-05.txt, June 2004
  - e. "Service Requirements for Layer-2 Provider Provisioned Virtual Private Networks", draft-ietf-l2vpn-requirements-01.txt, February 2004
  - f. "Virtual Private LAN Service", draft-ietf-l2vpn-vpls-bgp-02.txt, May 2004
  - g. "Virtual Private LAN Services over MPLS", draft-ietf-l2vpn-vpls-ldp-03.txt, April 2004
  - h. "Provisioning Models and Endpoint Identifiers in L2VPN Signaling", draft-ietf-l2vpn-signaling-01.txt, March 2004
  - i. "Using RADIUS for PE-Based VPN Discovery", draft-ietf-l2vpn-radius-pe-discovery-00.txt, February 2004
  - j. "Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)", draft-ietf-pwe3-requirements-08.txt, X Xiao, 12-Jan-04.
  - k. "Encapsulation Methods for Transport of Ethernet Frames over IP/MPLS Networks", draft-ietf-pwe3-ethernet-encap-07.txt, Luca Martini, Eric Rosen, Nasser El-Aawar, Giles Heron, 19-Jul-04.
  - l. "Encapsulation Methods for Transport of ATM Over IP and MPLS Networks", draft-ietf-pwe3-atm-encap-06.txt, Luca Martini, Matthew Bocci, Jeremy Brayley, Ghassem Koleyni, 19-Jul-04.
  - m. "Frame Relay over Pseudo-Wires", draft-ietf-pwe3-frame-relay-02.txt, Claude Kawa et al, February 2004.
2. Institute of Electrical and Electronics Engineers, Inc. (IEEE)

- a. Family of IEEE 802.1 standards
  - b. Family of IEEE 802.3 standards
3. All new versions, amendments, and modifications to the above documents and standards when offered commercially .

#### **C.2.6.12.1.4 Technical Capabilities**

The following Layer 2 Virtual Private Network Services (L2VPNS) capabilities are mandatory unless marked optional:

1. Virtual Private LAN Service (VPLS) [Optional] – The contractor shall support VPLS to provide the following:
  - a. Access to the contractor's backbone shall be supported.
  - b. This service shall enable the extension of Agency Local Area Networks (LANs) throughout the entire wide area network (WAN).
  - c. The contractor shall support a fully meshed Layer 2 Multi-point connectivity, by establishing tunnels (pseudo wires (PWs)), to Agency locations no matter where they are located; their connectivity shall be accomplished independently of the network access used.
  - d. The contractor shall provide the Agency with full control over their routing
  - e. The contractor shall provide transport of any routing protocol such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), and Border Gateway Protocol (BGP).
  - f. The contractor shall support the privacy over the Agency's addressing plan. This shall allow the Agency not to share the VPLS's addresses with the contractor.
  - g. The contractor shall provide the Agency with the ability of using duplicated addresses used in different VPLSs.
  - h. The contractor shall support hierarchical VPLS scheme (H-VPLS) comprising a two-tier structure: core and access.
  - i. The contractor shall support auto-discovery methods so the Agency's locations are discovered automatically as they are added to the Agency's VPLS domain such as Border Gateway Protocol (BGP)
  - j. The contractor shall support signaling protocols used to setup tunnels between the Agency's edge devices such as Border Gateway Protocol (BGP), Label Distribution Protocol (LDP)
  - k. Frames transported over a VPLS shall not be duplicated or be out of sequence.

2. Virtual Private Wire Service (VPWS) [Optional] – Layer 2 Service that provides point-to-point connectivity (virtual connections) across an IP network using the contractor's choice of encapsulation methods. Customers shall share the contractor's infrastructure and their virtual connections and their separation. Separation for customers choosing to have gateways to the Internet shall be met logically.
  - a. The contractor shall support logical interconnections visible to the Agency's UNI's at the SDP as single logical Layer 2 circuits.
  - b. The contractor shall support mapping of Layer 2 circuits into tunnels to the contractor's backbone.
  - c. The contractor shall support basic service interworking by allowing different customers to share tunnels in the contractor's backbone amongst several services such as ATM/FR, Ethernet, IP, TDM.
  - d. Single sided and double sided provisioning.
    - i. The contractor's network shall support single sided provisioning to allow the removal of an attachment circuit at one end of the virtual tunnel without the need to reconfigure the service when required by the Agency.
    - ii. The contractor's network shall support double sided provisioning in order to simplify the service provisioning if no short term reconfiguration is envisioned by the Agencies. This will allow full provisioning of remote endpoints at both sides using the same signaling procedure in the reverse direction.
  - e. The contractor's network shall support auto-discovery mechanisms such as LDP routing.
3. Service Interworking– The contractor shall support inter-working between two disparate protocols in order to preserve Agency's legacy ATM/FR switches, routers and multiplexers.
  - a. The contractor shall support Interworking Functions (IWFs) that terminate the protocol used in the Agency's network and maps its Protocol Control Information (PCI) into the protocol used by the contractor's network for the user/data, control and management planes.
  - b. The user data shall not be terminated or "touched" since the payload shall not affect the protocol mapping at the IWF.
  - c. The contractor's network shall support encapsulation of Ethernet, ATM, FR and TDM into different frame formats as part of service interworking based on the pertinent standards.
  - d. The service interworking function shall be able to mediate between the different address resolutions mechanisms between different services, and translating between the different frame formats.

4. Network Interworking – The contractor shall support the inter-working of higher layer protocols used in the L2VPNS.
2. The Agency shall be able to carry IPv4 or IPv6 transparently, irrespective of the layer 3 protocol in the contractor's network.
3. Any Layer 3 protocol used in the Agency's Local Area Network (LAN) shall also be transported across the Wide Area Network (WAN).
4. The Agency shall be able to transport legacy traffic such as Systems Network Architecture (SNA), NetBios and Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX).
5. L2VPNS protocols and standards supported by the contractor's network shall not interfere with the Layer 2 protocols being managed by the Agency's networks.
5. Routing Control. – The contractor shall ensure that the Agencies maintain full control over routing. The Agency will not provide updates to the contractor when making changes to the routes.
6. Scalability – L2VPNS shall scale so that installing and configuring a new Agency location does not require any changes to existing locations. The existing locations shall automatically recognize the new location.
7. User to Network Interfaces (UNIs) – The contractor shall support UNI(s) running Layer 2 protocols at the Agency's SDP that may be different to the ones running in other locations participating in the VPN. This intends to address the Agencies who may start out with a single Layer 2 protocol at the SDP, but wish to upgrade incrementally its SDPs over time to newer technologies.
8. Encapsulation Methods - The contractor shall indicate what encapsulation schemes are supported by its networks in order to support L2VPNS; i.e. Martini encapsulation, Q-tag stacking (Q-i-Q), MAC Address Stacking (MAS) and MAC in MAC (MIM).
9. Traffic Types – A L2VPNS shall support the following traffic types:
  - a. Unicast
  - b. Multicast
  - c. Broadcast
10. L2VPNS supported topologies shall include:
  - a. Point-to-Point
  - b. Point-to-Multipoint (hub-and-spoke)
  - c. Full mesh
  - d. Partial Mesh
  - e. Hierarchical



11. The contractor shall ensure that the Agency L2VPNS's internal configuration is not broadcasted or visible to third parties.
12. The contractor shall ensure traffic separation between different Agencies' L2VPNS unless data exchange is required and requested by the Agency.
13. Quality of Service (QoS) – The contractor shall support QoS functions when providing L2VPNS. The following shall be complied with if required by the subscribing Agency:
  - a. Shaping and Policing shall be supported by the contractor's routers
  - b. Mappings or translations of Layer 2 QoS parameters shall be supported in order to provide QoS transparency.
14. Management – Standard interfaces to manage L2VPNS shall be supported (i.e. standard Simple Network Management Protocol (SNMP) Management Information Base (MIB).
  - a. The contractor shall support proactive, around-the-clock management of the L2VPNS.
  - b. The contractor shall provide the subscribing Agency with administrative tools to manage the network and security policies.
  - c. The contractor shall provide view of the topology, operational state, order status statistics, near real-time performance statistics including but not limited to L2VPNS availability and latency (refer to Section C.2.7.12.4.1) via a performance graphic user interface - a secure, Website accessible by Agency clients.
15. Interoperability – The contractor shall ensure interoperability with the Agency's edge equipment as required by the Agency.
16. Government Agencies may require L2VPNS that span multiple contractors' networks, i.e., multiple administrative domains. The contractor shall ensure that any L2VPNS span multiple administrative domains still appear as a single, homogeneous L2VPNS. [Optional]

**C.2.6.12.2 Features**

The following Layer 2 Virtual Private Network Services (L2VPNS) features in Section C.2.7.12.2.1 are mandatory unless marked optional:

**C.2.6.12.2.1 Layer 2 Virtual Private Network Services (L2VPNS) Features**

ID Number	Name of Feature	Description
-----------	-----------------	-------------

1	Class of Service (CoS)	The contractor shall, provide multiple classes of service, to include but not limited to: <ol style="list-style-type: none"> <li>1. Premium – for time-critical traffic such as voice and video</li> <li>2. Enhanced – for business-critical traffic such as transactions</li> <li>3. Standard – for non-critical traffic such as email.</li> </ol>
2 (Optional)	Non-peered Private IP Network	The contractor shall provide the capability to run an Agency's L2VPNS service over transport that is not connected to the public Internet and allows separation of Agency traffic from any other Agency's traffic.
3	High availability options	Allow for the following high availability options: <ol style="list-style-type: none"> <li>1. Fault tolerance</li> <li>2. Load sharing</li> <li>3. Fail-over protection</li> <li>4. Diverse access points to service provider's POP(s).</li> </ol>

### C.2.6.12.3 Interfaces

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.7.12.4.1, are mandatory unless marked optional:

#### C.2.6.12.3.1 Layer 2 Virtual Private Network Services (L2VPNS) Interfaces

User-to-Network-Interfaces (UNI) applicable to this service are listed in the following table. Optional UNI lists are in the following Sections C.2.3.1, C.2.3.2, C.2.5.1, and C.2.5.2 .

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
1 (Optional)	Optical	IEEE 802.3z	1310 nm	1.25 Gbps	Gigabit Ethernet
2 (Optional)	Optical	IEEE 802.3z	850 nm	1.25 Gbps	Gigabit Ethernet
3	Optical	IEEE 802.3	1310 nm	125 Mbps	Fast Ethernet
4 (Optional)	Optical	IEEE 802.3ae	1310 nm	10 Gbps	10GBASE-SR (65 meters)
5 (Optional)	Optical	IEEE 802.3ae	850nm	10 Gbps	10GBASE-SW
6 (Optional)	Optical	IEEE 802.3ae	1550 nm	10 Gbps	10GBASE-ER
7 (Optional)	Optical	IEEE 802.3ae	1310 nm	10 Gbps	10GBASE-LR
8 (Optional)	Optical	IEEE 802.3ae	1550 nm	10 Gbps	10GBASE-LW
9 (Optional)	Optical	IEEE 802.3ae	1310 nm Single Mode	10 Gbps	10GBASE-LW (10,000 meters)
10 (Optional)	Optical	IEEE 802.3ae	1550 nm Single Mode	10 Gbps	10GBASE-EW (40,000 meters)
11	Electrical	IEEE 802.3	N/A	10 Mbps	10Base
12	Electrical	IEEE 802.3	N/A	100 Mbps	100 Base
13	Optical	IEEE 802.3		1 Gbps	1000Base
14	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-LX
15	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-SX
16 (Optional)	Electrical (Copper)	IEEE 802.3z	N/A	1 Gbps	1000BASE-CX
17 (Optional)	Electrical (Twisted pair)	IEEE 802.3z	N/A	1 Gbps	1000BASE-T
18 (Optional)	Optical	GR-253, ITU-T G.707	1310 nm	10 Gbps	SONET or SDH

#### C.2.6.12.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Layer 2 Virtual Private Network Services (L2VPNS) in Section C.2.7.12.4.1 are mandatory unless marked optional:

##### C.2.6.12.4.1 Layer 2 Virtual Private Network Services (L2VPNS) Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard Level	Acceptable Quality Level (AQL)	How Measured
Av(L2VPNS)	Routine	99.8%	> 99.8%	See Note 1
	Critical (Optional)	99.999%	≥ 99.999%	
Latency(L2VPNS)	Routine	100 ms	≤ 100 ms	See Note 2

Key Performance Indicator (KPI)	Service Level	Performance Standard Level	Acceptable Quality Level (AQL)	How Measured
CONUS				
Latency(L2VPNS) OCONUS	Routine	400 ms	≤ 400 ms	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	
Jitter(Packet)	Routine	10 ms	< 10 ms	See Note 4
Grade of Service (GOS) (Data Delivery Rate)	Routine	99.9%	≥ 99.9%	See Note 5 below
	Critical (Optional)	99.95%	≥ 99.95%	

## Notes:

- L2VPNS availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the L2VPNS is operationally available to the Agency. Availability is computed by the standard formula:
$$Av(L2VPNS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
- Latency value is the average round trip transmission between Agency premises routers for L2VPN with all of its CONUS sites. Relevant standards are RFC 1242 and RFC 2285.
- Refer to Section C.3.3.1.2.4 for definitions and how to measure.
- Measurements of Packet Jitter are performed by injecting packets at regular intervals into the network and measuring the variability in the arrival time. Relevant standard is RFC 2679.
- Network devices, such as switches and routers, sometimes have to hold data packets in buffered queues when a link is congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost. Relevant standards are RFC 1242 and RFC 2285.

## C.2.7 Conferencing Services

### C.2.7.1 Video Teleconferencing Services (VTS)

Agencies utilize Video Teleconferencing Services (VTS) to minimize expenses and permit individuals and groups to participate in activities they otherwise would be unable to attend due to various circumstances. VTS can support such diverse needs as conferencing, distance learning, remote testimony, and other applications. As a result, video communications and collaboration capabilities have evolved into a critical and growing real time communications environment for users.

For Agency applications, video conferencing must be reliable and interoperable in a heterogeneous environment consisting of networks and equipment operating within a widely diverse range of speeds. Video conferencing offerings must offer the capability for point-to-point and multi-point conferencing modes, enable real-time information sharing, and provide flexible scheduling options.

### **C.2.7.1.1 Service Description**

#### **C.2.7.1.1.1 Functional Definition**

Video Teleconferencing Service enables participants at different locations to simulate face to face meetings and conduct interactive dialogue with instant sharing of various applications and documents. VTS will provide point-to-point and multi-point conferencing with audio conference add-on capabilities to support the following three user configurations: desktop, portable roll about, and fixed conference room locations.

#### **C.2.7.1.1.2 Standards**

Video Teleconferencing Services shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Federal Telecommunications Recommendations (FTR) 1080B - 2002 (hereafter referred to as FTR-1080) issued by the Technology and Standards Division of the National Communication System (NCS).
2. FTR 1080 encompasses the specifications for narrow-band audio and video teleconferencing, from 56 Kbps to 1920 Kbps, primarily based on the following standards:
  - a. ITU-T H.320 recommendations for telephony networks [Optional].
  - b. ITU-T H.323 recommendations for packet based multi-media conferencing.
  - c. ITU-T T.120 recommendation for document conferencing.
3. IETF RFC 3261 Session Initiation Protocol (SIP) [Optional]
4. The VTS shall provide the capability to support channel aggregation and bonding for multi-rate DS-0 service (64 Kbps or 56 Kbps channels). [Optional]
5. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

#### **C.2.7.1.1.3 Connectivity**

Video Teleconferencing Services shall connect to and interoperate with:

1. IP Networks.
2. Internet.
3. Public Switched Telephone Network (PSTN).

VTS shall be available for domestic and non domestic users where available commercially from the contractor. VTS is an application-layer service that uses underlying network service(s) to carry video traffic. The different network services are as follows:

1. IP Packet switched networks.
2. Circuit switched data networks.
3. Private line networks for dedicated connectivity [Optional].

#### **C.2.7.1.1.4 Technical Capabilities**

The following Video Teleconferencing Services capabilities are mandatory unless indicated otherwise:

1. The contractor shall allow participants at different physical locations to simulate in person meetings and conduct interactive dialogue using point-to-point and point-to-multi-point video teleconferencing arrangements.
2. The contractor shall support two way video, one way video with interactive voice, and/or the instant sharing of various types of documents/data files among VTS participants as an adjunct to the video teleconferencing session.
3. The contractor shall support document sharing (data conferencing) which enables conference participants to interactively view, edit, and share or transfer data files and documents.
4. The contractor shall provide an audio conference add-on capability to support non video conference participants in a VTS call.
5. Agencies may require videoconferencing capabilities between different types of videoconferencing equipment and networks (e.g. IP packet switched, circuit switched and private line). The contractor shall supply gateways, gatekeepers, multi-point bridges, or other interfaces to enable for VTS between dissimilar interfaces or networks.
6. The contractor shall provide teleconferencing bridge capabilities including providing Internet Protocol (IP) packet switched bridging services for multiple IP VTS devices.
7. The contractor shall support the following modes of operation:
  - a. The contractor shall support Dial Out mode: An centralized arrangement where the conference bridge operator initiates a call and dials each participant at least 15 minutes prior to the conference start time.
  - b. The contractor shall support Meet Me (Dial In) mode: Each participant is responsible for individually initiating a call and dialing into the conference bridge.
  - c. The contractor shall support Mixed Dial mode: Providing the capability of supporting a combination or mix of both dial out and meet me (dial in) callers.

8. The contractor shall provide the capability for VTS users to request operator assistance to resolve technical issues.
9. The contractor shall maintain synchronization between the audio and video signals within  $\pm 2$  video frames to the extent possible with the video frame rate employed in the video teleconference.
10. The contractor shall allow users to establish a point-to-point VTS on demand without a reservation. Point-to-point VTS shall include full-duplex video, audio, and ancillary data transmission between participating locations.
11. The contractor shall provide VTS multi-point arrangements in conjunction with the contractor's VTS reservation system. The multi-point arrangement shall have the capability of simultaneously providing VTS to users of a different Network contractor's network and to users of public or other private networks on an off-net basis. During a multi-point conference, the addition of a party to, or the deletion of a party from, the conference shall be indicated by a tone or by a verbal or visual announcement.
12. The contractor shall provide multi-point arrangements with the following capabilities:
  - a. Voice Activation. The video signal transmitted to all VTS conference call locations is automatically switched by voice activation when the speaker's audio signal exceeds a preset level for a specified amount of time.
  - b. Continuous Presence. Multiple VTS locations may be viewed simultaneously on the same video screen. If the number of locations participating in the video conference exceeds the number being viewed via continuous presence, the selection of the video from a participating location that is displayed would be coordinated among the contractor and the participants.
  - c. Chairperson Control. The chair person in control of the VTS sends their own video or selects a return video from one of the participating locations to be sent to all participating locations. The chairperson has the capability of transferring control of the video teleconference to another presenter at his or her location.
  - d. Lecture Control (Broadcast Video with Audio Return). The video from the lecturer's location is transmitted to all VTS participants. Audio, but no video, is returned to the lecturer's location from all other participating locations. The lecturer can select one or all of the audio signals for transmission to all participants.
13. The contractor shall provide access to a secure central reservation system to permit authorized VTS users to schedule multi-point video teleconferences. For point-to-point conferences. For point-to-point conferences, reservations shall be

required only when coding conversion, format conversion, or rate adaptation features are needed, or for locations on a private network without off-net connectivity. The contractor's reservation system shall provide the following capabilities:

- a. Schedule a multi-point or point-to-point VTS conference within 30 minutes after the advance reservation request and to schedule a VTS conference up to one year in advance by voice, fax, or electronic means.
- b. The contractor shall permit VTS users to cancel a video teleconference prior to the scheduled start time of the video teleconference.
- c. Based on availability of bridging capacity and required network functions, request a delay in the scheduled termination time of a VTS conference, which is already in progress, shall be granted if the request is made at least 20 minutes before the scheduled terminating time of the VTS.
- d. The contractor shall provide the ability for VTS authorized users to schedule one or more video teleconferences by time and day of week either as a single event or recurring event on a daily, weekly, monthly or other periodic basis.
- e. The contractor shall allow users with operating at different (disparate) data rates/speeds to connect and conference at their preferred speed.
- f. The contractor shall describe the maximum conferencing capability for VTS. This includes the contractor's total overall VTS conferencing capability and the maximum number of endpoints that can participate in a single VTS multi-point conference operating at 384 Kbps.
- g. The contractor shall provide the ability to add participants or join a conference.
- h. The contractor shall provide the ability for the VTS users to schedule a "meet-me" reservation based video teleconference.
- i. The contractor shall provide the ability to obtain reservation information, only for their specific account, including all available unscheduled time slots by day, week and month.
- j. The contractor shall provide the ability to retrieve VTS reports and account information.

14. The contractor shall provide a video format conversion capability that permits operation between the following:

- a. Codec's which operate in the NTSC video format and codec's which operate in the Phase Alternation by Line (PAL) video format.
- b. Codec's which operate in the NTSC video format and codec's which operate in the Système Electronique Couleur Avec Memoire (SECAM) video format.

This is applicable when the contractor is providing the CODEC functionality.



15. The VTS shall deliver the following digital performance:
- a. When the contractor furnishes only a reservation, coding conversion, format conversion, and/or rate adaptation feature(s), the encoded audio, video, and ancillary data signals that the contractor delivers as part of VTS shall be in conformance with the signals required by the user's codec.
  - b. When the contractor furnishes the encoding/decoding function, the digital performance shall be in conformance with FTR 1080 performance at the data rate employed in the VTS.
16. The contractor shall provide VTS to any of the following service delivery points:
- a. When the VTS uses dedicated private line access, the service shall be delivered directly to one of the following: [Optional]
    - (i) Government furnished inverse multiplexer.
    - (ii) Government furnished codec. The contractor shall provide the service to the codec with or without the inverse multiplexing function according to the UNI specified.
    - (iii) Government furnished audio, video, and ancillary data source(s) inputs and outputs (e.g., cameras, speakers, microphones and data ports) of the codec that interfaces with the video teleconferencing equipment. The contractor shall provide the encoding/decoding function with or without the inverse multiplexing function according to the UNI specified.
  - b. When the VTS uses circuit switched ISDN or a private line, service shall be delivered directly to one of the following: [Optional]
    - (i) Government furnished codec.
    - (ii) Government furnished audio, video, and ancillary data source(s) inputs and outputs of the codec that interface with the video teleconferencing equipment. The contractor shall provide the encoding decoding function.
    - (iii) contractor furnished teleconferencing equipment and codec.
  - c. When the VTS uses IP communications, it shall support video communications devices that use the following protocols:
    - (i) ITU-T H.323 signaling protocol.
    - (ii) SIP (Session Initiation Protocol) IETF RFC 2543 for IP-based multimedia communications with specific media control extensions to the SIP protocol when available commercially. [Optional]
  - d. VTS for a desktop configuration shall support computer systems operating under Microsoft Windows 2K/NT or higher operating systems including the most current commercially available MS operating system.

17. The contractor's VTS shall have the ability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewalls are compatible with this service.
18. At a minimum, the contractor shall provide VTS summary and usage reports as described below. The contractor shall also make available any reports that are available to its commercial customer base.
  - a. Number and identification of video teleconferences scheduled using the reservation feature for the calendar month.
  - b. Number and identification of video teleconferences per month that did not start at the scheduled time, the cause of which was attributable to the contractor's actions.
  - c. Number and identification of video teleconferences per month which were started but then failed or suffered degraded quality due to the fault of the VTS contractor.
  - d. A directory of all locations authorized to use the VTS reservation system.
  - e. A history of reservation confirmation and cancellation notices within the reporting period.
  - f. Report on cause of unexpected VTS disconnects or non-connects.

**C.2.7.1.2 Features**

The following Video Teleconferencing Services features in section C.2.8.1.2.1 are mandatory unless marked optional:

**C.2.7.1.2.1 Video Teleconferencing Services Features**

ID Number	Name of Feature	Description
1	Attended Service	Contractor shall provide call monitoring, roll call, and coordination for a VTS conference. The contractor shall greet and introduce each VTS participant. The contractor shall verify proper conference operations prior to and during the conference to help ensure a successful VTS session.
2	Certification	The contractor shall provide pre-testing, registration, and certification that Agency owned equipment operates and is compatible with the contractor's VTS. In the event that the equipment is not certified, the contractor will notify the Agency of the deficiency and required changes to be operable with VTS.
3	Coding Conversion (Transcoding)	<ol style="list-style-type: none"> <li>1. The contractor shall provide transcoding that is compliant with FTR 1080 formats.</li> <li>2. [Optional] The contractor shall provide a coding conversion capability that permits operation between Codecs, all of which use the National Television Standards Committee (NTSC) video format, but none of which support the FTR 1080 standard and none of which use the same encoding/decoding algorithm(s). At a minimum, the contractor shall support the following compression algorithms as needed by the Agency:</li> </ol>

ID Number	Name of Feature	Description
		SG3/SG4, CTX, and CTX+. 3. [Optional] The contractor shall provide a coding conversion capability that permits operation between Codecs, all of which use the NTSC video format, in which one or more of the codec's support the FTR 1080 and in which one or more of the codec's do not support the FTR 1080. At a minimum, the contractor shall support the following compression algorithms as needed by the Agency: SG3/SG4, CTX, and CTX+.
4	Rate Adaptation	The contractor shall provide a data rate adaptation capability to ensure that all VTS locations participating in a video teleconference can interconnect with each at dissimilar data rates.
5	Security – Sensitive but Unclassified	The contractor shall provide transparent and secure VTS communications paths to support sensitive but unclassified (SBU) video communications. The security capabilities are described in the FTR1080 recommendation
6	Security-Classified (Optional)	The contractor shall provide transparent and secure VTS communications paths and support video information that is categorized as classified (National Security Agency type 1 encryption) video communications. The security capabilities are described in the FTR1080 recommendation.

### C.2.7.1.3 Interfaces

#### C.2.7.1.3.1 Network Interface

The user-to-network interfaces (UNIs) at the SDP as defined in the Section C.2.8.1.3.2 are mandatory unless marked optional:

#### C.2.7.1.3.2 Video Teleconferencing Services Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1 (Optional)	Digital Line: ISDN BRI S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 Kbps (2x64 Kbps) and multi-rate DS-0's (px64)	ITU-TSS Q.931
2 (Optional)	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
3 (Optional)	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
4 (Non Domestic / OCONUS) (Optional)	Digital Trunk: E-1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
5	All IEEE 802.3 cable and connector types	Up to 100 Mbps	IEEE 802.3. IPv4. [IPv6 when available commercially from the contractor.]

1. If the Agency provides the codec and the inverse multiplexer and the contractor provides only reservation, coding conversion, and/or format conversion, the UNIs supported shall include:
  - a. ITU-TSS V.35
  - b. EIA RS-449
  - c. EIA RS-530
  - d. RJ-x (e.g., RJ-45)
  - e. Data Interface(s) (any combination of the following data interfaces shall be supported by the VTS):
    - (i) EIA RS-232
    - (ii) EIA RS-449
    - (iii) ITU-TSS V.35
    - (iv) EIA RS-530

**C.2.7.1.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of key performance indicators (KPIs) for Video Teleconferencing Services in Section C.2.8.1.4.1 are mandatory.

**C.2.7.1.4.1 Video Teleconferencing Services Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 Hours	≤ 8 hours	
Grade of Service (Completed Service Requests)	Routine	95% of VTS conference requests met	≥ 95%	See Note 3

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that VTS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

3. The Grade of Service (completed service requests) applies to video conferences that are reserved and confirmed. It shall be calculated as the ratio of the number of locations successfully completing a VTS call divided by the total number of locations scheduling a VTS call within a calendar month. The contractor shall compute the number of completed service requests by counting the cumulative number of locations associated with each conference that were successfully completed. The contractor shall compute the number of service requests denied by counting the cumulative number of locations associated with each VTS conference that could not be scheduled for a particular date and time requested in a calendar month. VTS calls that were disconnected and then re-established only due to the fault of the contractor would be included as a denied request.

### **C.2.7.2 Audio Conferencing Service (ACS)**

The Government has a large community of audio conferencing users. The following sections provide the requirements for ACS.

#### **C.2.7.2.1 Service Description**

##### **C.2.7.2.1.1 Functional Definition**

Audio Conferencing Service (ACS) enables participants to engage in a multipoint audio conference call. The audio connection from the conference participants to the ACS conference-bridge is provided by services, such as Voice Services (VS) and Cellular/PCS Service (CPCS); and, optionally from Frame Relay Service (FRS), Asynchronous Transfer Mode Service (ATMS), and Voice over IP Transport Service (VoIPTS).

##### **C.2.7.2.1.2 Standards**

Audio Conferencing Service shall comply with the following standards, as applicable:

1. ANSI T1.101 for T1
2. ANSI T1.607 and 610 for ISDN
3. ANSI SS7, and optionally enhanced SS7 standards for interworking [e.g., address translation] between circuit-switched network and IP network
4. Telcordia Notes on the Networks (SR-TSV-2275), currently Issue 4, October 2000
5. IETF RFC 3661 through 3665 for SIP (Session Initiation Protocol) [Optional]
6. IETF RFC 3435 for MGCP (Media Control Gateway Protocol) [Optional]
7. ITU-TSS H.323/225/245/248 (enhanced for VoIP) [Optional]

##### **C.2.7.2.1.3 Connectivity**

Audio Conferencing Service shall connect to and interoperate with:

1. Government specified locations (i.e., at SDPs, such as single-line telephones, multiline key telephone systems, conference-room audio equipment, PBX, Centrex; and, optionally Workstation/PC based soft-phone)
2. Public Switched Telephony Network (PSTN)
3. Internet (for VoIP) [Optional]
4. Contractor's network, if applicable; and, optionally to all other Network contractors' and Government specified networks for
  - a. Circuit-switched services (for Voice and Cellular/PCS)
  - b. IP service (for VoIP) [Optional]
  - c. Frame Relay service (for VoFR) [Optional]
  - d. ATM service (for VoATM) [Optional]

#### C.2.7.2.1.4 Technical Capabilities

The following Audio Conferencing Service capabilities are mandatory unless marked optional:

1. **Multipoint Bridging Capability.** The bridging capability shall allow selective two-way or one-way conversations between conferencing ports; i.e., it shall allow a subset of conferees to participate in a two-way conference while the remaining conferees are listeners only. During the conduct of a multipoint conference, the addition of a party to, or the deletion of a party from, the conference shall be indicated by a tone or by a verbal announcement.
2. **Conference Set-up Capability.** The contractor shall provide the following conference set-up support services:
  - a. **User-Controlled Conference.** This capability shall allow authorized users and users with an authorization-code/calling-card to establish a conference call by dialing a designated number to access the service. If calling card is used, all charges shall be billed against the calling card. The following two automated modes of user-initiated conferencing capabilities shall be supported:
    1. **Meet-Me Conference** - This capability shall allow each user to be connected in a Conference by dialing a designated number and authorization code at a predetermined time or as directed by the operator. For recurring meet-me conferences, the contractor shall permit the participants to reuse the same dial access number and authorization code and allow bookings of recurring conferences in three month increments (e.g., every Monday morning at 10:00 AM for the next three months).

2. **Preset Conference** - This capability shall allow an authorized user to activate a previously defined conference with associated conferees by dialing an access number followed by an authorization code. Once activated, the system shall attempt to connect the pre-designated participants using the predefined lists.
  - b. **Attendant-Assisted Conference.** This capability shall allow operators to establish a conference. Conferees shall be able to recall an operator during a conference for immediate attention, such as general assistance or adding or dropping participants.
3. **Audio Conference Reservation System.** The audio conference reservation system shall permit authorized Government users to schedule audio conferences. The reservation system shall have the following capabilities:
  - a. A single point of contact with the contractor (preferably, the Customer Service Center) to schedule reservation-based audio conferences.
  - b. Ability for authorized users to schedule one or more conferences by time and day of the week either as a single event or recurring event on a daily, weekly, monthly, or other periodic basis. In addition, it shall be possible to schedule an emergency audio conference call within 15 minutes if bridging capacity is available.
  - c. The ability for authorized users to submit reservation requests up to one year in advance by phone or E-Mail or fax or via online through Internet.
  - d. The ability to store and retrieve predefined conferences.
  - e. The ability to create printed reports with reservation confirmation and cancellation notices.
  - f. The reservation system shall contain the following information:
    1. Type of conference (e.g., video, audio)
    2. Name of the person scheduling the conference
    3. Organization of the person scheduling the conference
    4. Telephone number of the person scheduling the conference
    5. Name of an alternate contact person
    6. Telephone number of the alternate contact person
    7. Name of the contact person at participating locations (attendant- assisted only)
    8. Telephone numbers of the contact persons participating in the conference (attendant-assisted only)
    9. Name, organization, telephone number, and email address of each person participating in the conference (at the user's discretion)

10. Locations of the persons participating in the conference (at the user's discretion)
  11. Date of the conference
  12. Time of the conference
  13. Scheduled length of the conference
  14. Email confirmation notification to each participants with conference details (at the user's discretion)
  15. Authorization code or calling card number
4. Audio Conferencing Service shall provide users with the following service intervals:
- a. Schedule a non-recurring conference within 30 minutes after the advance reservation request, provided that the bridging capacity and the other required network support functions are available.
  - b. When bridging capacity and other required network support functions are available, requests for a delay in the scheduled termination time of a conference that is already in progress shall be granted if the request is made at least 20 minutes before the scheduled terminating time of the conference.
  - c. Permit ACS users to cancel an audio conference up to 30 minutes before the scheduled start time of the conference without incurring any charge for the canceled conference.
5. Automatic port expansion. This capability shall allow, without operator assistance, automatic expansion to additional ports to the conference in progress beyond the dial-in ports reserved as long as facilities are available.
6. Announce late participant. This capability shall provide either the announcement of participants arriving late to the call or blocking of late participants from joining the conference based on user's instruction.
7. Enable and disable conferee tones. This capability shall enable or disable conferee tone when a participant enters or exit a conference.
8. Enable and disable music on hold. This capability shall enable or disable music on hold when a participant is put on hold.
9. Enable and disable self mute. This capability shall provide self mute if this capability is not available on their phone.
10. Guaranteed duration of dial-in call. This capability shall provide guaranteed duration of dial-in call and shall allow participants to hang up at any time and rejoin the conference later.



11. Listen-only broadcast mode. This capability shall allow listen-only broadcast mode.
12. Mixed mode. This capability shall provide mixed mode, i.e., both listen-only and interactive modes.
13. Participant count. This capability shall provide a count of participants.
14. Roll call. This capability shall require the operator to conduct a roll call of participants so that all participants know who are on the conference.
15. Audio Conferencing Service shall be available 24 hours a day, seven days a week.
16. Attendant assistance shall be available at any time during an audio conference.

**C.2.7.2.2 Features**

The following Audio Conferencing Service features in Section C.2.8.2.2.1 are mandatory unless marked optional. In addition, any other features available commercially are included in the scope of the contract.

**C.2.7.2.2.1 Audio Conferencing Service Features**

ID Number	Name of Feature	Description
1	Audio recording of call [Optional]	The contractor shall allow recording of conference call into a storage- media (e.g., disc or cassette tape) for later replay.
2	Access Controlled Call	The contractor shall allow the conference leader to prevent operator from monitoring the call as well as additional/late participants from joining the call
3	Language translation [Optional]	The contractor shall provide language translation to English from other languages (e.g., Spanish) for transcription of pre-recorded audio conference.
4	Moderator led questions and answers	The contractor shall provide conference moderator led questions and answers only.
5	Participant list report	The contractor shall provide a report of all participants in the conference.
6	Password screening	The contractor shall screen password for joining a conference to authorized participants only.
7	Replay of pre-recorded audio conference [Optional]	The contractor shall allow, under password protection, replaying of pre-recorded audio conference at a later time and shall allow remote control of the recording with keypad access to functions like pause, rewind, and fast-forward.
8	Transcription of pre-recorded audio call [Optional]	The contractor shall provide transcription of pre-recorded audio call.
9	Temporary blocking of ports	The contractor shall allow temporarily blocking audio conference ports in order to remove a sub-set of participants/users from the conference.
10	Secured Audio	The contractor shall support voice conferencing capability for

ID Number	Name of Feature	Description
	Conference [Optional]	sensitive voice conferences with end-user encryption to support discussions of a sensitive-but-unclassified (SBU) nature between multiple locations with protection from unauthorized interception (i.e., eavesdropping). [Note. Government furnished encryption unit at the SDP will be based on commercially available encryption devices (Standard: NIST DES/AES). The contractor must synchronize encryption key of similar encryption unit(s) of the audio conference bridge before each conference.]

### C.2.7.2.3 Interfaces

The following interfaces at the SDP for audio connection to the conferencing-bridge as defined in Section C.2.8.2.3.1 below, unless marked optional, if the contractor does not provide any of these services: VS, FRS, ATM, and CPCS.

#### C.2.7.2.3.1 Audio Conferencing Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
2	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
3	Digital Trunk: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
4 (Non-US)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702) (Optional)	Up to 1.92 Mbps	SS7, E1 Signaling
5 (Non-US)	Digital Trunk: E3 Channelized (Std: ITU-TSS G.702) (Optional)	Up to 30.72 Mbps	SS7, E1 Signaling

### C.2.7.2.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Audio Conferencing Service in Section C.2.8.2.4.1 are mandatory unless marked optional.

#### C.2.8.2.4.1 Audio Conferencing Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
GOS (Operator Assistance Response Delay)	Routine	54 seconds	≤ 54 seconds	See Note 3

##### Notes:

1. ACS availability is calculated as a percentage of the total reporting interval time that ACS is operationally available to the Agency. Availability is computed by the standard formula:
 
$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
2. Refer to Section C.3.3.1.2.4 for definition and how to measure.
3. GOS (Operator Assistance Response Delay) is the delay experienced by conference participants to receive operator assistance during a conference. Delay is measured as the interval between the end of signaling (e.g., dialing for operator assistance) and the receipt of voice response from the operator.

#### C.2.7.3 Web Conferencing Service (WCS)

Web Conferencing Services (WCS) enables Agencies to enhance traditional conferencing by offering the capability to meet, present, and interact with information via a web browser. WCS is typically used in conjunction with an audio and/or video connection. Agencies can utilize WCS to effectively disseminate information quickly and easily, reduce the cost of training and educational programs, and permit individuals and groups to participate in activities they otherwise would be unable to attend due to a variety of conflicts.

##### C.2.7.3.1 Service Description

###### C.2.7.3.1.1 Functional Definition

Web Conferencing Service allows Agencies to share information, documents, or applications interactively via the Internet between remote participants. WCS enables Agencies to improve productivity and communicate more efficiently by offering secure, reliable, and user friendly web conferencing.

###### C.2.7.3.1.2 Standards

Web Conferencing Service shall comply with the following standards and recommendations, as applicable. After award, the contractor may propose alternatives

at no additional cost to the Government that meet or exceed the provisions of the standards listed.

1. Hyper Text Transfer Protocol (HTTP)
2. Hyper Text Transfer Protocol Secure (HTTPS)
3. IETF RFC 3261 for Session Initiation Protocol (SIP)
4. ITU-T T.120 Series of Data Protocols for Multimedia Conferencing
5. Secure Sockets Layer (SSL) Encryption Secure Sockets Layer
6. Transmission Control Protocol/Internet Protocol (TCP/IP) Suite
7. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

#### **C.2.7.3.1.3 Connectivity**

Web Conferencing Service shall connect to and interoperate with:

1. Internet

Web Conferencing Service shall be accessible via a Universal Resource Locator (URL) address. Agency Internet access to WCS is not included as part of this service.

#### **C.2.7.3.1.4 Technical Capabilities**

The following Web Conference Service capabilities are mandatory:

1. The contractor shall provide a capability that enables participants to collaborate. This shall include real time document sharing, file transfer capability and electronic whiteboards in a private and secure WCS session.
2. The contractor shall provide the following are minimum capabilities:
  - a. The contractor shall provide authentication and password protection
  - b. The contractor shall provide a customized greeting (or message) screen
  - c. The contractor shall provide Online Help
  - d. The contractor shall provide support point-to-point and multi-point web conferences
3. The contractor's WCS shall interoperate with the Internet and subscribing Agencies' IP network(s).
4. The contractor's WCS shall be compatible with commercially available Internet web browser software packages.
5. The contractor shall provide a means by which users can test and verify that their web browser and desktop software are compatible with WCS service prior to the scheduled conference. If required, the contractor shall provide the appropriate "plug ins" in order to deliver WCS to the subscriber. The browser "plug in" software shall be limited to utilities required for the user to playback, participate in, or lead a web conference session. This can include "plug ins" that enable Agency users to playback recorded conferences from their web browser, develop

WCS presentation slides within existing Agency owned software applications (i.e. Microsoft PowerPoint) or view WCS from mobile devices such as a Personal Digital Assistant (PDA) where applicable.

6. The contractor's WCS shall support dynamic content, i.e., the ability to use Audio Visual Interleave (AVI's) files, flash, animated gif, and dynamic html pages.
7. The contractor's WCS shall be available on demand within 30 minutes prior to the requested conference time and via scheduled reservation with a single point of contact.
8. The contractor shall provide a reservation system shall provide the ability for authorized WCS users to schedule or cancel one or more web conferences within at least one year in advance. Scheduling can be by time and day of the week either as a single event or recurring event on a daily, weekly, monthly, or other periodic basis.
9. The contractor shall provide an e-mail notification with a meeting invitation and RSVP to WCS participants.
10. The contractor's WCS shall offer the capability to extend the scheduled conference time upon request from the subscribing Agency and to add participants.
11. The contractor's WCS shall be secure and offer authentication and encryption capabilities to identify and authenticate subscribers who are authorized access to WCS before providing such access.
12. The contractor's WCS shall be accessible via a Universal Resource Locator (URL) address with a login and password for valid participants.
13. The contractor shall provide passwords for both conference leaders and participants.
14. The contractor's WCS shall provide the capacity to support at least 31 simultaneous participants in an individual web conference. The contractor shall also state the maximum conferencing capacity (e.g. both the number of simultaneous web conferencing participants and conferences) for the WCS.
15. The contractor's WCS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.
16. The contractor shall provide the capability for subscriber's to request operator assistance to immediately resolve any technical or WCS service issues or problems.
17. The contractor's WCS shall annotation, which is the ability to emphasize a specific area of a presentation slide with a marker or pointer tool.
18. The contractor's WCS shall provide a participant list, which is the ability to view the names of other participants attending the WCS presentation (e.g. audience-viewing list).

19. The contractor's WCS shall provide the ability to for the conference leader to control and share a remote participant's desktop application. Authorized participants shall be provided with the capability to remotely access a conference participant's personal computer. The remote conference participant shall be notified when the authorized party is requesting remote access to their personal computer and have the capability to allow or reject the request before granting access.
20. The contractor shall provide the capability for group web surfing, which is the ability for the conference leader to guide and navigate WCS participants to a web page.
21. The contractor shall support file transfer. File transfer is the ability to upload a file and have the WCS participant able to download it within the meeting or event. The file transfer can be sent to all participants or selected participants. The receiving participant shall have the option to accept or reject the file transfer.
22. The contractor shall allow multiple presenters on a WCS meeting or event.
23. The contractor shall provide a polling and voting capability. This allows the conference leader to pose questions and receive feedback from participants during a presentation with a variety of different answer sets (multiple choices, open ended, yes/no) on demand. The participant shall have the capability to signal the conference leader when they have a question.
24. The WCS polling/voting feedback capability shall be available instantly for the WCS conference leader and if requested, via a polling/voting results report.
25. The contractor shall provide privacy, which is the ability for the conference leader to lock and unlock access to the meeting. When the meeting is "locked," no additional participants can join the active conference. [Optional]
26. The contractor shall provide the capability for conference leaders to print the presentation used during the WCS or save it to a file. Participants shall have the same capability if permitted by the conference leader.
27. WCS shall support text chat, which enables real time text communications between WCS conference participants. The chat shall provide options for a public text chat for all participants with the conference leader and private chats between select participants.
28. The contractor shall provide the capability to present a survey to all or a random percentage of participants to gather feedback and/or capture customer satisfaction data.

### C.2.7.3.2 Features

The following Web Conferencing Service features in Section C.2.8.3.2.1 are mandatory:

#### C.2.7.3.2.1 Web Conferencing Service Features

ID Number	Name of Feature	Description
1	Streaming Audio	The contractor shall provide the ability to deliver one way audio over the Internet during a WCS session. The streaming audio shall be synchronized with any data portions of the web conference.
2	Streaming Video	The contractor shall provide the ability to deliver one way video over the Internet during a WCS session. The streaming video shall be synchronized with any data portions of the web conference.
3	Web Based Presentation Replay	The contractor shall provide the capability to replay (or playback) web based presentations for participants that were unable to attend the live conference. The replay shall be available for a minimum of 30 days after the initial conference. The contractor shall provide the Agency an option for extending the conference replay, in 30 day increments, for a period of 1 year.

#### C.2.7.3.3 Interfaces

Not applicable. Web Conferencing Service is an application-layer service.

#### C.2.7.3.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of key performance indicators (KPI's) for Web Conferencing Services in Section C.2.8.3.4.1 below are mandatory.

##### C.2.7.3.4.1 Web Conferencing Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.7%	≥ 99.7%	See Note 1
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that WCS is operationally available to the Agency. Availability is computed by

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

the standard formula :

2. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

## **C.2.8 Managed Networking Services**

### **C.2.8.1 Managed Network Services (MNS)**

Managed Network Services (MNS) enable an Agency to obtain design and engineering, implementation, management, and maintenance services for Agency networks. MNS provide the necessary technical and operational capabilities that ensure the availability and reliability of Agencies' increasingly complex networks.

#### **C.2.8.1.1 Service Description**

##### **C.2.8.1.1.1 Functional Definition**

MNS offer comprehensive network management solutions to meet Agency requirements. Under the MNS offering, the contractor provides overall management of an Agency's network infrastructure. In addition, the contractor provides real-time proactive network monitoring, rapid troubleshooting and service restoration. Agencies need contractor support for networks of varying complexity in terms of size, bandwidth, and functionality. The contractor is the Agency's single point of accountability for all networks managed under this service, including operations, maintenance, and administration activities.

##### **C.2.8.1.1.2 Standards**

Managed Network Services shall comply with the following standards, as applicable:

1. The specific Standards and recommendations identified in the Agency task order.
2. All appropriate standards for any applicable underlying Network access and transport services

##### **C.2.8.1.1.3 Connectivity**

MNS shall work with underlying Network offerings such as Frame Relay, ATM, IP-Enabled Frame Relay/ATM, IP, IP Virtual Private Network (VPN), Private Lines and other services as needed, to ensure seamless connectivity to Agency networking environments.

##### **C.2.8.1.1.4 Technical Capabilities**

The following Managed Network Services capabilities shall be provided by the contractor, and will be procured by the Agencies as required to meet Agency needs:

###### **C.2.8.1.1.4.1 Design and Engineering Services**

1. The contractor shall provide design and engineering services that fully satisfy Agency requirements. Design and engineering services include a review of the current network traffic, performance, transport, hardware and software components; and an overall evaluation of network topology, configuration, addressing, bandwidth, availability, scalability, reliability, and disaster recovery requirements. The contractor shall document the design and engineering services. The contractor shall also review the design and engineering services that have been implemented to ensure that ongoing Agency needs are satisfied.



2. The contractor shall incorporate the Agency's security requirements into the design to ensure that all factors influencing data and circuit integrity are captured. This may include the integration of a security package or individual Network security services.
3. The contractor shall identify network components, and determine protocols, redundancy, traffic filtering, and traffic prioritization requirements. The contractor shall also recommend the appropriate Committed Information Rates (CIRs), Permanent Virtual Circuit (PVC) levels, and network access speeds, as required.
4. The contractor shall provide complete project management including design, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. The contractor shall coordinate installation activities with the Agency in order to minimize the impact on the current networking environment.

#### **C.2.8.1.1.4.2 Implementation, Management and Maintenance**

1. The contractor shall provide integrated management of services, to the extent needed by the Agency that includes managing services that are delivered to the Agency by other contractors.
2. The contractor shall develop, implement, and manage comprehensive solutions constructed from components of the Network services and their enhancements, in order to meet Agency-specific requirements. The solutions shall include but not be limited to:
  - a. Access solutions that use a combination of different services, such as Wireline and Wireless Access Services, for specific Agency locations, and also Satellite Access Arrangements at particular locations to meet Agency performance metrics for availability and disaster recovery
  - b. Transport solutions that distribute traffic over multiple contractor backbone networks to provide redundancy and carrier diversity, and vary the traffic allocation dynamically based on Agency-specified performance requirements
  - c. Customer premises solutions that provide Agency-specific interfaces, software, and equipment to meet Agency requirements
  - d. Security Solutions as required by the Agency
3. The contractor shall supply and manage the hardware, firmware, and related software required by the Agency. Components include but are not limited to routers and switches, ATM devices, CSUs/DSUs, hubs, ISDN adapters, and modems.
4. The contractor shall manage the network in real-time on a 24x7, basis. The contractor shall support remote management capabilities from its operations center, including but not limited to, equipment configuration, testing, monitoring, troubleshooting, fault/problem resolution, and maintenance. The contractor shall proactively monitor utilization and packet loss and errors, probing in intervals of

at least fifteen minutes to ensure proper equipment/network operation and performance.

5. The contractor shall support SNMP data feeds that provide the Agency with managed equipment information, as applicable.
6. The contractor shall perform configuration changes that include but are not limited to the following:
  - a. Adding a protocol
  - b. Adding, moving or removing Customer Premises Equipment (CPE)
  - c. Changing addressing, filtering, and traffic prioritization schemes
  - d. Modifying PVCs
  - e. Optimizing network routes
  - f. Updating equipment software and/or configuration, including but not limited to firewall and VPN security devices
  - g. Upgrading or downgrading bandwidth
7. The contractor shall provide IP Address Management as applicable. The contractor shall supply registered IP addresses to the Agency as required, and assist in the translation of non-registered private IP addresses into public addresses for routing purposes.
8. The contractor shall monitor and control access to equipment under its control including limiting access to authorized personnel, and implementing passwords and user permissions as directed and approved by the Agency.
9. The contractor shall regularly perform off-site equipment configuration backups, in order to ensure the availability of recent configuration data for restoration purposes. The contractor shall provide the Agency secure access to backup logs as needed.
10. The contractor shall perform the necessary hardware and software upgrades, updates, patch deployments and bug fixes as soon as they become available. The contractor shall implement updates in coordination and mutual agreement with the Agency; and test new releases to resolve any security concerns, ensure compatibility with the Agency environment, minimize service disruptions, and maintain equipment functionality.
11. The contractor shall proactively detect problems, respond to alerts and promptly report situations that adversely affect throughput to the impacted Agency. The contractor shall provide notification of alarms, network troubles and service interruptions via email, pager, telephone, or as directed by the Agency.
12. The contractor shall provide the Agency with real-time access to the following:
  - a. Installation schedule detailing the progress of activities such as the implementation of equipment, access and transport circuits, ports, and PVCs, as applicable. This allows Agencies to track the provisioning

process through completion at any time. Near real-time access to the installation schedule is acceptable

- b. Network statistics and performance information including equipment data; availability, throughput and delay statistics; Class of Service (CoS) settings; and application-level performance information, as applicable
- c. Trouble reporting and ticket tracking tools
- d. Security logs

13. The contractor shall provide the Agency with secure access to current and historical information which shall include, but not be limited to, the following as applicable:

- 1. Bandwidth and service quality information
- 2. Burst analysis identifying under or over utilization instances
- 3. Data errors
- 4. Delay, reliability, data delivery summaries
- 5. End-to-end network views
- 6. Exception analysis
- 7. Link, port and device utilization
- 8. Network statistics
- 9. Protocol usage
- 10. PVC, DLCI, and CPU utilization
- 11. Traffic, PVC, port and protocols views

**C.2.8.1.2 Features**

The Managed Network Services features in Section C.2.9.1.2.1 below are mandatory:

**C.2.8.1.2.1 Managed Network Services Features**

ID Number	Name of Feature	Description
1	Government Furnished Property (GFP) Maintenance	The contractor shall maintain and repair Government Furnished Property if not maintained under a SED monthly maintenance charge
2	Agency-Specific Network Operations Center (NOC)	The contractor shall provide Agency-specific help desk services and shared or dedicated Network Operations Centers (NOCs) to meet Agency requirements.
3	Network Testing	The contractor shall support Agency-specific development services which address the Agency's potential need to test equipment, software and applications on the contractor's network prior to purchase and deployment. This shall cover voice, data, and video technologies including but not be limited to ATM, Frame Relay, IP VPN, ISDN, Voice over Frame (VoFR), and Voice over Internet Protocol (VoIP). Testing shall be

ID Number	Name of Feature	Description
		performed at the Agency's discretion and structured in collaboration with the contractor.

**C.2.8.1.3 Interfaces**

Managed Network Services shall support the User-to-Network Interfaces (UNIs) defined in the following Sections as applicable:

1. C.2.3.1 Frame Relay Service (FRS) [Optional]
2. C.2.3.2 Asynchronous Transfer Mode Service (ATMS) [Optional]
3. C.2.5.1 Private Line Services (PLS) [Optional]
4. C.2.4.1 Internet Protocol Service (IPS)
5. C.2.7.2 Premises-based IP VPN Services (PBIP-VPNS) [Optional]
6. C.2.7.3 Network-based IP VPN Services (NBIP-VPNS)

The service shall also support the UNIs for all underlying Network access and transport services implemented using MNS, as required.

**C.2.8.1.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Managed Network Services in Section C.2.9.1.4.1 are mandatory. In addition to the components specified in Section C.2.9.1.4.1, contractors may provide KPIs applicable to their MNS offering:

**C.2.8.1.4.1 Managed Network Services Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (Network End-to-End)	Routine	99.9%	≥ 99.9%	See Note 1
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Agencies can specify and request performance metrics that modify and/or augment these KPIs in their task order, on an individual case basis, in order to meet Agency-specific needs. Modifications can include how specific KPIs shall be measured and monitored. The contractor shall provide services at the performance levels specified by the Agency.

## Notes:

1. MNS availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the service is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(MNS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

## C.2.9 Security Services

### C.2.9.1 Managed Firewall Service (MFS)

Managed Firewall Service (MFS) is implemented to secure internal networks. Similar to commercial enterprises, Agencies face increasing network security risks which they seek to mitigate. This offering is one of the security tools that will help reduce service disruptions caused by malicious access. MFS will prevent unauthorized access to or from private networks, such as Local Area Networks (LANs).

#### C.2.9.1.1 Service Description

##### C.2.9.1.1.1 Functional Definition

MFS safeguards internal networks and systems from hostile activity, protecting critical data from compromise and tampering. As buffers between trusted internal networking environments and external networks, firewalls inspect traffic according to a set of defined security policies, blocking all traffic not meeting the Agency's criteria. MFS may consist of a hardware or software solution. The service can be implemented on servers, routers, as standalone firewall hardware, or be network-based which removes the need for additional on-site equipment and/or software. In the case of premises-based firewalls, the policies can be tailored for specific locations. On the other hand, network-based firewalls enable Agencies to deploy a common set of policies across several locations. The service provides design, implementation, monitoring, maintenance, and ongoing management of the solution.

##### C.2.9.1.1.2 Standards

Managed Firewall Service shall comply with the following standards, as applicable. The contractor may offer alternatives, for Government consideration, that meet or exceed the provisions of the standards listed below:

1. E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
2. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 140 - 2 — Security Requirements for Cryptographic Modules

3. NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems
4. NIST Special Publication (SP) 800-41 — Guidelines on Firewalls and Firewall Policy
5. United States Computer Emergency Readiness Team (US-CERT) reporting requirements
6. All new versions, amendments, and modifications of the above when offered commercially
7. All appropriate standards for any applicable underlying Network access and transport services

#### **C.2.9.1.1.3 Connectivity**

Managed Firewall Service shall connect to and interoperate with the Agency networking environment, including Demilitarized Zones (DMZs) and secure LANs, as required by the Agency. The service shall also support connectivity to extranets and public networks such as the Internet.

#### **C.2.9.1.1.4 Technical Capabilities**

The following Managed Firewall Service capabilities are mandatory:

1. The contractor shall provide firewall software and hardware components, including log servers, as applicable. The service shall include the following, as required by the Agency:
  - a. Premises-based firewalls
  - b. Network-based firewalls
  - c. Application/proxy-based firewalls
2. The contractor shall support remote monitoring capabilities; and proactively monitor the firewall, including hardware/software components, on a 24x7 basis.
3. The contractor shall monitor the overall performance of the firewall, including monitoring the adequacy of the firewall as the network expands.
4. The contractor shall ensure that firewall statistics and logs are sent to the contractor's operation center via secure means.
5. The contractor shall implement firewall security policies according to the Agency's needs.
6. The contractor shall detect suspicious activity and policy violations.
7. The contractor shall employ various protection techniques including but not limited to:

- a. Stateful Packet Inspection by which the firewall goes beyond just examining a packet's source and destination, but also verifies its legitimacy. The firewall confirms requests made, and matches open connections to valid packets prior to allowing them through the network.
  - b. Network Address Translation (NAT) and Port Address Translation (PAT) in order to disguise internal IP addresses, shielding systems from the outside world, especially from malicious activity.
8. The contractor shall guard the Agency's networks from attacks, including but not limited to:
  - a. Denial of Service (DOS) assaults which flood the network with false requests, overwhelming servers and eventually causing them to crash.
  - b. Ping of Death or Long Internet Control Message Protocol (ICMP) attacks in which packets larger than 65,536 bytes are sent deliberately in an attempt to crash the system.
  - c. IP Spoofing attacks in which packets' IP addresses are disguised. These packets appear to have originated from a trusted source with appropriate authorization or privileges.
  - d. SYN Flood attacks which clog connections and prevent legitimate session requests from being established.
  - e. Tear Drop attacks in which packet fragments are deliberately designed to disrupt proper packet reassembly at the receiving end.
9. The contractor shall block hostile Java applets, JavaScript, and ActiveX controls to guard against potentially unsafe code, as required. The contractor shall also block cookies and web bugs, as required.
10. The contractor shall maintain a problem detection system for the diagnosis of alerts and violations.
11. The contractor shall notify the Agency of events via email, pager, fax, or telephone, as directed by the Agency.
12. The contractor shall provide the Agency with secure web access to the service in order to request/perform security policy updates, report troubles, track status of reported problems, obtain firewall logs, and administer user databases, as needed. The information shall contain but not be limited to the following, as applicable:
  - a. Active Surfers
  - b. Authentication Reports
  - c. Change Requests
  - d. Configuration Modifications
  - e. Connections/Attempts - Accepted/Rejected

- f. Events
  - g. Firewall Statistics
  - h. Firewall Utilization
  - i. FTP Connections Counts
  - j. HTTP Destinations Counts
  - k. IP Addresses
  - l. Mail Statistics
  - m. Originating and terminating addresses
  - n. Outages
  - o. Port Activity
  - p. Protocol Data for HTTP, HTTPS, FTP, SMTP, and Telnet
  - q. Rule Violations
  - r. Tickets
  - s. URL and Visited Websites Reports
  - t. Web Hits per specified period
13. The contractor shall maintain the latest configuration information for restoration purposes.
14. The contractor shall maintain the firewall, performing the necessary hardware/software upgrades, updates, and necessary replacements.
15. The contractor shall test and deploy the latest patches and bug fixes as soon as they become available and are approved by the Agency, in order to ensure optimal performance of the firewall.
16. The contractor shall perform configuration and change management, including modifying the following attributes, as applicable and as requested by the Agency:
- a. Filtering and blocking requirements
  - b. Firewall policies and rules
  - c. Virtual Private Networks (VPNs) characteristics
  - d. IP Hosts such as Web and mail servers impacted by the firewall
  - e. Protocols
  - f. User/groups
17. The contractor shall perform firewall security scans capable of detecting open port vulnerabilities in order to ensure that the firewall is secure.



18. The contractor shall provide DNS and SMTP configuration support to ensure the firewall is appropriately set-up to handle DNS queries and mail traffic, as required.
19. The contractor shall support firewalls of varying complexity, in terms of size, performance, and capabilities.

### C.2.9.1.2 Features

The Managed Firewall Service features in Section C.2.10.1.2.1 are mandatory unless marked optional:

#### C.2.9.1.2.1 Managed Firewall Service Features

ID Number	Name of Feature	Description
1	Demilitarized Zones (DMZs) Support	The contractor shall support connections to Demilitarized Zones (DMZs) which serve as buffers between the Agency's private networks and outside public networks. DMZs can apply to Web (HTTP), FTP, email (SMTP), and DNS servers.
2	Email Security	The contractor shall support email security measures that can conceal, limit, or change information about the Agency's networks or domains, reducing visibility to outsiders. The contractor shall also have the capability to block email attachments that are above a specified size.
3	Extranet Support	The contractor shall support connections to extranets which can facilitate inter-Agency interactions, or enable the Agency to interface with various trusted stakeholders, such as contractors or vendors for example.
4	Fast Ethernet Connection	The contractor shall support fast Ethernet connections (100BaseT/1000BaseT) which provide greater data flows from the firewall to the Agency's internal networks.
5	Firewall Load Balancing	The contractor shall implement a hardware or software load balancing capability, as required by the Agency. The service shall distribute traffic across multiple firewalls, in order to minimize potential downtime caused by any single point of failure. This provides firewall scalability, ensures availability, and adds further safeguards against hardware and software problems.
6	Firewall Redundancy	The contractor shall provide a firewall redundancy solution based on a dual firewall systems approach, in a primary/secondary set-up. The system, comprised of hardware and software as applicable, will enable automatic transfers from one system to the next in case of severe hardware/software failures to maintain availability of the firewall.
7	Firewall-to-Firewall VPNs	The contractor shall support firewall-to-firewall VPNs which establish secure tunnels between Agency firewalls, and also between firewalls and the contractor's operation center.
8	Personal Firewalls (Optional)	The contractor shall provide personal firewalls or personal firewall appliances in order to secure remote personal computers or small remote networks (i.e., home offices), as required by the Agency.
9	Remote Client VPNs	The contractor shall provide remote Agency users with secure access to the network, employing VPN encryption technology.
10	Uniform Resource Locator (URL)	The contractor shall support URL blocking, as required. URLs may fall in categories such as:

ID Number	Name of Feature	Description
	Filtering	<ol style="list-style-type: none"> <li>1. Advertisements (i.e., banner ads)</li> <li>2. Computer Hacking</li> <li>3. Criminal Skills</li> <li>4. Drugs, Alcohol &amp; Tobacco</li> <li>5. Extremists</li> <li>6. Gambling</li> <li>7. Hate Promotion</li> <li>8. Illegal or Questionable Sites</li> <li>9. Online Gaming (Non-Gambling)</li> <li>10. Satanism and Cults</li> <li>11. Search Engines</li> <li>12. Sexually Explicit/Adult Material</li> <li>13. Sports and Leisure</li> <li>14. Violence or Profanity</li> </ol>
11	User Authentication Integration	<p>The contractor shall support the integration of the firewall service with the Agency's own authentication services, as specified by the Agency. The Agency may employ several user authentication tools such as, but not limited to:</p> <ol style="list-style-type: none"> <li>1. Lightweight Directory Access Protocol (LDAP)</li> <li>2. Microsoft Active Directory</li> <li>3. Microsoft Windows NT</li> <li>4. Operating System passwords</li> <li>5. Remote Authentication Dial-In User Service (RADIUS)</li> <li>6. RSA SecureID</li> <li>7. Terminal Access Controller Access Control System (TACACS), Extended TACACS (XTACACS), or TACACS+</li> </ol>

### C.2.9.1.3 Interfaces

Managed Firewall Service shall support the User-to-Network Interfaces (UNIs) defined in the following Sections, as applicable.

1. C.2.3.1 Frame Relay Service (FRS) [Optional]
2. C.2.3.2 Asynchronous Transfer Mode Service (ATMS) [Optional]
3. C.2.4.1 Internet Protocol Service (IPS)
4. C.2.7.2 Premises-based IP VPN Services (PBIP-VPNS) [Optional]
5. C.2.7.3 Network-based IP VPN Services (NBIP-VPNS)

**C.2.9.1.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Managed Firewall Service in Section C.2.10.1.4.1 are mandatory:

**C.2.9.1.4.1 Managed Firewall Service Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Event Notification (EN)	Routine	Next business day for a Low category event	≤ Next business day	See Note 2
		Within 4 hours of a Medium category event	≤ 4 hours	
		Within 30 minutes of a High category event	≤ 30 minutes	
Grade of Service (Configuration/Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	See Note 3
		Within 2 hours for an Urgent priority change	≤ 2 hours	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. MFS availability is calculated as a percentage of the total reporting interval time that the MFS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(MFS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification of the Agency. Events are categorized as follows:
  - a. Low — Events in the Low category have a negligible impact on service. They include firewall incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.
  - b. Medium — Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.
  - c. High — Events in the High category represent firewall violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software

and configuration problems, and are immediately reported via email, pager, or telephone, as specified by the Agency.

3. The Grade of Service (Configuration/Change) value represents the elapsed time between the configuration/change request and the change completion. Changes are initiated and prioritized by the Agency, or may be implemented in response to an event. Changes initiated by the contractor require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
4. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

### **C.2.9.2 Intrusion Detection and Prevention Service (IDPS)**

Agency enterprise networks, like their commercial counterparts, continue to be challenged with increasing security risks. Intrusion Detection and Prevention Service (IDPS) will serve as a component of the Agency's security infrastructure by providing an extra layer of protection for its internal networks. IDPS is a security offering that helps reduce network service disruptions caused by malicious attacks.

#### **C.2.9.2.1 Service Description**

##### **C.2.9.2.1.1 Functional Definition**

IDPS consists of software and hardware components that enable the monitoring and identification of potential security threats. The service detects signs of intrusion that may jeopardize the confidentiality, integrity, availability, and control of Agency networks. IDPS provides intrusion sensors that analyze packet activity for indications of network attack, misuse, and anomalies. The service then generates alerts and records suspicious events. In addition, IDPS provides immediate corrective responses that stop or alleviate malicious attacks, which include dropping or rerouting malicious packets.

##### **C.2.9.2.1.2 Standards**

Intrusion Detection and Prevention Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
2. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 140 - 2 — Security Requirements for Cryptographic Modules
3. NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems
4. NIST Special Publication (SP) 800-31 — Intrusion Detection Systems (IDS)
5. United States Computer Emergency Readiness Team (US-CERT) reporting requirements
6. All new versions, amendments, and modifications of the above when offered commercially

7. All appropriate standards for any applicable underlying Network access and transport services

#### **C.2.9.2.1.3 Connectivity**

Intrusion Detection and Prevention Service shall connect to and interoperate with the Agency networking environment, including Demilitarized Zones (DMZs) and secure LANs. The service shall also support connectivity to extranets and public networks such as the Internet.

#### **C.2.9.2.1.4 Technical Capabilities**

The following Intrusion Detection and Prevention Service capabilities are mandatory:

1. The contractor shall provide design and implementation services. This will enable the Agency and the contractor to discuss matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, escalation procedures.
2. The contractor shall provide installation support to include testing of equipment, testing of software, and loading of any Agency relevant data, as required by the Agency.
3. The contractor shall provide intrusion detection software and hardware components to include sensors, taps, and switches, as applicable.
4. The contractor shall provide host intrusion detection in order to protect critical Agency servers. The contractor shall monitor the servers for security breaches and misuse while enforcing best industry practices, and Agency security policies.
5. The contractor shall perform a scan of the intrusion detection system to verify the integrity of service components and validate installation and configuration activities.
6. The contractor shall support remote monitoring capabilities and proactively monitor the network on a 24X7 basis. The contractor shall continuously monitor the network for indications of compromise such as intrusions, anomalies, malicious activities, and network misuse.
7. The contractor shall detect precursor activities such as unauthorized network probes, sweeps, and scans that may indicate a potential attack.
8. The contractor shall perform anomaly detection in order to identify atypical traffic trends and unusual behaviors that may indicate a potential attack.
9. The contractor shall perform signature-based detection and analyze system activity for known attacks such as, but not limited to:
  - a. Buffer Overflows
  - b. Brute Force
  - c. Denial of Service (DOS)

d. Reconnaissance Efforts

10. The contractor shall monitor the network for signatures which take advantage of vulnerabilities identified in the SANS/FBI (SysAdmin, Audit, Network, Security Institute/Federal Bureau of Investigation) Twenty Most Critical Internet Security Vulnerabilities list.
11. The contractor shall automatically update the signature sets in use as new signatures become available.
12. The contractor shall support Agency-defined signatures in the signature database for increased security as required by the Agency.
13. The contractor shall perform policy-based detection to reveal violation of Agency security policies and detect potentially harmful traffic not intercepted by the firewall.
14. The system shall provide alerts based on known vulnerabilities and Agency security policies.
15. The contractor shall analyze suspicious security alerts to determine the significance of an event and immediately notify the Agency when the event is deemed of high priority. This focuses attention on real threats without greatly affecting legitimate traffic and minimizes false alarms.
16. The contractor shall notify the Agency of events via email, pager, fax, or telephone, as directed by the Agency.
17. The contractor shall provide the Agency with immediate access to severe alert information, which shall contain but not be limited to the following:
  - a. Incident Description
  - b. Incident Target
  - c. Incident Origin
  - d. Potential Incident Impacts
  - e. Incident Remedies
  - f. Incident Prevention Measures
18. The service shall respond dynamically to threats and take proactive and corrective actions to secure the network. These measures shall include, but not be limited to the following, as applicable:
  - a. Automatic termination of affected connections
  - b. Blocking traffic from the originating host
  - c. Disconnecting ports
  - d. Fixing the vulnerability
  - e. Focusing the monitoring on suspicious areas
  - f. Forwarding, limiting, or discarding malicious traffic
  - g. Logging off users

h. Modifying configurations

19. The contractor shall recommend appropriate responses to attacks.
20. The contractor shall employ defense mechanisms to detect and accurately stop attacks. These mechanisms include, but are not limited to pattern-matching; protocol/traffic anomaly review; and stateful, deep-packet, and multi-packet inspection.
21. The contractor shall advise the Agency on controlling and eliminating identified vulnerabilities.
22. The contractor shall provide post alarm support to include analysis and interpretation of attack data.
23. The contractor shall ensure that suspected attack information is sent via secure means to the contractor's operation center for evaluation.
24. The contractor shall provide the Agency with secure Web access to logs and service information, which shall contain but not be limited to the following, as applicable:
  - a. Attack name, description, level, impact date, time and remedies
  - b. Change Requests
  - c. Configuration Modifications
  - d. Device Identification
  - e. Intrusion Statistics
  - f. Originating and terminating IP addresses
  - g. Outages
  - h. Originating and terminating port
  - i. Protocol Affected
  - j. Sensor IP Address
  - k. Targeted Weaknesses
  - l. Tickets
  - m. Top Events
  - n. Top originating and terminating IP addresses
25. The contractor shall perform configuration changes as initiated and prioritized by the Agency.
26. The contractor shall maintain the intrusion detection system and perform necessary hardware/software upgrades, updates, and replacements.

27. The contractor shall test and deploy the latest patches and bug fixes as soon as they become available in order to ensure optimal performance of the service.
28. The contractor shall maintain the latest configuration information for restoration purposes.
29. The contractor shall perform periodic security scans that are capable of revealing vulnerabilities of the intrusion detection system.
30. The contractor shall document the results of the scans and the solutions to the identified vulnerabilities.
31. The contractor shall support networks of varying complexity with respect to size, bandwidth, and speeds.

**C.2.9.2.2 Features**

No features specified.

**C.2.9.2.3 Interfaces**

Intrusion Detection and Prevention Service shall support the User-to-Network Interfaces (UNIs) defined in the following Sections, as applicable:

1. C.2.4.1 Internet Protocol Service (IPS)
2. C.2.7.2 Premises-Based IP VPN Services (PBIP-VPNS) [Optional]
3. C.2.7.3 Network-Based IP VPN Services (NBIP-VPNS)

**C.2.9.2.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Intrusion Detection and Prevention Service in Section C.2.10.2.4.1 are mandatory:

**C.2.9.2.4.1 Intrusion Detection and Prevention Service Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Event Notification (EN)	Routine	Within 24 hours of a Low category event	≤ 24 hours	See Note 2
		Within 10 minutes of a High category event	≤ 10 minutes	
Grade of Service (Configuration/Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	See Note 3
		Within 2 hours for an Urgent priority change	≤ 2 hours	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	



## Notes:

1. IDPS availability is calculated as a percentage of the total reporting interval time that the IDPS is operationally available to the Agency. Availability is computed by the standard formula:  

$$Av(IDPS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
2. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification of the Agency. Events are categorized as follows:
  - a. Low — Events in the Low category have a negligible impact on service and do not significantly affect network security. They may include minor deviations from normal traffic activity, and minor hardware, software and configuration problems.
  - b. High — Events in the High category have a severe impact on service and operations. They indicate an actual threat, breach, or compromise of network security, and are immediately reported via email, pager, telephone, as specified by the Agency.
3. The Grade of Service (Configuration/Change) value represents the elapsed time between the configuration/change request and the change completion. Changes are initiated and prioritized by the Agency, or may be implemented in response to an event. Changes initiated by the contractor require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
4. See Section C.3.3.1.2.4 for the definitions and measurement guidelines

**C.2.9.3 Vulnerability Scanning Service (VSS)**

Vulnerability Scanning Service (VSS) allows Agencies to conduct effective and proactive assessments of critical networking environments, and correct vulnerabilities before they are exploited. This offering helps to guard Agency systems and network infrastructure against emerging threats.

**C.2.9.3.1 Service Description****C.2.9.3.1.1 Functional Definition**

VSS searches for security holes, flaws, and exploits on Agency systems, networks and applications. The service tests for vulnerabilities by comparing scanned information to data contained in a database, which is updated as new threats are discovered. VSS can also simulate a real intrusion in a controlled environment, in order to gauge a network's susceptibility to attacks. The service performs external scans by remotely probing a network for vulnerabilities that generally come from the outside; and internal scans which detect flaws originating from the inside.

**C.2.9.3.1.2 Standards**

Vulnerability Scanning Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
2. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 199 — Standards for Security Categorization of Federal Information and Information Systems
3. NIST Special Publication (SP) 800-51 — Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
4. United States Computer Emergency Readiness Team (US-CERT) reporting requirements
5. All new versions, amendments, and modifications of the above when offered commercially.
6. All appropriate standards for any applicable underlying Network access and transport services

**C.2.9.3.1.3 Connectivity**

Vulnerability Scanning Service shall connect to and interoperate with the Agency networking environment, including Demilitarized Zones (DMZs) and secure LANs, as required by the Agency. The service shall also support Internet connectivity.

**C.2.9.3.1.4 Technical Capabilities**

The following Vulnerability Scanning Service capabilities are mandatory:

1. The contractor shall support the Agency in establishing, implementing and maintaining a vulnerability scanning service, which shall be operational on a 24x7 basis. The service shall provide the following:
  - a. External Vulnerability Scanning which tests Internet connected nodes in the network, including web environments.
  - b. Internal Vulnerability Scanning which looks for local/host flaws and internal threats, usually inside the firewall.
2. The systems shall periodically probe networks, including operating systems and application software, for potential openings, security holes, and improper configurations.
3. The contractor shall probe Agency systems for vulnerabilities in, but not limited to, the following areas as applicable:
  - a. Backdoors
  - b. Bind
  - c. Browser

- d. Brute Force Attacks
- e. Common Graphic Interfaces - Binary (CGI-Bin)
- f. Daemons
- g. Distributed Component Object Model (DCOM)
- h. Databases
- i. Domain Name Service (DNS)
- j. eCommerce Applications
- k. Email
- l. Firewalls
- m. File Sharing
- n. File Transfer Protocol (FTP)
- o. General Remote Services
- p. Hardware and Network Appliances
- q. Hubs
- r. Information/Directory Services
- s. Instant Messaging
- t. Lightweight Directory Access Protocol (LDAP)
- u. Mail Applications
- v. Multimedia Internet Mail Extension (MIME)
- w. Network
- x. Network Sniffers
- y. Netbios
- z. Network File System (NFS)
- aa. Network Information System (NIS)
- bb. NT-Critical Issues
- cc. NT-Groups
- dd. NT-Networking
- ee. NT-Password Checks
- ff. NT Policy Issues
- gg. NT Registry
- hh. NT-Services
- ii. NT-Users
- jj. Port Scans

- kk. Protocol Spoofing
- ll. Router-Switch
- mm. Remote Procedure Call (RPC)
- nn. Shares
- oo. Simple Mail Transfer Protocol (SMTP)
- pp. Simple Network Management Protocol (SNMP)
- qq. Server Message Block (SMB)
- rr. Transmission Control Protocol/Internet Protocol (TCP/IP)
- ss. Trojan Horses
- tt. Web Scans
- uu. Web Servers
- vv. Wireless Access Points
- ww. X-Windows

4. The contractor shall proactively identify network vulnerabilities, and propose appropriate countermeasures, fixes, patches, and workarounds.
5. The contractor shall notify the Agency of vulnerabilities discovered via email, pager, fax, or telephone, as directed by the Agency.
6. The contractor shall also provide the Agency with secure Web access to vulnerability information, scan summaries, device/host reports, and trend analyses.
7. The contractor shall review vulnerabilities discovered with the Agency, as required.
8. The contractor shall provide scan scheduling flexibility to the Agency in order to minimize any interruptions in normal business activities.
9. The contractor shall provide the Agency with non-destructive and non-intrusive vulnerability scans that will not crash the systems being analyzed, or disrupt Agency operations. The scans shall not provoke a debilitating denial of service condition on the Agency system being probed.
10. The contractor shall use other analytical means to ascertain the vulnerability of Agency systems if a particular scan is potentially destructive or intrusive.
11. The contractor shall ensure that the scanning engine is regularly updated with new vulnerabilities information in order to maintain effectiveness of the service.
12. The contractor shall support networks of varying size and complexity.

#### **C.2.9.3.2 Features**

The Vulnerability Scanning Service feature in Section C.2.10.3.2.1 is mandatory:

**C.2.9.3.2.1 Vulnerability Scanning Service Features**

ID Number	Name of Feature	Description
1	VSS Application Programming Interface (API)	The contractor shall provide the Agency the ability to integrate the service into its own tools and applications, using for example, a standard Extensible Markup Language (XML) Application Programming Interface (API), as required by the Agency. This will assist in-house security personnel with tasks such as scanning IP addresses, assessing the vulnerabilities of hosts, creating user accounts, exporting vulnerability data.

**C.2.9.3.3 Interfaces**

Vulnerability Scanning Service shall support the User-to-Network Interfaces (UNIs) defined in the following Sections, as applicable:

1. C.2.4.1 Internet Protocol Service (IPS)
2. C.2.7.2 Premises-based IP VPN Services (PBIP-VPNS) [Optional]
3. C.2.7.3 Network-based IP VPN Services (NBIP-VPNS)

**C.2.9.3.4 Performance Metrics**

The performance level and Acceptable Quality Level (AQL) of the Key Performance Indicators (KPIs) for Vulnerability Scanning Service in Section C.2.10.3.4.1 are mandatory:

**C.2.9.3.4.1 Vulnerability Scanning Service Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. VSS availability is calculated as a percentage of the total reporting interval time that the VSS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(VSS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

#### **C.2.9.4 Anti-Virus Management Service (AVMS)**

Anti-Virus Management Service enables the detection and removal of system viruses. The service scans executable files, boot blocks and incoming traffic for malicious code. Anti-virus applications are constantly active in attempting to detect patterns, activities, and behaviors that may signal the presence of viruses. AVMS enables Agencies to procure anti-virus capabilities that protect the network infrastructure.

##### **C.2.9.4.1 Service Description**

###### **C.2.9.4.1.1 Functional Definition**

AVMS provides the most current anti-virus software and tools. It includes traffic scanning, anti-virus software/hardware, monitoring of anti-virus advisories, management, and maintenance. The service monitors traffic for malicious content, and complements the anti-virus software already implemented on Agency desktops.

###### **C.2.9.4.1.2 Standards**

Anti-Virus Management Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
2. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) 140 - 2 — Security Requirements for Cryptographic Modules
3. NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems
4. United States Computer Emergency Readiness Team (US-CERT) reporting requirements
5. All new versions, amendments, and modifications of the above when offered commercially
6. All appropriate standards for any applicable underlying Network access and transport services

###### **C.2.9.4.1.3 Connectivity**

Anti-Virus Management Service shall connect to and interoperate with the Agency networking environment, including Demilitarized Zones (DMZs) and secure LANs, as required by the Agency. The service shall also support connectivity to extranets and public networks such as the Internet.

###### **C.2.9.4.1.4 Technical Capabilities**

The following Anti-Virus Management Service capabilities are mandatory:

1. The contractor shall provide design and implementation services in order to determine the appropriate anti-virus solution suited to Agency needs.
2. The contractor shall provide installation, configuration and integration support to the Agency, including testing of service equipment and software.
3. The contractor shall provide, as part of the anti-virus service, the software and hardware components, including servers and gateways, as required by the Agency. This shall include, as applicable:
  - a. A managed gateway-based anti-virus service which provides a gateway that scans web and email traffic for worms, viruses, and malicious content.
  - b. A server-based anti-virus service that scans all files and software housed on a specific server, including the operating system. This host-level scanning is provided at Agency-specified time intervals.
4. The contractor shall monitor the system on a 24x7 basis for indications of infection.
5. The service shall allow real-time and on-demand virus scanning.
6. The contractor shall screen incoming and outgoing FTP, HTTP, POP, and SMTP traffic for possible infection. The contractor shall also protect against viruses passed via HTTPS for the server-based server.
7. The service shall perform data integrity checks and, at a minimum, protect against the following:
  - a. Known viruses
  - b. Behaviors and patterns that may indicate the presence of viruses
  - c. Malicious mobile code
  - d. Different strains of polymorphic viruses
  - e. Viruses in compressed files, as required by the Agency
  - f. Viruses in different languages (e.g., JAVA, ActiveX, Visual Basic)
  - g. Trojan horses and worms
  - h. Macro viruses
8. The service shall respond to infections and violations of the Agency networking environment and provide the following minimum capabilities:
  - a. Alert Service:
    - i. Systems/Network Administrator notification via email, pager, fax, or telephone, as directed by the Agency's notification procedures.
    - ii. Sender and recipient notification, in case of email-borne virus.
  - b. Infected file isolation for cleaning, deletion, or post alert analysis and interpretation.
  - c. Control of user access and environment for the malicious file.

9. The contractor shall maintain the anti-virus system and perform the necessary hardware/software upgrades, updates, and replacements.
10. The contractor shall deploy the latest system patches and bug fixes as soon as they become available in order to ensure optimal performance of the service.
11. The contractor shall provide automatic and timely updates of the virus pattern and signature files as they become available to ensure adequate protection.
12. The contractor shall perform periodic gateway scans capable of revealing any vulnerabilities of the anti-virus system.
13. The contractor shall perform configuration changes as initiated and prioritized by the Agency. Changes initiated by the contractor require Agency consent prior to implementation.
14. The contractor shall provide the Agency with secure Web access to logs and service information, which shall contain, but not be limited to, the following, as applicable:
  - a. Infections detected
  - b. Malicious emails
  - c. Rule violations
  - d. Traffic/mail statistics
15. The contractor shall support networks of varying complexity in terms of size, bandwidth, and speeds.

**C.2.9.4.2 Features**

The Anti-Virus Management Service feature in Section C.2.10.4.2.1 is mandatory:

**C.2.9.4.2.1 Anti-Virus Management Service Features**

ID Number	Name of Feature	Description
1	Anti-Virus Load Balancing	The contractor shall implement a hardware or software load balancing capability, as applicable. This addresses large systems requirements by distributing traffic across multiple servers.

**C.2.9.4.3 Interfaces**

Anti-Virus Management Service shall support the User-to-Network Interfaces (UNIs) defined in the following Sections, as applicable:

1. C.2.4.1 Internet Protocol Service (IPS)
2. C.2.7.2 Premises-based IP VPN Services (PBIP-VPNS) [Optional]
3. C.2.7.3 Network-based IP VPN Services (NBIP-VPNS)



### C.2.9.4.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Anti-Virus Management Service in Section C.2.10.4.4.1 are mandatory:

#### C.2.9.4.4.1 Anti-Virus Management Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Grade of Service (Virus Updates)	Routine	Within 24 hours for a Normal priority update	≤ 24 hours	See Note 2
		Within 2 hours for an Urgent priority update	≤ 2 hours	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. AVMS availability is calculated as a percentage of the total reporting interval time that the AVMS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(AVMS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. The Grade of Service (Virus Updates) value represents the time between the release of the anti-virus update, and the deployment of the update to the Agency. This indicator is to ensure automatic and timely delivery of updates. Note that the Agency will accept updates in shorter timeframes, as they become available. Updates are categorized as follows.
  - a. Normal — Updates in the Normal category represent regular virus definition file releases. They protect against viruses discovered since the prior release.
  - b. Urgent — Updates in the Urgent category represent emergency cures, signatures and patches released in response to a rapid or widespread outbreak.
3. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

### C.2.9.5 Incident Response Service (INRS)

In an effort to combat cyber attacks and crime, Agencies intend to implement Incident Response Service (INRS). This offering is one of the security tools that will help in responding to potential malicious attacks that can lead to service disruptions. INRS allows Agencies to complement in-house security expertise, or obtain outside assistance with a greater depth and breadth of experience.

### **C.2.9.5.1 Service Description**

#### **C.2.9.5.1.1 Functional Definition**

INRS is comprised of both proactive and reactive activities. Proactive services are designed to prevent incidents. They include onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training. Reactive services involve telephone and on-site support for responding to malicious events such as Denial of Services (DoS) attacks; virus, worm, and trojan horse infections; illegal inside activities, espionage, and compromise of sensitive internal Agency databases. INRS provides an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks. In addition, INRS provides forensics services that can assist in apprehending and prosecuting offenders.

#### **C.2.9.5.1.2 Standards**

Incident Response Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government, that meet or exceed the provisions of the standards listed below:

1. E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
2. Internet Engineering Task Force - Request for Comments (IETF-RFC) 2350 Expectations for Computer Security Incident Response
3. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 199 — Standards for Security Categorization of Federal Information and Information Systems
4. NIST Special Publication (SP) 800-61 — Computer Security Incident Handling Guide
5. United States Computer Emergency Readiness Team (US-CERT) reporting requirements
6. All new versions, amendments, and modifications of the above when offered commercially
7. All appropriate standards for any applicable underlying Network access and transport services

#### **C.2.9.5.1.3 Connectivity**

Incident Response Service shall provide the Agency secure Web access to contractor incident analyses and recommendations.

#### **C.2.9.5.1.4 Technical Capabilities**

The following Incident Response Service capabilities are mandatory:

1. The contractor shall review the Agency's security infrastructure and develop the appropriate strategic plans in collaboration with the Agency. These plans shall detail the incident response process, identify internal resources, assign duties to team members, describe policies, define severity levels, list escalation chains, and specify emergency/recovery procedures.
2. The contractor shall provide the Agency with effective incident response support on a 24x7 a week basis.
3. The contractor shall provide incident analysis and assessment in order to determine the scope and impact of incidents.
4. The contractor shall coordinate with the Agency to handle potential security incidents according to the appropriate response procedures.
5. The contractor shall provide countermeasures to contain the security incident, limit its spread, and protect internal systems.
6. The contractor shall recommend the fixes necessary to eliminate identified vulnerabilities, and the appropriate procedures to guard against future attacks.
7. The contractor shall provide the Agency with secure Web access to incident analysis findings and recommendations.
8. The contractor shall assist the Agency in containing the damage and restoring affected systems to their normal operational state.
9. The contractor shall assist the Agency in testing restored systems in order to ensure that identified vulnerabilities have been corrected.
10. The contractor shall provide dedicated support until resolution of the problem.
11. The contractor shall provide post-incident investigative and forensics services. This includes isolating the impacted area, capturing and collecting data, categorizing malicious or illegal events, and performing reconstruction analyses. The contractor shall handle and preserve the data collected according to sound scientific and evidence rules, as the information may serve as evidence in administrative actions and legal proceedings. The contractor shall trace the offenders and assist in prosecuting attackers, as required.
12. The contractor shall provide telephone support to the Agency, as required.
13. The contractor shall deploy cyber security personnel to Agency sites to handle security incidents, as necessary.
14. The contractor shall provide security awareness training to Agency personnel as required. This includes mock attack drills, emerging threats and vulnerabilities workshops, and new incident response tools and processes demonstrations. The frequency and nature of training activities may vary according to Agency needs.

#### **C.2.9.5.2 Features**

No features specified.

### C.2.9.5.3 Interfaces

Incident Response Service analyses and recommendations shall be accessible via secure Web interfaces.

### C.2.9.5.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Incident Response Service in Section C.2.10.5.4.1 are mandatory:

#### C.2.9.5.4.1 Incident Response Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Response Time (Telephone)	Routine	Within 1 hour of the notification for a Low category incident	≤ 1 hour	See Note 1
		Within 15 minutes of the notification for a High category incident	≤ 15 minutes	
Response Time (On-Site)	Routine	Within 36 hours of the notification for a Low category incident	≤ 36 hours	See Note 2
		Within 24 hours of the notification for a High category incident	≤ 24 hours	

Notes:

1. The Telephone Incident Response value represents the elapsed time between the Agency's notification to the contractor, and the contractor's implementation of response procedures. These procedures, as well as what constitutes Low and High incidents, are detailed in the agreed upon strategic plan.
2. The On-Site Incident Response value represents the elapsed time between the Agency's notification to the contractor, and the contractor's arrival to the affected site for implementation of response and investigative procedures. These procedures, as well as what constitutes Low and High incidents, are detailed in the agreed upon strategic plan.

### C.2.9.6 Managed E-Authentication Service (MEAS)

Managed E-Authentication Service (MEAS) provides Agencies with electronic authentication services in order to seamlessly conduct electronic transactions and implement E-Government initiatives via the Internet. The service enables an individual to remotely authenticate his or her identity to an Agency Information Technology (IT) system.

#### C.2.9.6.1 Service Description

### **C.2.9.6.1.1 Functional Definition**

Managed E-Authentication Service consists of hardware and software components that provide for remote authentication of individual people over a network for the purpose of electronic government and commerce. The service provides for the electronic validation and verification of a user's identity and enables the use of electronic signatures over the Internet, the contractor's network and other public networks.

### **C.2.9.6.1.2 Standards**

Managed E-Authentication Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. DIAMETER Protocol RFC 3588
2. Federal CIO Federal Identity Credentialing Committee (FICC) Shared Service Provider (SSP) program documents suite
3. GSA eGov E-Authentication Technical Suite
4. International Telecommunications Union – Telecommunications Sector (ITU-T) Recommendation X.509 version 3 certificates
5. ITU-T X.500 Series of Recommendations
6. LDAP v2 or higher for Certificate Revocation List (CRL) retrieval
7. LDAPS (LDAP Secure, i.e., LDAP over SSL) for CRL retrieval
8. Liberty Alliance format (currently versions 1.1. and 2.x)
9. NIST FIPS 140-2 – Security Requirements for Cryptographic Modules
10. NIST Interagency Report (NISTIR) 6887 – 2003 Edition, Government Smart Card Interoperability Specification (GSC-IS) v2.1
11. NIST Special Publication (SP) 800-63 – Recommendation for Electronic Authentication
12. NIST Special Publication (SP) 800-73 – Integrated Circuit Card for Personal Identity Verification (currently still Draft)
13. Online Certificate Status Protocol (OCSP)
14. PKIX Internet Engineering Task Force (IETF) Request For Comments (RFC) 3280
15. Remote Authentication Dial In User Service (RADIUS) Protocol
16. RFC 3647 – Internet X.509 PKI Certificate Policy and Certification Practices Framework, and its updated version RFC 3647
17. Security Assertion Markup Language (SAML)
18. Shibboleth security middleware specification
19. Simple Certificate Validation Protocol (SCVP)

20. Terminal Access Controller Access Control System (TACACS) /TACACS+ (Cisco) Protocol
21. Web services security language (WS-Security) specification by OASIS
22. X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework
23. All appropriate standards for any applicable underlying Network access and transport services
24. All new versions, amendments, and modifications to the above when offered commercially.

#### **C.2.9.6.1.3 Connectivity**

Managed E-Authentication Service uses underlying transport and access services for transfer of authentication information. The service shall connect to Agency networking environments including, but not limited to Agency Demilitarized Zones (DMZs) and secure LANs, as required by the Agency. MEAS shall also connect to public networks such as the Internet and also allow connectivity to extranets.

#### **C.2.9.6.1.4 Technical Capabilities**

The following Managed E-Authentication Service capabilities are mandatory unless indicated otherwise. The core service will provide products and services that enhance the security of networked systems and facilitate digital signatures. The service will establish the required client and server software, hardware, and operational procedures to establish an Agency authentication capability.

##### **C.2.9.6.1.4.1 Design and Engineering Services**

1. The contractor shall provide E-Authentication networking infrastructure design and engineering services that meet Agency requirements. These services include but are not limited to system architecture and equipment recommendations, a baseline assessment, a final design configuration and operational procedures.
2. The contractor shall support the Agency in developing detailed plans for implementing of the user authentication service. The contractor shall offer to provide installation and integration support to the Agency, including but not limited to testing of equipment and software, cost information and loading of customer relevant data.

##### **C.2.9.6.1.4.2 Token-Based Implementation and Management**

###### **C.2.9.6.1.4.2.1 Token-Based Implementation**

1. The contractor for the managed PKI service shall setup the authentication service at the identity authentication assurance level specified by the Agency and issue smart cards and/or other token devices in the quantities needed by an Agency. Examples of user authentication tokens include:
  - a. Token cards with or without PIN pad

- b. Key fob
  - c. Soft token
2. The service shall follow the E-Authentication federated authentication model to allow Agencies to validate multiple levels of authentication via a single interface, enable inter-Agency acceptance of digital certificates, and single sign-on capability.
  3. The contractor shall support the Agency specified user ID naming scheme to meet Agency requirements.
  4. The contractor shall implement Secure Sockets Layer (SSL) and/or Transport Layer Security (TLS) equipped servers as well as appropriate acceleration capabilities as required by the Agency to meet Agency performance requirements.
  5. The contractor shall provide methods including, but not limited to, the following, as needed by an Agency:
    - a. Password and personal identification number (PIN)
    - b. Authentication methods based on fingerprints
    - c. Network authentication systems and servers for embedded devices (e.g., routers, modem servers, switches, etc.).
  6. The contractor shall support the government in developing, implementing, and maintaining the Authentication, Authorization and Accounting (AAA) system and servers for network access, including the related tokens, based on but not limited to, the following protocols:
    - a. RADIUS
    - b. TACACS/TACACS+ (Cisco)
    - c. DIAMETER

#### **C.2.9.6.1.4.2.2 Token-Based Management**

1. The contractor shall manage and maintain the user authentication service including the related tokens, such as, but not limited to:
  - a. One-time password devices
  - b. Smart cards
  - c. Hardware tokens
2. The contractor shall provide change management functions of the authentication service, as requested by Agency designated Points of Contact (POCs), including but not limited to:
  - a. Adding a new user
  - b. Deleting a current user
  - c. Reset the PIN
  - d. Changing, adding, or deleting IP addresses of software agent

e. User ID administration

3. The contractor shall ensure uninterrupted operations using mechanisms such as redundant servers that are located in geographically separate locations with the content continuously synchronized between them.

#### **C.2.9.6.1.4.3 Certificate-Based Implementation and Management**

##### **C.2.9.6.1.4.3.1 Certificate-Based Implementation**

1. The contractor shall set-up a managed Public-Key Infrastructure (PKI) that comprises, but is not limited to, Certification Authority (CA), Registration Authority (RA), directory and associated servers.
2. The contractor shall host and administer PKI certificates for an Agency, including but not limited to certificate issuance, validation services, Agency application certificate registration, and management.
3. The contractor for the managed PKI service shall setup the authentication service at the identity authentication assurance level specified by the Agency and issue digital certificates in the quantities needed by an Agency.
4. The service shall follow the E-Authentication federated authentication model to allow Agencies to validate multiple levels of authentication via a single interface, enable inter-Agency acceptance of digital certificates, and single sign-on capability.
5. The contractor shall establish a networking environment that provides the communication among PKI elements including but not limited to Certification Authorities (CAs). The contractor shall implement SSL and/or TLS equipped servers as well as appropriate acceleration capabilities as required by the Agency to meet Agency performance requirements.

##### **C.2.9.6.1.4.3.2 Certificate-Based Management**

1. The contractor for the managed PKI service shall maintain the database of:
  - a. User names
  - b. User IDs
  - c. Passwords
2. The contractor shall provide digital certificates and digital signatures within PKI as well as CA services.
3. The contractor shall ensure uninterrupted operations using mechanisms such as redundant servers that are located in geographically separate locations with the content continuously synchronized between them.
4. The contractor shall provide change management functions of the managed PKI service, as requested by Agency designated POCs, including but not limited to:
  - a. Adding a new user
  - b. Deleting a current user



- c. Reset the password
- d. Changing, adding, or deleting IP addresses of software agent
- e. User ID administration

### C.2.9.6.2 Features

The Managed E-Authentication Service features in C.2.10.6.2.1 are mandatory, unless marked optional:

#### C.2.9.6.2.1 Managed E-Authentication Service Features

ID Number	Name of Feature	Description
1	Biometric Characteristics	The contractor shall provide Biometric authentication methods including iris scan, voice, and facial recognition, as required by the Agency.
2	Encryption/Digital Signature Client Software	The contractor shall provide and support the encryption/digital signature client software for the Agency designated POCs.
3	E-Authentication Training	The contractor shall provide E-Authentication training to Agency personnel as required. This includes but is not limited to user authentication, PKI, and CAs. The frequency and nature of training activities may vary according to Agency needs.
4	Directory/Repository Function	The contractor shall develop, implement, and maintain a Directory/Repository function that will support the PKI and/or other e-authentication mechanism chosen by the Agency.

### C.2.9.6.3 Interfaces

Managed E-Authentication Service shall support the User-to-Network Interfaces (UNIs) defined in the following Sections, as applicable:

1. C.2.3.1 Frame Relay Service (FRS) [Optional]
2. C.2.3.2 Asynchronous Transfer Mode Service (ATMS) [Optional]
3. C.2.4.1 Internet Protocol Services (IPS)
4. C.2.7.2 Premises-Based IP-VPN Services (PBIP-VPNS) [Optional]
5. C.2.7.3 Network-Based IP-VPN Services (NBIP-VPNS)

### C.2.9.6.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of the Key Performance Indicators (KPI) for Managed E-Authentication Service in Section C.2.10.6.4.1 are mandatory.

#### C.2.9.6.4.1 Managed E-Authentication Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.99%	≥ 99.99%	See Note 1
Event Notification (EN)	Routine	Within 4 hours of a Low category event	≤ 4 hours	See Note 2
		Within 30 minutes of High category event	≤ 30 minutes	
Grade of Service (Configuration Change)	Routine	Within 24 hours for a Normal priority change	≤ 24 hours	See Note 3
		Within 2 hours for an Urgent priority change	≤ 2 hours	
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. MEAS availability is calculated as a percentage of the total reporting interval time that the MEAS is operationally available to the Agency. [Note. It includes that of the various databases and servers that are employed (such as but are not limited to directory, RADIUS, and TACACS) to provide the service.]. Availability is computed by the standard formula:

$$Av(MEAS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. The Event Notification (EN) value represents the elapsed time between the detection of the event by the contractor and the notification of the Agency. Events are categorized as follows:
  - a. Low — Events in the Low category have a negligible impact on service overall. They include non-critical server alerts that indicate systems configuration problems, authentication server hardware or software failures that do not disrupt service, and multiple rejects of an individual User ID.
  - b. High — Events in the High category have a severe impact on service and operations. They include server failures that disrupt service, suspicious activities detected by the contractor, and request for an emergency reset of PIN to a static password for a user who has lost use of a token but needs to gain access. These events are immediately reported to Agency designated POCs via such as but are not limited to email, pager, and telephone as specified by the Agency.

3. The Grade of Service (Configuration Change) value represents the elapsed time between the change request by the Agency POC and the change completion by the contractor. The elapsed time is measured by logs/reporting. Changes are initiated and prioritized by the Agency. Changes initiated by the contractor require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
4. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

#### **C.2.9.7 Reserved**

#### **C.2.9.8 Secure Managed Email Service (SMEMS)**

Email is one of the most important communication methods used by Agencies. However, its increasing use exposes Agency networks to a variety of security risks and unsolicited content, such as viruses, spam, and inappropriate material. Secure Managed Email Service (SMEMS) provides Agencies with a complete, secure and fully managed email security solution.

##### **C.2.9.8.1 Service Description**

###### **C.2.9.8.1.1 Functional Definition**

Email security solutions implemented at Agency gateways and desktops usually attempt to handle events that have already breached the network. Any delay in applying security updates to this infrastructure exposes the network to rapid outbreaks and dynamic threats. SMEMS offers an additional layer of protection by proactively scanning and monitoring email traffic at the contractor's security platform, before it enters the Agency's network. The service supports email security functions such as Anti-Virus Scanning, Anti-Spam Filtering, and Content Control. Security engines are continuously updated to maintain effectiveness against threats and inappropriate material. The contractor's fault tolerant and load-balanced platform is able to scan millions of email messages a day without noticeable delay to end-users. SMEMS works in conjunction with existing Agency email systems, and is implemented without additional investment in hardware and software at Agency sites.

###### **C.2.9.8.1.2 Standards**

Secure Managed Email Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
2. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 140 - 2 — Security Requirements for Cryptographic Modules
3. NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems

4. NIST SP 800-45 — Guidelines on Electronic Mail Security
5. United States Computer Emergency Readiness Team (US-CERT) reporting requirements
6. All new versions, amendments, and modifications of the above when offered commercially
7. All appropriate standards for any applicable underlying Network access and transport services

#### **C.2.9.8.1.3 Connectivity**

Secure Managed Email Service shall connect to and interoperate with the Agency's email system and networking environment. The service shall support connectivity to the Internet.

#### **C.2.9.8.1.4 Technical Capabilities**

The following Secure Managed Email Service capabilities are mandatory:

1. The contractor shall monitor email in real-time, on a 24x7 basis, for timely and accurate detection of harmful traffic and unwanted content.
2. The email security system shall support the following functions:
  - a. Anti-Virus Scanning which monitors all inbound and outbound messages and attachments for:
    - i. Known viruses and unknown viruses
    - ii. Trojan horses, worms, macro viruses and other malicious files
    - iii. Behaviors and characteristics that may indicate the presence of email viruses
    - iv. Different strains of polymorphic viruses
    - v. Viruses in compressed files, as required by the Agency
    - vi. Viruses in different languages (e.g., JAVA, ActiveX, Visual Basic)
  - b. Anti-Spam Filtering which prevents unsolicited marketing and messages from entering the Agency's network, and taxing human, bandwidth and storage resources. The system shall support:
    - i. Anti-spam methods including fingerprinting, blacklists, open relay blocking, honeypots, Bayesian probability, heuristic and rule-based filtering, as appropriate
    - ii. Capability to distinguish between legitimate email and spam, reducing false negatives and positives
    - iii. Agency ability to customize spam lists, and specify domains, IP and email addresses which are to be allowed or blocked

- c. Content Control which screens inbound and outbound email for content that may signal system abuse or violation of Agency communications policies. The systems shall support the following:
  - i. Blocking of specific words, phrases; adult or sexually explicit material, and other inappropriate content
  - ii. Preventing transmission of intellectual property and confidential information
  - iii. Stopping files and attachments based on type, size, formats, number, and delivery time
3. The service shall respond to email infections and Agency policy violations, providing the following at a minimum:
  - a. Alerts notifying the Systems/Network Administrator via email, pager, fax, or telephone, as directed by the Agency's notification procedures. The sender and recipient shall also be notified, as applicable.
  - b. Virus infected file isolation for cleaning, deletion, or post alert analysis and interpretation. The system shall also store or forward spam and policy violating content to an alternate email address for Agency review in order to prevent the deletion of legitimate business email, or handle such content according to Agency directives.
4. The contractor shall support a secure Web-based management interface which provides, but is not limited to the following:
  - a. Configuration tools allowing the Agency to set policies, rules and routing requirements
  - b. Email activity trends, such as daily, weekly, monthly, and yearly volumes and patterns
  - c. Email cleaned, deleted or rejected
  - d. Forwarding of weekly reports to designated Agency representative
  - e. Management of user and domain permissions
  - f. Potential threats flagged
  - g. Real-time service statistics and availability data
  - h. User and company domain activity
  - i. Viruses, spam, and other inappropriate content blocked on a daily, weekly, monthly or yearly basis
5. The contractor shall queue and retain email in the event of an Agency mail server or connection failure, in order to prevent messages from bouncing. The contractor shall gradually transmit queued email upon resolution of the problem to avoid overloading the servers.
6. The contractor shall implement security procedures to preserve the confidentiality and integrity of all Agency email traversing its network and data center, as

required by the Agency. These include, but are not limited to, authentication, encryption, and access restriction.

7. The contractor shall support email requirements of varying complexity, in terms of load and volume.

**C.2.9.8.2 Features**

No features specified.

**C.2.9.8.3 Interfaces**

Secure Managed Email Service shall support the User-to-Network Interfaces (UNIs) defined in Section C.2.4.1 Internet Protocol Service (IPS), as applicable.

**C.2.9.8.4 Performance Metrics**

The performance level and Acceptable Quality Level (AQL) of the Key Performance Indicator (KPI) for Secure Managed Email Service in Section C.2.10.8.4.1 are mandatory:

**C.2.9.8.4.1 Secure Managed Email Service Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.999%	≥ 99.999%	See Note 1
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Note:

1. SMEMS availability is calculated as a percentage of the total reporting interval time that the SMEMS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(SMEMS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definition and measurement guidelines.

**C.2.10 Management & Applications Services**

**C.2.10.1 Reserved**

**C.2.10.2 Call Center / Customer Contact Center Services (CCS)**

Call Center/Customer Contact Center Services (CCS) provides services and personnel to enable Agencies to efficiently and effectively deliver customer service to their clientele across multiple contact channels (voice, fax, email, and Internet website, etc) by providing a single network call queue or multiple call queues (where applicable). A

network call queue manages multimedia customer interactions such as voice, e-mail, Web submissions, and fax. The call queue(s) provides the consistent, real-time management and distribution of multi-media calls to an Agency contact center. CCS may be used in conjunction with Toll Free and other network services to facilitate Agency communications with the general public, businesses, and other Agencies. CCS also offers a call answering service with the call queue. The CCS call answering service enables the Agency to utilize contractor provided resources to respond to caller inquiries. The contractor provided call answering resources can be situated at either (1) an Agency location(s) or (2) a contractor location(s).

#### **C.2.10.2.1 Service Description**

##### **C.2.10.2.1.1 Functional Definition**

Call Center/Customer Contact Center Services can enable subscribing Agencies to deliver customer service to their designated customer base across multi-media contact channels (voice, fax, email, and Internet website, etc) and provide additional enabling services for end to end customer service. The basic service provides intelligent call routing capabilities with a network call queue. The CCS will apply to single site, multiple site, and enterprise wide Agency contact centers.

##### **C.2.10.2.1.2 Standards**

Call Center/Customer Contact Center Services shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Computer Supported Telephony Applications (CSTA) [Optional]
2. IETF RFC's for Internet Protocol (IP) IPv4. IPv6 when and where offered commercially by the contractor.
3. ITU-T H.248.1 / Megaco (IETF RFC 3525) when and where offered commercially by the contractor.
4. ITU-T H.323 when and where offered commercially by the contractor.
5. ITU-T T.30, T.37, T.38, and T.120
6. Skinny Client Control Protocol (SCCP) [Optional]
7. IETF RFC 3261 for Session Initiation Protocol (SIP) when and where offered commercially by the contractor.
8. Voice eXtensible Markup Language (VXML)
9. All appropriate standards for any underlying access and transport services.
10. The contractor shall comply with all new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

##### **C.2.10.2.1.3 Connectivity**

Call Center/Customer Contact Center Services shall connect and interoperate with:

1. Internet
2. Public Switched Telephone Network (PSTN)

**C.2.10.2.1.4 Technical Capabilities**

The following Call Center/Customer Contact Center Services capabilities are mandatory unless marked optional:

**C.2.10.2.1.4.1 CCS Delivery Methods**

1. The contractor shall provide five independent service delivery methods for CCS based upon the subscribing Agencies needs. Three service delivery methods shall be available for Call Management service and two methods for Call Answering service.
2. The contractor shall provide the following five independent service delivery methods for CCS:
  - a. Contractor Provided and Contractor Based (CPCB) Call Management Service. The contractor shall provide the necessary components required for CCS Call Management Service. This includes, but is not limited to, hardware, software, inside wiring, and power. The components shall be located within the contractor's network and maintained by the contractor. Agency supplied personnel will answer calls distributed by CCS Call Management service.
  - b. Contractor Provided and Agency Based (CPAB) Call Management Service. The contractor shall provide the necessary components required for CCS Call Management Service to be located at an Agency provided location. This includes, but is not limited to, CCS hardware and software. The contractor shall install, configure, and maintain the CCS equipment. The Agency will provide the power, inside wiring, and physical location for the contractor's CCS equipment. Agency supplied personnel will answer calls distributed by CCS Call Management service.
  - c. [Optional]. Contractor Based and Agency Provided (CBAP) Call Management Service. The Agency will provide the necessary components required for CCS Call Management Service including hardware and software. The contractor shall provide power, inside wiring, and a physical location for the Agency provided CCS equipment. The contractor shall install, configure, and maintain the Agency CCS equipment. Agency supplied personnel will answer calls distributed by CCS Call Management service.
  - d. CCS Provided at an Agency Location (CPAL) Call Answering Service. The contractor provided personnel shall perform operations at an Agency provided location. The Agency will be responsible for providing the work space, furniture, workstation hardware, software, and all necessary building utilities required for the call center. The contractor shall include CPCB Call Management service as part of CPAL.
  - e. CCS Provided at a contractors Location (CPCL) Call Answering Service. The contractor personnel shall be located and perform operations at a contractor



provided location. The contractor shall be responsible for providing the work space, furniture, workstation hardware, software, and all necessary building utilities for the call center. The contractor shall include CPCB Call Management service as part of CPCL

#### **C.2.10.2.1.4.2 CCS Call Management Service (Network Call Queue)**

1. The contractor shall provide the capability for a network call queue (a single queue or multiple queues according to Agency needs) to manage the routing and distribution of contacts (calls) from multi-media channels such as voice, e-mail, facsimile, and an Agency web site.
2. The Intelligent routing and distribution of contacts shall be determined according to the real time operating status of the subscribing Agencies contact center(s) and their business rules. The Agency business rules can be based upon parameters such as media type, real time status of the contact center, caller profile, call content, and agent skills. The CCS shall provide the capability to prioritize queue and contacts (calls) within the queue.
3. The contractor's CCS shall interoperate with the subscribing Agencies CCS communications channels such as the Internet website, e-mail, voice, and facsimile (when applicable).
4. The contractor's CCS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.
5. The contractor shall support service observation. Service observation provides Agency authorized personnel with the capability to monitor the CCS trunks, agents, and agent groups for call quality. Service observation shall provide options for silent monitoring (default) and three way audio conferencing. Service observation shall be made available for monitoring both local and remote agents and support local and remote observers. Service observation shall be secure and available only to authorized Agency designated individuals.
6. The contractor shall provide the subscribing Agency with the capability to manage its specific network queue, call routing algorithms, contact center agent profiles, and reports. The CCS shall enable authorized Agency designated individuals to perform both real time and scheduled changes. The CCS management system shall be user friendly and provide the following minimum administrative capabilities:
  - a. An audit trail and change log history.
  - b. Authentication with password protection for authorized administrators.
  - c. Ability to perform scheduled and real time changes.
  - d. Ability to view the Agency CCS configuration.
7. The contractor shall provide half hourly, hourly, daily, weekly, monthly, quarterly, annual (Fiscal Year or Calendar Year according to Agency needs) and special

reports with different management views. This shall include an annual report with monthly summaries and totals for all categories of CCS management information for all data elements that can be totaled. The reports shall be available on demand or on a scheduled basis.

8. The contractor shall provide historical and real time reports with a unified view of all the communication channel activity and performance within the contact center across a single site, multiple sites (if applicable) and enterprise wide at a given time. This shall include, but is not limited to, reporting on both the queue and agent/skill levels. Both summary and detail reports shall be provided. Reporting archive data shall be available for a minimum of one year. The contractor shall provide the ability to electronically export reporting data, in a standard file format (e.g. CSV) to Agency applications (i.e. spreadsheets, databases). The Agency management reporting requirements shall be identified during a discovery session.
9. The contractor shall present report data in a user friendly format. For multi-location CCS applications, individual location reports shall have the option to present data according to an individual location's local time zone in a easy to read format (e.g. time is reported in hh:mm:dd format).
10. The contractor shall provide the subscribing Agency with access to graphical, real time reporting of the CCS queue status. The real time reporting shall monitor performance and identify all interactions (voice, email, fax, and web) by contact channel and agent status. The reports shall include summaries and totals (where applicable). The real time reporting shall provide the following minimum capabilities:
  - a. Number of inbound contacts (calls).
  - b. Status of inbound contacts (calls).
  - c. Number of contacts (calls) in queue.
  - d. Length of oldest contact (call) in queue.
  - e. Average queue time.
  - f. Number of abandon calls.
  - g. Agent status and performance statistics.
  - h. Service level information.
  - i. Number of contacts handled by workgroup or skill.
11. The contractor shall provide the capability to inform the caller of the queue status including the callers estimated wait time in queue when a queue threshold exceeds an Agency defined threshold. This can also include an option for announcing the caller's expected wait time prior to entering the queue. The contractor shall provide Agencies with the ability to change recorded announcements.
12. The contractor shall provide the capability to transmit and deliver music on hold (or recordings) to the originating caller. The music on hold source can be contractor or Agency provided according to the subscribing Agency's needs.

13. The contractor shall perform a “Discovery Session” with key stakeholders to gather requirements, review and identify the scope of work, schedule, and deliverables required to meet the Agencies CCS needs.
14. The contractor shall supply terminal devices (e.g. phones, IP phones, softphones, etc.) required for delivery of CCS if requested by the subscribing Agency. Terminals shall have the capability to support caller ID (ANI) and an optional name /message display (where applicable).
15. The contractor shall provide the capability to accommodate Agency contact center closings (e.g. scheduled holiday’s, unplanned closings, outside of normal business hours, and for maintenance activities) by providing announcements, messages, or re-routing of contacts during the period which the Agency contact center is closed.

#### **C.2.10.2.1.4.3 CCS Call Answering Service**

1. The contractor shall provide a CCS call answering service. The contractor shall provide Agencies with a complete turnkey call center operation, including the appropriate network services, technology, personnel, business processes and workflows, training, and reporting to respond to caller inquiries and meet pre-determined performance or customer satisfaction levels.
2. For CCS call answering service the contractor shall meet the following minimum requirements:
  - a. The contractor shall receive and accurately respond to caller inquiries during established Agency operating hours within the agreed upon key performance indicators.
  - b. The contractor shall manage and accurately respond to caller inquiries received during non operational hours and holidays according to the subscribing Agencies needs.
  - c. The CCS shall be interoperable with the subscribing Agencies required back office systems or databases (if required and as identified by the Agency) to deliver the specified customer service functions at the agreed upon performance levels.
  - d. The contractor shall provide resources, processes, and technology to reasonably accommodate inquiries from different types of callers as identified by the subscribing Agency. This shall include responding to inquiries from callers that may have foreign language requirements or callers with disabilities including but not limited to speech disabilities, deaf, hard-of-hearing, deaf-blind or blind (e.g. support TDD/TTY calls)
  - e. The contractor shall provide a description of their capability to quickly increase the capacity of CCS operations in crisis or high priority situations. The contractor shall quantify its capacity to provide such contact center services in terms of capacity, operating hours, staffing, language support and implementation start-up time.

3. The contractor shall provide call answering resources, as needed in order to meet the requirements specified in the Agency service order, according to the descriptions listed in Section C.2.11.2.1.4.4 below.

**C.2.10.2.1.4.4 CCS Call Answering Resource**

ID Number	Role	Description
1	Basic Call Answering	<ol style="list-style-type: none"> <li>a. Receive inbound calls and respond to caller inquiries</li> <li>b. Question callers to obtain full understanding of what information is being requested.</li> <li>c. Document all customer contacts</li> <li>d. Follow contact center operational procedures</li> <li>e. Communicate clearly and effectively</li> <li>f. Have good listening skills</li> <li>g. Ability to manage assigned performance goals</li> <li>h. High School Diploma or General Education Development (GED) certificate required</li> <li>i. A minimum of six (6) months customer service experience required</li> <li>j. English language proficiency required</li> </ol>
2	Advanced Call Answering	<ol style="list-style-type: none"> <li>a. Same requirements as Basic Call Answering</li> <li>b. Additional responsibilities as defined by the Agency</li> </ol>

4. The contractor shall provide the following deliverables for CCS call answering service:
  - a. The contractor shall perform a project start-up meeting with key stakeholders to discuss and review requirements, scope of work, schedule, and deliverables required to meet the Agencies CCS needs. A CCS Project Plan deliverable shall be included as an output of the meeting. The deliverable, at a minimum, shall include the project schedule, identify deliverable and deliverable dates, identify project roles and responsibilities, an organization chart, list of key personnel, escalation list, and identify project risks with a mitigation strategy.
  - b. The contractor shall provide a CCS Migration Plan with a migration schedule for the transfer of call/contact center operations from the incumbent call center operator (an Agency or contractor) to the contractor. The migration plan shall identify the necessary tasks and schedule to provide a seamless migration of operations and implement the contractors CCS. The migration plan shall also identify migration risks and provide a risk mitigation strategy. When this service is cancelled by an Agency, the contractor shall assist the subscribing Agency with migrating operations to the new organization responsible (successor) for the call center. The assistance shall include but is not limited to providing an accurate inventory of the Agencies CCS configuration, call history information, and access to the CCS facility for a site survey.

- c. The contractor shall establish and maintain a CCS Staffing Plan to identify the staffing, skill sets, and organizational structure required for CCS call answering service. The staffing plan shall also identify the contractor's plans for recruitment and orientation for new CCS agents
- d. The contractor shall establish and maintain a CCS Training Plan to identify initial and continuous training requirements for CCS. The training plan, at a minimum, shall describe the schedule, curriculum, materials, and resources required to ensure that the CCS agents and program content are updated according to the subscribing Agencies needs.
- e. The contractor shall establish and maintain a CCS Call Center Management Plan to document and identify the tasks and processes used for management of the CCS. It shall include detailed documentation of the subscribing Agencies call center configuration, equipment inventory, customer service and operational processes, and contact information for key call center staff. The call center management plan shall also include a description of the testing, verification, and acceptance procedures required for the delivery of the CCS
- f. The contractor shall establish and maintain a CCS Continuity of Operations Plan (COOP) designed to prevent interruption of customer service functions and mission critical operations for the CCS according to the subscribing Agencies needs. The plan shall identify risks and the steps necessary to prevent them from occurring. The plan shall define backup and restoration processes and the steps necessary to recover and restore service as quickly as possible. The plan shall describe the roles and responsibilities of the contractor and Agency personnel when it is executed. The plan shall include procedures to execute and test the plan on a regular basis to ensure preparedness for such events. The contractor shall update the COOP annually and upon implementation of any significant CCS changes that would impact the COOP.
- g. The contractor shall establish and maintain a CCS Security Plan to ensure CCS compliance with the subscribing Agencies security and privacy requirements as described in the Agencies service order. The plan shall provide an overview of the security requirements and the existing or planned controls (management, operational, and technical) for meeting those requirements. The plan shall also describe the relevant CCS systems and describe the responsibilities of individuals who access those systems.
- h. The contractor shall establish and maintain a CCS Quality Assurance (QA) Plan to ensure the requirements of the service order are performed as specified by the subscribing Agency. The plan shall identify the requirements, resources, and processes for monitoring the quality of agent interactions as well as continuous improvement initiatives. The plan shall also identify methods of improving the efficiency and effectiveness of the Agencies call

center operations, improving customer satisfaction, and how to identify trends in customer satisfaction and service delivery.

- i. The contractor shall conduct weekly status meetings with the subscribing Agency to review CCS performance metrics and discuss new and/or open CCS issues. The contractor shall provide a CCS Monthly Status Report deliverable that, at a minimum, identifies key CCS issues and their status, provides monthly performance metrics, documents accomplishments, and planned activities for the reporting period.

**C.2.10.2.2 Features**

The following Call Center/Customer Contact Center Services features in Section C.2.11.2.2.1 below are mandatory:

**C.2.10.2.2.1 Call Center/Customer Contact Center Services Features**

ID Number	Name of Feature	Description
1	Call Recording and Monitoring	<p>The contractor shall provide digital recording and monitoring of inbound and outgoing multimedia contacts (telephone, email, and web self service channels) and associated data (agent screen capture) to capture the caller experience. At a minimum, the date, time, duration, caller ID information (if available), dialogue, and identity of the agent handling the call shall be captured and recorded. Archived calls shall be able to be retrieved by date, time, agent, content, contact channel, or identity of the caller. The following minimum capabilities shall be provided:</p> <ol style="list-style-type: none"> <li>1. Archive recordings</li> <li>2. Playback of recording</li> <li>3. Provide the capability for the recording of an agent to be activated and de-activated on demand.</li> <li>4. Remote monitoring and playback</li> <li>5. Reporting (management and administrative)</li> <li>6. Scheduled and random call recording</li> <li>7. Selective recording (based on business rules)</li> </ol>

ID Number	Name of Feature	Description
		8. Support free seating 9. Total and random recording of all calls 10. Convert call recordings to .wav or mp3 file format  The call monitoring system shall also provide the capability for evaluating and scoring calls and performing random call quality reviews.
2	Collaborative Browsing	This contractor shall allow bi-directional sharing of web pages between the contract center agent and the caller. It shall enable a caller to request a co-browse session with a contact center agent. The agent shall have the capability to highlight text and scroll the browser screen to a specific section of a web page. The agent shall have the capability to push a web page to the caller and vice-versa. The contractor shall allow the capability for an agent to transfer control of a collaborative browsing session to another agent and log all collaborative interactions between the agent and caller. The contractor shall state if there are any restrictions or limitations regarding the type of web browser software used by the caller or contact center agent for use with this feature.
3	Computer Telephony Integration (CTI)	The contractor shall provide Computer Telephony Integration (CTI) capability to enable transfer of caller information and Agency specified data between the contractor and Agency specified systems simultaneously with the associated inbound contact channel (call). This feature can be used to support a diverse set of Agency applications such as screen pop/splash, intelligent routing, third party call control, keyboard dialing, enhanced reporting, and multi-channel call blending solutions.
4	Customer Contact Application	The contractor shall provide an application to track, document, and manage the CCS customer contacts across multiple contact channels. The customer contact application shall contain the following minimum capabilities: <ol style="list-style-type: none"> <li>1. Record caller contact information</li> <li>2. Record caller account information</li> <li>3. Record caller contact history and status of inquiry</li> <li>4. Record nature of the inquiry</li> <li>5. Record date and time of the contact</li> <li>6. Record call disposition</li> <li>7. Record agent handling the inquiry</li> <li>8. Assign &amp; escalate inquiries according to business rules</li> <li>9. Assign a unique case or record number to each inquiry</li> </ol> The customer contact application shall also provide the capability to create and provide scripted responses for the contact center agents. The contact system shall also provide summary and detailed management reports.
5	E Mail Response Management	The contractor shall provide e-mail response management (ERM) that shall assign a tracking ID to

ID Number	Name of Feature	Description
		<p>each email and route e-mail communication according to Agency specified business rules. The ERM shall provide the following minimum capabilities:</p> <ol style="list-style-type: none"> <li>1. Auto response</li> <li>2. Automatic acknowledgement</li> <li>3. Email classification and prioritization</li> <li>4. Email routing based upon business rules</li> <li>5. Filtering capability</li> <li>6. Content analysis and knowledge base for suggested and personalized responses</li> <li>7. Management reports</li> <li>8. Multiple language support (English and Spanish)</li> <li>9. Real time exception reports</li> </ol> <p>The ERM shall be compatible with the subscribing Agencies e-mail application.</p>
6	Interactive Voice Response (IVR)	<p>The contractor shall provide an interactive voice response application that allows callers to be provided with information based upon input from (a) telephone DTMF key pad entries or via (b) speech recognition. The minimum capabilities are listed below:</p> <ol style="list-style-type: none"> <li>1. Select pre-recorded announcement messages with the capability for announcements and provide the ability for a caller to opt out during an announcement to a predefined termination. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in (a) U.S. English, (b) Spanish (American) and (c) other foreign languages after obtaining subscribing Agency script approval.</li> <li>2. Leave caller information via telephone DTMF keypad signal or speech (e.g., name, address, account information, etc.).</li> <li>3. A means for the subscribing Agency to retrieve caller-entered DTMF or speech messages.</li> <li>4. For transcription of caller information, the contractor shall provide (a) transmission of the recorded voice files and DTMF data for each transaction to the Agency and (b) [Optional] a report of caller responses that transcribes the caller provided information for the subscribing Agency based upon a subscribing Agency's needs and transmits it to the Agency. The contractor shall provide transcription reports from English- and Spanish-speaking callers.</li> <li>5. Query a database that delivers Agency-provided information to the caller. The database may be housed in the (a) subscribing Agency or, at the subscribing Agency's discretion, (b) housed in a contractor location and updated by the subscribing Agency. Provide a default</li> </ol>



ID Number	Name of Feature	Description
		<p>routing or message (Agency option) if the database is unavailable.</p> <p>6. Provide a capability to allow callers to hear and verify their names and addresses in an Agency-provided name and address database after the caller has entered their telephone number via DTMF, or based on the caller's ANI. (Text to Speech).</p> <p>7. Support speech recognition as a valid caller input. The contractor shall support at a minimum, all spoken numeric digits as well as "yes" and "no." English and Spanish language callers shall be supported. The contractor shall be able to accept and process at a minimum 95 percent of the above speech responses. The speech responses which are not accepted shall be routed to default location designated by the subscribing Agency.</p> <p>8. Provide the capability to perform surveys (via DTMF or speech) to IVR callers. The surveys can be provided to all or a random percentage of callers according to Agency needs. Survey results shall be provided electronically to the subscribing Agency.</p> <p>9. Provide a facsimile "fax back" capability (e.g. Fax Catalog application) that shall permit callers to retrieve Agency specific documents or forms. The contractor shall fax back the request documents within one hour of the initial call and retry a minimum of 13 attempts over a six hour interval in order to complete the request. Fax transmittal shall include an option for a cover sheet (standard or customized).</p> <p>10. At the Agency's option, the caller's IVR selection(s) information shall be transferred to the Agency.</p> <p>11. The contractor's IVR capacity must be configured such that the application answers a call within 3 ring cycles for 99 % of the offered call volume (measured on an hourly basis).</p> <p>12. Features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats. These electronic form lines need not be voice feature enabled.</p> <p>13. The contractor shall provide summary reporting that at a minimum provides information on the caller, average call duration, caller opt out (transfer) and disposition of the calls within the IVR application on a daily, weekly and monthly basis.</p> <p>14. The contractor shall make available any IVR reports</p>

ID Number	Name of Feature	Description
		that are available with its equivalent commercial offerings
7	IVR - Agency Based Database (Host Connect)	<p>The contractor shall provide the ability to route calls or provide information based upon a database query(s) of information provided by a database located at the subscribing Agency premise. The query(s) could be to single, redundant, or multiple databases depending upon Agency specifications and the complexity of the application.</p> <p>The contractor shall implement and provide the appropriate interface and connectivity for the contractors IVR application to successfully query and access the subscribing Agency's database(s). The IVR caller shall have the capability to retrieve, review, and modify information located on the Agency based database based upon the subscribing Agency needs. The Agency database(s) can be a (a) mainframe (e.g. IBM System 360/370/390/3090) or (b) server based relational database.</p> <p>If the database does not respond to the network query within 250 milliseconds, an Agency defined default routing plan shall be used.</p>
8	IVR – Office Locator database	<p>The contractor shall provide the capability to enable a caller to query an Agency designed database that delivers Agency provided information (e.g. caller enters his/her zip code and the nearest Agency office location is provided. Data elements can include: Name, Address, City, State, Zip code [NACSZ] or account code) to route calls to the appropriate destination. The application can allow the callers to respond to a series of questions before call termination. The application can include routing based upon time of day, day of week, ANI, or call entered digits.</p>
9	IVR - Speech Recognition	<p>The contractor shall provide natural speech recognition for IVR applications with the ability, at a minimum, to recognize spoken vocabulary, digits, zip codes, credit card numbers, credit card expiration date, account numbers, alpha numeric numbers. At a minimum, the contractor shall provide natural speech recognition capabilities and vocabularies for both English (American) and Spanish (American) dialects. The minimum accuracy threshold for speech recognition shall be at least 95%.</p>
10	Language Interpretation Service	<p>The contractor shall provide telephone language interpretation services. The service should be available, on demand, for three way conferencing with the contact center agent and foreign language caller to provide interpretation between the caller's foreign language and English and vice versa. This feature shall have the following minimum capabilities:</p> <ol style="list-style-type: none"> <li>1. Available 24x7</li> <li>2. Accessible via a toll free number</li> <li>3. Identify the foreign language of the caller</li> </ol>

ID Number	Name of Feature	Description
		<ol style="list-style-type: none"> <li>4. Provide an appropriate interpreter within one minute of the request</li> <li>5. Provide management reports identifying the date, time, duration, interpreter, and identity of the agent requesting the service.</li> </ol> <p>The contractor shall propose and provide a list of the foreign languages available for interpretation.</p>
11	Outbound Dialer	<p>The contractor shall provide the capability for automated outbound dialing. The dialer service shall have the capability to support either centralized or distributed call center environments according to the subscribing Agency needs. The dialer shall have the following minimum capabilities:</p> <ol style="list-style-type: none"> <li>1. Automatically initiate domestic and international outbound calls</li> <li>2. Call conferencing and call transfer capability</li> <li>3. Predictive dialing - capture real-time statistics from the call queue and automatically adjusting the outbound dialing frequency according to Agency defined service level parameters</li> <li>4. Preview dialing – allow agents to preview the customer record before a outbound call is initiated and provide an option for the agent to cancel the call</li> <li>5. Receive and manage inbound calls</li> <li>6. Support agent blending. The integration of outbound and inbound call handling to determine how to best use agent resources. (agents can handle both outbound and inbound calls)</li> <li>7. Support service observation</li> <li>8. Reporting – Provide comprehensive historical, real time management, and exception reports.</li> </ol>
12	Text Chat (Web Chat)	<p>The contractor shall provide the ability to enable the contact center agents to engage in real time text chat with callers directed from their web site. The text chat shall provide the following minimum capabilities:</p> <ol style="list-style-type: none"> <li>1. Archive text chat sessions (create transcripts)</li> <li>2. Allow agents to manage multiple text chat sessions</li> <li>3. Allow file transfers</li> <li>4. View the active web page the text chat caller is on</li> <li>5. Provide a log of text chat sessions</li> <li>6. Provide an automatic spell check and grammar check option that is enabled when typing in active session.</li> <li>7. Supervisor chat monitoring</li> </ol>
13	Web Call Back	<p>The contractor shall provide the capability for a customer to request a call back by filling out a form on the Agency's web site. The call back algorithm shall be based upon the availability of a contact center agent. The call back request shall be automatically distributed to the most appropriate agent based upon availability of an agent (within Agency operating hours).</p>

ID Number	Name of Feature	Description
14	Web Call Through	The contractor shall provide the capability to enable customers browsing the Agency's web site the ability to call through (e.g. "click to talk") and simultaneously have a voice conversation with a contact center agent.
15	Workforce Management	The contractor shall provide a workforce management (WFM) system that automates forecasting and scheduling calculations based upon real time and historical contact center data. The WFM shall enable Agencies to effectively schedule resources, accurately forecast call volumes and analyze/review performance statistics for single or multiple sites and blended applications. The workforce management system should provide the following minimum capabilities:  <ol style="list-style-type: none"> <li>1. Forecast staffing needs including agent skills, skill levels, and shifts.</li> <li>2. Forecast contact volumes and workload - overall call volume and by contact channel.</li> <li>3. Provide agent scheduling and create optimized agent schedules by shift and skill.</li> <li>4. Report schedule adherence – real time tracking, alerting, and graphical reporting of agent adherence to their individual schedule.</li> <li>5. Reporting – Provide comprehensive historical, real time management, and exception reports. Reports shall include totals and summary information.</li> </ol>

**C.2.10.2.3 Interfaces**

**C.2.10.2.3.1 Network Interfaces**

Call Center/Customer Contact Center Services is an application layer service which uses underlying network service(s) to deliver customer service capabilities. Where applicable, refer to the Interfaces requirements section of this contract for the services listed below:

1. C.2.2 Circuit Switched Services
2. C.2.4 Internet Services
3. C.2.7 Virtual Private Network Services

**C.2.10.2.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI's) for Call Center/Customer Contact Center Services in Section C.2.11.2.4.1 below are mandatory:

**C.2.10.2.4.1 Call Customer Contact Center Services Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
	Critical (Optional)	99.9%	≥ 99.9%	
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

#### Notes

1. Availability is measured and calculated as a percentage of the total reporting interval time that CCS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.10.3 Reserved**

**C.2.10.4 Reserved**

**C.2.10.5 Reserved**

**C.2.10.6 Reserved**

**C.2.10.7 Reserved**

**C.2.10.8 Reserved**

#### **C.2.10.9 Customer Specific Design and Engineering Services (CSDS)**

Agencies are in need of technical support services that are directly related to Network service offerings. Customer Specific Design and Engineering Services (CSDS) enable Agencies to utilize the contractor's expertise and resources to meet their specific business requirements and objectives. The technical support can include analysis, design, implementation, and testing of network equipment and applications. The support activity can be performed as described in a Statement Of Work, on an individual case basis, according to the Agency's specific requirements. All orders issued for CSDS shall comply with the underlying terms and conditions of this contract and resulting modifications.

##### **C.2.10.9.1 Service Description**

**C.2.10.9.1.1 Functional Definition**

Customer Specific Design and Engineering Services provides a range of technical support offerings directly related to services within the scope of the Networx contract and based upon individual Agency specific requirements described in a Statement Of Work. The services that can be acquired under this offering are summarized below:

1. Network architecture design and implementation.
2. Network design validation.
3. Evaluation of network technology alternatives.
4. Simulation and testing on test bed facilities.
5. Equipment and applications testing on the contractor's live network.
6. Engineering support.

**C.2.10.9.1.2 Standards**

Customer Specific Design and Engineering Services shall comply with the specific standards as identified in the Agency Statement Of Work.

**C.2.10.9.1.3 Connectivity**

Customer Specific Design and Engineering Services connectivity requirements shall be identified in the Agency Statement Of Work.

**C.2.10.9.1.4 Technical Capabilities**

The following Customer Specific Design and Engineering Services capabilities are mandatory. The contractor's CSDS activity shall be directly related to services available on the Networx contract. All orders issued for CSDS shall comply with the underlying terms and conditions of this contract and resulting modifications. The contractor shall not invoice the Government for any items not already in the contract. The Agency Statement Of Work will define the specific requirements on an individual case basis.

1. The contractor shall provide network architecture design services. This shall include but is not limited to technical support to assist Agencies with network architecture planning and design, solutions development, and the identification and evaluation of network solutions and technologies to meet Agency business concepts and requirements. Tasks associated with this activity can include:
  - a. Requirements gathering, definition, and analysis.
  - b. Development of specifications.
  - c. Development and evaluation of alternative technical approaches.
  - d. Computer aided design, modeling and/or simulation.
  - e. Network design recommendations.
  - f. Identification of cost and performance tradeoffs.
  - g. Feasibility and capacity analysis.
  - h. Preliminary planning.

2. The contractor shall provide network and related systems design validation. The contractor shall review and validate the design of existing or proposed networks, related services, and systems identified by the subscribing Agency. The review shall include but is not limited to network performance, routing, IP addressing, numbering plans, physical/logical redundancy and diversity, network equipment, security, interoperability, and scalability. Tasks associated with this activity can include:
  - a. Assessment of network strengths, weaknesses, and vulnerabilities.
  - b. Capacity and traffic pattern analysis on current and projected traffic loads.
  - c. Measurement and assessment of network performance and availability.
  - d. Recommendations for network optimization, simplification, or cost reduction.
  - e. Identification of critical applications, protocols and vital data impacting the network.
  - f. Network discovery including development of a topology map.
  - g. Development of strategies to improve reliability, availability, and security.
  - h. Develop and validate current infrastructure drawings/schematics.
  - i. Validate service interoperability with other networks and systems.
3. The contractor shall evaluate network technologies alternatives and approaches to meet Agency requirements. The contractor shall provide a report deliverable detailing the evaluation, recommendations, and the advantages and disadvantages of each alternative.
4. The contractor shall perform modeling and simulation of applications and network services prior to implementation in a production environment. The contractor shall provide a report deliverable with the findings and recommendations upon completion of the task. The contractor shall provide any software or materials used to develop the deliverable if requested by the subscribing Agency.
5. The contractor shall ensure rigorous and thorough testing is performed under a controlled test bed environment or the contractor's production network, according to subscribing Agency's needs, to verify and evaluate the suitability and compatibility of new services. Activities can involve the application of various techniques demonstrating that a prototype performs in accordance with the objectives outlined in the original design. The contractor shall validate and verify that the services and/or applications under test operate according to the Agency's requirements and objectives. The contractor shall document the methodology, findings, and results of the testing along with any relevant recommendations.
6. The contractor shall provide technical support to facilitate the transition of services into a sustainable pilot or production service that operates on the Agencies networks. Task associated with this activity can include:

- a. Evaluation of the impact of new services upon Agency networks.
  - b. Development of transition plans.
  - c. Implementation support.
  - d. Development of test and acceptance plans and criteria.
  - e. Measurement and assessment of network performance.
7. The contractor shall provide design and engineering services for engineering prototypes relative to Network services to include but are not limited to:
- a. Installation of network hardware and software.
  - b. Configuration of network devices such as routers, switches, and gateways.
  - c. Installation of on-premises cable and network drops.
  - d. Performing testing and acceptance procedures.
- Refer to Section H.32 Service Trials for additional information.
8. The contractor shall ensure that delivery of CSDS is according to Agency requirements as described in the Statement Of Work and met within the agreed upon deliverable schedule.

**C.2.10.9.2 Features**

Not applicable.

**C.2.10.9.3 Interfaces**

**C.2.10.9.3.1 Network Interfaces**

The specific User to Network Interfaces (UNIs) at the SDP shall be identified in the Agency Statement Of Work.

**C.2.10.9.3.1.1 Customer Specific Design and Engineering Services Interfaces**

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling or Protocol Type
Refer to Agency Statement Of Work	Refer to Agency Statement Of Work	Refer to Agency Statement Of Work	Refer to Agency Statement Of Work

**C.2.10.9.4 Performance Metrics**

None. The Agency can specify and request performance metrics in their Statement Of Work.

**C.2.10.10 Storage Services (SS)**

Agencies need highly available, robust, resilient Storage Services (SS) so that Agency data can be accessed securely without interruption through reliable, disaster-tolerant systems.

**C.2.10.10.1 Service Description**



**C.2.10.10.1.1 Functional Definition**

Storage Services provide 3 types of services:

1. Backup and Restore (BBKUP&R) to enable an Agency to backup copies of Agency data to contractor's data centers to be securely stored. The contractor would restore the data as needed by the Agency.
2. Network Attached Storage (NAS) to enable an Agency to securely store and have continuous access to its files from contractor's data centers.
3. Storage Area Networks (SANs) to enable an Agency to securely store and continually access its data from contractor's data centers.

An Agency may also need additional services such as, but not limited to, assessment and development of Agency storage strategy, engineering and detailed design, and support of Agency Continuity of Operations (COOP).

**C.2.10.10.1.2 Standards**

Storage Services (SS) shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. Storage Networking Industry Association (SNIA)
  - a. SNIA Storage Management Initiative Specification VERSION 1.0.1
2. Fibre Channel (FC) Industry Association (FCIA)
  - a. SFF-8410 Specification for HSS Copper Testing and Performance Requirements Rev 16.1 March 20, 2000
3. Internet Engineering Task Force (IETF)
  - a. RFC 3347 - Small Computer Systems Interface protocol over the Internet (iSCSI) Requirements and Design Considerations. M. Krueger, R. Haagens. July 2002. (Status: PROPOSED STANDARD)
  - b. RFC 3385 - Internet Protocol Small Computer System Interface (iSCSI) Cyclic Redundancy Check (CRC)/Checksum Considerations. D. Sheinwald, J. Satran, P. Thaler, V. Cavanna. September 2002. (Status: INFORMATIONAL)
4. International Standards Organization (ISO)
  - a. IS 18810:2001: Information technology - 8 mm wide magnetic tape cartridge for information interchange - Helical scan recording - AIT-2 with MIC Format
  - b. IS 14443-4:2001: Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol

- c. IS 9541-1:1991/AM1:2001: Information technology - Font information interchange - Part 1: Architecture - Amendment 1: Typeface Design Grouping
5. International Committee for Information Technology Standards (INCITS)
- a. INCITS 131:1994 [R1999] Small Computer System Interface - 2 (SCSI-2) [T10 ]
  - b. INCITS 230:1994 [R1999] Fibre Channel (FC) - Physical and Signaling Interface (FC-PH) [T11 ]
  - c. INCITS 232:1996 [R2001] SCSI-2 Common Access Method Transport and SCSI Interface Module [T10 ]
  - d. INCITS 269:1996 [R2001] SCSI-3 Fibre Channel Protocol (FCP) [T10]
  - e. INCITS 270:1996 [R2001] SCSI-3 Architecture Model (SAM) [T10 ]
  - f. INCITS 272:1996 [R2001] Fibre Channel - Arbitrated Loop (FC-AL) [T11]
  - g. INCITS 289:1996 [R2001] Fibre Channel - Fabric Generic Requirements (FC-FG) [T11 ]
  - h. INCITS 297:1997 [R2002] Fibre Channel 2nd Generation (FC-PH-2) (formerly FC-EP) [T11 ]
  - i. INCITS 301 (formerly X3.301):1997 [R2002] SCSI-3 Primary Commands (SPC) [T10 ]
  - j. INCITS 302:1998 SCSI-3 Parallel Interface - 2 (SPI-2) [T10]
  - k. INCITS 303:1998 Fibre Channel Physical and Signaling Interface-3 (FC-PH-3) [T11]
  - l. INCITS 304:1997 [R2002] SCSI-3 Multimedia Commands (MMC) [T10]
  - m. INCITS 305:1998 SCSI Enclosure Services (SES) [T10]
  - n. INCITS 305:1998/AM1:2000 [ ] Information Technology - SCSI - Enclosure Services (SES) - Amendment 1 [T10 ]
  - o. INCITS 306:1998 SCSI-3 Block Commands (SBC) [T10]
  - p. INCITS 309:1997 [R2002] Serial Storage Architecture - SCSI-3 Protocol (SSA-S3P) [T10]
  - q. INCITS 314:1998 SCSI-3 Medium Changer Commands (SMC) [T10]
  - r. INCITS 318:1998 SCSI Controller Commands - 2 (SCC-2) [T10]
  - s. INCITS 321:1998 Fibre Channel - Switched Fabric & Switched Control Requirements (FC-SW) (Formerly FC-XS) [T11.3 ]
  - t. INCITS 325:1998 SCSI-3 Serial Bus Protocol 2 (SBP-2) [T10 ]
  - u. INCITS 326:1999 Fibre Channel (FC) 10KM Cost-Reduced Physical Variant (FC-10KCR) [T11 ] INCITS 335:2000 Information technology - SCSI-3 Stream Commands (SSC) [T10 ]

- v. INCITS 336:2000 Information technology - SCSI Parallel Interface-3 (SPI-3) [T10]
  - w. INCITS 342:2001 Fibre Channel Backbone (FC-BB) [T11.3]
6. Storage Performance Council (SPC)
- a. SPC Benchmark-1 (SPC-1), Official Specification, Revision 1.7.0 (July 2003)
7. All new versions, amendments, and modifications to the above documents and standards when offered commercially.

#### **C.2.10.10.1.3 Connectivity**

Storage Services (SS) shall connect to and interoperate with Agency data center networks including Agency SANs and LANs.

Interconnection to transfer data between Agency locations and contractor's data centers shall be accomplished by the use of underlying transport services supported by Network, such as SONET, DFS, OWS, PLS, and Ethernet..

#### **C.2.10.10.1.4 Technical Capabilities**

The following Storage Services (SS) capabilities are mandatory unless marked optional:

1. The contractor shall support the interfaces for all tiers of storage devices and services, such as Gigabit Ethernet (GigE), and Fibre Channel, as required by the Agency.
2. The contractor shall provide secure data centers to store Agency data.
  - a. The contractor shall provide logical partitioning of storage resources so that storage capacity is dedicated for use by an Agency.
  - b. The contractor shall support dedicated resources, such as but not limited to storage controllers, Fibre Channel ports, and storage cache for Agency use to the extent needed.
  - c. Reserved
  - d. The contractor shall support storage services that meet Agency security assessment and authorization requirements, including storage services for classified data if needed by the Agency.
3. Storage resources management.
  - a. The contractor shall provide management tools to the subscribing Agency which support basic storage services.
  - b. If required by the Agency, the contractor shall support the Agency's investments in storage resources by customizing the service to allow compatibility with Agency storage management policies, procedures, and tools.

4. The contractor shall perform scheduled maintenance during off-peak hours. The contractor shall ensure that contractor maintenance windows are arranged to meet Agency needs.
5. Backup and Restore (BBKUP&R) services requirements are the following:
  - a. The contractor shall backup Agency designated files and databases automatically, including files that are open at the time of the backup.
  - b. The contractor shall perform automated data backup at least daily, and, if needed by an Agency, on a more frequent schedule.
  - c. Daily incremental and full weekly backups of data shall be performed, and, if needed by an Agency, on a more frequent schedule.
  - d. The stored backup data shall be kept securely in a geographically separate location as needed by an Agency. The contractor shall provide storage facilities that meet Agency security requirements.
  - e. The contractor shall retain a full backup copy of a month's worth of data for at least three months, and for longer if needed by the Agency.
  - f. The contractor shall restore backup data as needed by the Agency.
  - g. The contractor shall provide Remote Data Replication (RDR) services, such as for Agency archive purposes, by writing Agency data into storage media and then physically transporting and storing the media in a geographically separate secure location.
    - i. The contractor shall enable both automated and manually initiated replication as needed by the Agency.
    - ii. The contractor shall provide secure storage for the media to meet Agency requirements, including storage for classified data if needed by the Agency.
  - h. Remote Data Mirroring (RDM) services shall be provided, if needed by the Agency, to enable two or more locations, such as Agency datacenters and COOP sites, to store and share the same data.
6. Network Attached Storage (NAS) services requirements are the following:
  - a. The contractor shall provide, operate, and manage storage that is scalable to meet Agency needs.
  - b. The contractor shall perform storage upgrades that shall be transparent to the Agency and the Agency shall not experience downtime during upgrades.
  - c. Rigorous security policies and procedures shall protect Agency data to meet Agency security needs.
7. Storage Area Network (SAN) services requirements are the following:
  - a. The contractor shall provide, operate, and manage storage that is scalable to meet Agency needs.

- b. The contractor shall perform storage upgrades that shall be transparent to the Agency and the Agency shall not experience downtime during upgrades.
- c. Rigorous security policies and procedures to protect Agency data to meet Agency security needs.

**C.2.10.10.2 Features for Storage Services (SS)**

None.

**C.2.10.10.3 Interfaces**

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.11.10.3.1, are mandatory unless marked optional.

**C.2.10.10.3.1 Storage Services (SS) Interfaces**

UNI Type	Interface Type	Standard	Frequency of Operation	Payload Data Rate or Bandwidth	Signaling or Protocol Type
1	Optical	IEEE 802.3z	1310 nm	1.25 Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1.25 Gbps	Gigabit Ethernet
3	Optical	IEEE 802.3	1310 nm	125 Mbps	Fast Ethernet
4	Optical	ANSI	1310 nm	133 Mbps	Fibre Channel
5	Optical	ANSI	1310 nm	266 Mbps	Fibre Channel
6	Optical	ANSI	1310 nm	531 Mbps	Fibre Channel
7	Optical	ANSI	1310 nm	2 Gbps	Fibre Channel
8	Optical	IBM	850 nm 1310 nm	1.06 Gbps	ISC
9	Optical	GR-253, ITU-T G.707	1310 nm	155 Mbps	SONET or SDH
10	Optical	GR-253, ITU- G.707	1310 nm	155 Mbps	SONET or SDH Concatenated
11	Optical	GR-253, ITU- G.707	1310 nm	622 Mbps	SONET or SDH
12	Optical	GR-253, ITU-T G.707	1310 nm	622 Mbps	SONET Concatenated
13	Optical		1310 nm	155 Mbps	ATM
14	Optical		1310 nm	155 Mbps	ATM over SONET
15	Optical		1310 nm	622 Mbps	ATM
16	Optical		1310 nm	622 Mbps	ATM over SONET
17	Optical	GR-253, ITU-T G.707	1310 nm	2.5 Gbps	SONET or SDH
18	Optical	GR-253, ITU-T G.707	1310 nm	2.5 Gbps	SONET or SDH Concatenated
19	Optical	GR-253, ITU-T G.707	1310 nm	10 Gbps	SONET or SDH
20	Copper/Optical/Coaxial Cable	10 Base-T/TX/FX (Std: IEEE 802.3)	-	Link bandwidth: Up to 10 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC
21	Copper/Optical/Coaxial	100 Base-TX/FX (Std:	-	Link bandwidth: Up to 100 Mbps	1. IP (v4/v6) 2. IEEE 802.3

UNI Type	Interface Type	Standard	Frequency of Operation	Payload Data Rate or Bandwidth	Signaling or Protocol Type
	Cable	IEEE 802.3)			Ethernet MAC
22	Optical	1000 Base-T/L/LX/B/BX/PX (Std: IEEE 802.3)	-	Link bandwidth: Up to 1 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC
23 [Optional]	Optical	10 GbE (Std: IEEE 802.3)	-	Link bandwidth: Up to 10 Gbps	2. IP (v4/v6) 3. IEEE 802.3 Ethernet MAC

#### C.2.10.10.4 Performance Metrics for Storage Services (SS)

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Storage Services (SS) in Section C.2.11.10.4.1, are mandatory unless marked optional.

##### C.2.10.10.4.1 Storage Services (SS) Performance Metrics

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
<b>Backup and Restore</b>				
<b>Av(SS/BBKUP&amp;R)</b>	Routine	99.9%	≥ 99.9%	See Note 1
<b>Grade of Service (Restore Time)</b>	Routine	30 min	≤ 30 min	See Note 2
<b>NAS</b>				
<b>Av (SS/NAS) (single server)</b>	Routine	99.9%	≥ 99.9%	See Note 1
<b>Av(SS/NAS) (clustered servers)</b>	Routine	99.99%	≥ 99.99%	
<b>Av(SS/NAS) (mirrored servers)</b>	Routine	99.999%	≥ 99.999%	
<b>EN (Total Scheduled Downtime)</b>	Routine	8 hours/month	≤ 8 hours per month	
	Critical (Optional)	8 hours/year	≤ 8 hours per year	
<b>SAN</b>				
<b>Av(SS/SAN) (Single connectivity)</b>	Routine	99.95%	≥ 99.95%	See Note 1
<b>Av(SS/SAN) (Dual connectivity)</b>	Routine	99.999%	≥ 99.999%	
<b>Time to Restore (TTR)</b>	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	< 8 hours	

Notes:

1. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the storage service is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

Availability represents the time the service is available for use by the Agency during the calendar month.

2. Restore time is the time taken to restore the first 50 GBytes of data. Therefore, all data is expected to be restored at a rate greater than 100 GBytes/hour.
3. Refer to Section C.3.3.1.2.4 for definitions and how to measure

### **C.2.10.11 Unified Messaging Service (UMS)**

Unified Messaging Service (UMS) enables Agencies to communicate more efficiently and effectively through the management of multi-media messages from a single mailbox interface.

#### **C.2.10.11.1 Service Description**

##### **C.2.10.11.1.1 Functional Definition**

Unified Messaging Service allows subscribers to manage messages from different communications media such as e-mail, voice, or fax from a single mailbox interface via the telephone or a web browser.

##### **C.2.10.11.1.2 Standards**

Unified Messaging Service shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Facsimile: ITU-T T.30, T.37, T.38, Group 3 Fax,
2. Internet Message Access Protocol (IMAP4)
3. Lightweight Directory Access Protocol (LDAP)
4. Message Application Protocol Interface (MAPI)
5. Multi-purpose Internet Mail Extensions (MIME)
6. Post Office Protocol (POP3)
7. Secure Sockets Layer (SSL)
8. Simple Message Transfer Protocol (SMTP)
9. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

##### **C.2.10.11.1.3 Connectivity**

The Unified Messaging Service shall connect to and interoperate with:

1. Internet
2. Public Switched Telephone Network

The Unified Messaging Service mailbox shall be accessible via a single telephone number or the Internet. The contractor shall provide UMS for both local and toll free telephone numbers.

#### **C.2.10.11.1.4 Technical Capabilities**

The following Unified Messaging Service capabilities are mandatory unless marked optional.

1. The contractor shall provide Agency subscribers with a single mailbox interface to retrieve, store, record, and forward messages from different media such as voice, e-mail, and facsimile. There are two distinct methods of UMS architecture described below:
  - a. Unified messaging – Provide a single unified repository (“mailbox”) and interface for multi-media message management.
  - b. Integrated messaging – Provide a single interface to multiple disparate messaging systems (voice, e-mail).

The contractor shall describe the proposed method(s) of UMS.

2. The contractor's UMS shall be accessible from a web browser (e.g. Internet Explorer, Netscape, or wireless web) to access and manage messages.
3. The contractor shall provide a mailbox with a secure login and authentication. The UMS mailbox shall provide the following minimum capabilities:
  - a. A set of mailbox management commands:
    - i. Mailbox navigation.
    - ii. Message compose/forward/reply options.
    - iii. Message playback.
  - a. Annotate or reply to e-mail messages with a voice message.
  - b. Create distribution lists (personal and system lists).
  - c. Forward e-mail messages to a fax machine.
  - d. Receive a fax and convert it to an e-mail message.
  - e. Message notification – normal and urgent prioritization.
  - f. Send message notification to different devices (Pager, phone/cell phone, Personal Digital Assistant (PDA)).
  - g. Provide a personal voice mail greeting.



- h. Allow a subscriber to return a call while listening to voice mail.
- 4. The contractor shall provide Automatic Number Information (ANI), if available, in message header information and with message notifications.
- 5. The contractor shall provide the capability to translate text messages into synthesized speech to allow e-mail and fax messages to be read back to the subscriber via the telephone.
- 6. The contractor shall provide the ability to filter and customize message handling on an individual mailbox basis.
- 7. The contractor shall provide information management capabilities such as a calendar for scheduling and address book for managing contact information.
- 8. The contractor shall provide the capability to import and export UMS calendar and address book information to Agency information stores, synchronize contact information with PDA's, and support directory services (including but not limited to Active Directory).
- 9. The contractor shall voice message files shall be stored in a standard file format (.wav or .mp3).
- 10. The contractor shall provide strong authentication access and security by means of voice recognition and voice print, if required, by the subscribing Agency. [Optional]
- 11. If an Agency's existing local or toll free telephone number was supplied to the contractor for UMS, the Agency will have the option to retain its telephone number upon termination of service or at contract expiration.

**C.2.10.11.2 Features**

The following Unified Messaging Service features in Section C.2.11.11.2.1, are mandatory:

**C.2.10.11.2.1 Unified Messaging Service Features**

ID Number	Name of Feature	Description
1	Follow Me Service	The contractor shall provide the ability to route inbound callers and messages to alternate destinations based upon business rules such as: <ol style="list-style-type: none"> <li>1. Call Status (No answer/Busy)</li> <li>2. Caller ID</li> <li>3. Day of week</li> <li>4. Time of day</li> </ol> The contractor shall provide a call waiting indication when a new incoming call has arrived.
2	Speech Enabled (Activated) Messaging	The contractor shall provide speech recognition capabilities for the subscriber to manage their mailbox for the following commands: <ol style="list-style-type: none"> <li>1. Mailbox navigation</li> <li>2. Message composition / reply</li> <li>3. Message playback</li> <li>4. Message deletion</li> </ol>

**C.2.10.11.3 Interfaces**

**C.2.10.11.3.1 Application Interface**

None. UMS is an application-layer service. The contractor shall support UMS to different devices. At a minimum, the following devices types shall be supported by UMS:

- a. Cellular phones.
- b. Facsimile (fax).
- c. Pagers.
- d. Personal Digital Assistants (PDA).
- e. Telephones.
- f. Desktop workstations.
- g. E-mail Servers.
- h. Laptop computers.

**C.2.10.11.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI's) for Unified Messaging Service in Section C.2.11.11.4-1 are mandatory.

**C.2.10.11.4.1 Unified Messaging Service Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.7%	≥ 99.7%	See Note 1
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Note:

1. Availability is measured and calculated as a percentage of the total reporting interval time that UMS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.10.12 Collaboration Support Services (CoSS)**

Agencies can utilize Collaboration Support Services (CoSS), to enable individuals and groups to share information and communicate online, in real time, from dispersed locations. CoSS provides real time instant messaging capabilities for Agencies to conduct business activity in a closed user community. This can include “one to one”,

“one to many”, and “many to many” bi-directional messaging between both internal and external entities. CoSS is an application hosted by the contractor which provides instant messaging services to multiple users. The following sections provide the requirements for CoSS which is delivered at the application layer.

#### **C.2.10.12.1 Service Description**

##### **C.2.10.12.1.1 Functional Definition**

Collaboration Support Services enables individuals and groups in disparate locations to collaborate by enabling the bi-directional, real time sharing of information via instant messaging in a private, closed user community.

##### **C.2.10.12.1.2 Standards**

Collaboration Support Services shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Internet Message Access Protocol (IMAP4) IETF RC 3501
2. Lightweight Directory Access Protocol (LDAP)
3. Message Application Protocol Interface (MAPI)
4. Multipurpose Internet Mail Extensions (MIME) IETF RFC 2045
5. Post Office Protocol (POP3) IETF RFC 1939
6. Secure Sockets Layer (SSL) encryption
7. Simple Message Transfer Protocol (SMTP) IETF RFC 2821
8. SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE)
9. ITU-T T.120 Data conferencing
10. Transmission Control Protocol/ Internet Protocol (TCP/IP) suite
11. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially

##### **C.2.10.12.1.3 Connectivity**

Collaboration Support Services shall connect to and interoperate with:

1. Internet

Collaboration Support Services is an application-layer service. The underlying network service is not included as part of this service offering.

##### **C.2.10.12.1.4 Technical Capabilities**

The following Collaboration Support Services capabilities are mandatory:

1. The contractor shall enable Agency subscribers to collaborate and share information, in real time, between groups and individuals in a closed user community.
2. The contractor shall provide Instant Messaging (IM) capability. The IM shall enable subscribers to engage in a private real time text chat between parties.

The IM shall provide the capability for individual text chat sessions and group or broadcast messages.

3. The contractor shall provide presence information which allows a subscriber provide status on his/her availability, establish a list of contacts, and identify the status of those contacts and if they are available for a IM text chat. Subscribers shall have the capability to activate presence status information settings with, at a minimum, the following options:
  - a. At a meeting
  - b. Available
  - c. Away from the computer
  - d. Busy
  - e. On the phone
  - f. Custom message assigned by the subscriber

When a presence status is activated, a scripted message to be returned to anyone attempting to IM the subscriber.

4. The contractor shall provide IM conferencing capability that enables subscribers to perform the real time exchange of information among multiple parties. A subscriber shall be able to initiate an IM conference on demand and be the moderator of the conference. The moderator shall have the capability to invite any subscriber assigned to his/her contact list to the conference. The invitee shall have the ability to decline or accept the invitation. The contractor shall support, at a minimum, a conference of at least twenty five concurrent participants. The feature shall have an option for a subscriber to initiate a private chat between subscribers during a conference.
5. The contractor shall provide the ability to store text chat messages intended for offline subscribers and deliver them when the target subscriber is available ("store and forward"). The CoSS shall store the text chat messages offline for a minimum duration of three days. The originating subscriber shall have the capability to cancel a text chat message from the store and forward queue prior to delivery.
6. The contractor shall allow the subscriber to save and archive text chat messages and search for key words within the message content.
7. The contractor shall provide the subscriber with an option for IM text chat messages to be automatically forwarded to an SMTP email address in the event he/she is offline.
8. The contractor shall provide the ability to allow or deny other subscribers from communicating with a subscriber. Before a subscriber can add another subscriber to his/her contact list they shall be required to obtain authorization from the subscriber they are attempting to add.

9. The contractor shall provide a directory service which lists all of the subscribers within the subscribing Agencies CoSS account. The directory service shall allow searching for contacts and provide the option to add a contact to the CoSS subscribers contact list.
10. The contractor shall provide the ability for a subscriber to upload a file and send it to one or more subscribers. The receiving party shall have the option to accept or reject the transfer. This capability should be available on a per subscriber basis. The subscriber shall also have the option to permanently restrict receipt of a file transfer in their profile.
11. The contractor shall provide the ability for a subscriber to push or launch a web page URL to another user.
12. The contractor shall provide the following minimum requirements to allow Agency administrative control from a Web browser:
  - a. Manage subscriber directory information (add, delete, change)
  - b. Manage access – restrict or add subscriber access and communication to external IM service users or domains
  - c. De-activate IM subscriber ID's
  - d. Assign and change subscriber passwords
  - e. Activation of an SMTP email address to forward IM messages when offline
  - f. Provide management summary reports and any reports that are available with the contractors equivalent commercial service offering
  - g. Provide audit trail for messages that, at a minimum, identifies the sender and receiver of the IM, delivery status, date and time stamps, and message body
  - h. Enable or restrict file transfer capability
13. The contractor shall provide each subscriber with a login and password. The CoSS password shall be a minimum of six alpha or numeric characters.
14. The contractor shall provide subscribers with the following minimum administrative capabilities:
  - a. Change and manage individual password
  - b. Change and maintain personal directory information
  - c. Change presence status information

15. The CoSS shall be secure and offer authentication and encryption capabilities to identify and authenticate subscribers who are authorized access to CoSS before providing such access and encrypt messages and file transfers.
16. The contractor's CoSS shall be interoperable with subscribing Agencies networks.
17. The contractor shall support dynamic content -- the ability to use Audio Visual Interleave (AVI's) files, flash, animated gif, and dynamic html pages.
18. The contractor's CoSS IM shall have the capability to communicate with other IM services. The CoSS administrator shall have the capability to allow or deny communications to other IM service users on a CoSS subscriber basis.
19. The CoSS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.
20. The contractor shall provide a technical support line for CoSS system administrators to receive support and resolve CoSS service issues.
21. The contractor shall ensure that CoSS is protected from security threats such as transmission of a Virus, Worms, and Spam over Instant Messaging (SPIM).

**C.2.10.12.2 Features**

The following Collaboration Support Services features in Section C.2.11.12.2.1 are mandatory:

**C.2.10.12.2.1 Collaboration Support Services Features**

ID Number	Name of Feature	Description
1	Branded CoSS	The contractor shall provide CoSS IM client software with a private label or Agency brand and administrative web pages with an Agency logo or image and buttons.

**C.2.10.12.3 Interfaces**

None. Collaboration Support Services is an application-layer service.

**C.2.10.12.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Collaboration Support Services in Section C.2.11.12.4.1, are mandatory:

**C.2.10.12.4.1 Collaboration Support Services Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.7%	≥ 99.7%	See Note 1
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Note

1. Availability is measured and calculated as a percentage of the total reporting interval time that CoSS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definition and measurement guidelines.

### C.2.10.13 Agency Specific Custom Services (ASCS) for FTS2001 Transition

GSA will allow Agencies, by special exception, the option to incorporate the services remaining on a FTS2001 Continuity Bridge contract into a single sole source task order for each Networkx contractor. The excepted Agency will be responsible for developing a sole source task order for each contractor from whom the Agency has not completed the transition of their services.

The Agency must prepare and approve sole source justifications and award short term task orders to temporarily move services from all Continuity Bridge contract(s) to the same provider's Networkx contract(s) and subsequently complete the transition to the Networkx provider(s) the Agency previously selected through the Fair Opportunity (FO) process. Each sole source task order will be limited to a one year or less period of performance under the Networkx contract, starting at the expiration of the Continuity Bridge contract (or earlier if GSA authorizes during Networkx contract(s) modification to add the agency's ASCS CLINs).

#### C.2.10.13.1 Service Description

##### C.2.10.13.1.1 Functional Definition

For instances where GSA provides authorization to agencies by special exception, Agency Specific Custom Services (ASCS) for FTS2001 Transition shall be offered by the contractor to support uninterrupted service to agencies for those services that have been provided under the Continuity Contract that cannot be transitioned to the Networkx Contract before the Continuity Bridge Contract ends.

The contractor shall offer ASCS on an agency specific basis only. Agency specific ASCS ICB CLINs, ASCS ICB Cases, and ASCS custom fixed priced CLINs will be added to the Networx Contract by contract modification, as mutually agreed between GSA and the Contractor.

**C.2.10.13.1.2 Standards**

The Agency Specific Custom Services (ASCS) for FTS2001 Transition shall comply with any specific standards identified within contract modifications for agency specific ASCS services.

**C.2.10.13.1.3 Connectivity**

The contractor shall work closely with each Agency to ensure connectivity requirements for ASCS solutions are identified and documented within the contract modifications for these ASCS services.

**C.2.10.13.1.4 Service Specification**

The contractor shall work closely with each Agency to ensure service specification requirements for ASCS solutions are identified and documented within the contract modifications for these ASCS services.

**C.2.10.13.2 Features**

The contractor shall propose features for the Agency Specific Custom Service (ASCS) for FTS2001 Transition on an agency specific basis only.

ASCS features required to support ASCS solutions shall be identified and documented within contract modifications for these ASCS services.

**C.2.10.13.3 Interfaces**

The contractor shall work closely with each Agency to ensure interface requirements applicable for ASCS solutions are identified and documented within the contract modifications for these ASCS services.

**C.2.10.13.4 Performance Metrics**

The contractor shall comply with any specified SLAs and performance objectives identified within contract modifications for ASCS solutions. No Networx SLAs or other Networx KPIs will apply unless specifically noted in contract modifications for ASCS solutions.



### **C.2.10.13.5 Management and Operations**

#### **C.2.10.13.5.1 Service Ordering**

The contractor shall meet and comply with the Service Ordering requirements in Section C.3.5 in addition to the task ordering requirements specific for the Agency Specific Custom Services (ASCS) for FTS2001 Transition.

The contractor shall assist agencies with Continuity Bridge disconnect/Networkx ordering.

For the excepted Agencies, the contractor shall include in the Networkx ASCS task orders the reconciled Agency Inventory of non-transitioned services remaining when the Continuity Bridge contracts expire. Networkx ASCS CLINs for Agency specific ASCS solutions will be reflected within the Networkx Inventory. Non-transitioned Continuity Bridge inventory will not be reflected in the Networkx inventory.

Networkx ASCS task orders shall have a limited period of performance (no more than one year).

ASCS task orders shall be priced using Networkx ASCS CLINs.

#### **C.2.10.13.5.2 Billing**

The contractor shall meet and comply with the Billing requirements in Section C.3.6 in addition to the billing requirements specific for the Agency Specific Custom Services (ASCS) for FTS2001 Transition.

The contractor shall ensure the billing data dictionary is updated to identify ASCS as a new service type. The agency name (three character initials) shall be added to the ICB CLIN descriptions; ASCS CLIN descriptions shall identify the agency on the ASCS task orders and separate CLINs will be created for each agency per task order. The words "for FTS2001 Transition" shall be added to the ICB CLIN descriptions to identify the task order for ASCS.

Agency specific ASCS billing solutions will be identified and documented within contract modifications, added to the Networkx Contract as mutually agreed between GSA and the Contractor.

- The contractor may elect to aggregate all services into single NRC / MRC cases or establish separate case pricing related to service categories.
- Any ASCS MRC ICB case pricing required will be established based on the reconciled starting inventory and may include usage (e.g. Toll Free), as applicable, from the baseline Continuity Bridge inventory.

- The Continuity Bridge order / billing systems will be retained to capture monthly order activity (including disconnects, moves and changes) and usage and associated SCID billing.
- Network billing adjustments (credits) to reconcile billing with actual usage will be calculated and applied based on the contractor's and agency's concurrence of the reconciliation schedule and procedures identified within contract modifications for agency specific ASCS solutions. Adjustments cannot be carried forward to this Network task order from the Continuity Bridge contract.
- An NRC and or MRC case may be charged to pay for retention of the Continuity Bridge OSS or other associated costs.

## **C.2.11 Management and Application Services**

### **C.2.11.1 TeleWorking Services (TWS)**

Agencies utilize teleworking to enable employees to perform officially assigned work duties remotely from their primary office location. TeleWorking Services (TWS) will offer Agencies services ranging from providing a teleworker's basic telecommunications connectivity to providing a fully managed service.

#### **C.2.11.1.1 Service Description**

##### **C.2.11.1.1.1 Functional Definition**

TeleWorking Services can enable geographically disperse Agency staff to perform their officially assigned job duties through the use of electronically supported communications and collaboration capabilities. The TWS will enable remote communications to Agency systems and applications from the teleworkers location.

##### **C.2.11.1.1.2 Standards**

Teleworking Services shall comply with the following standards and recommendations as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below:

1. ANSI Integrated Services Digital Network (ISDN) Standards [Optional]
2. Federal Telecommunications Recommendation (FTR) 1080B-2002 for Multi-Media Teleconferencing
3. General Routing Encapsulation Protocol (GRE) IETF RFC 2784
4. Hyper Text Transfer Protocol (HTTP) IETF RFC 2616
5. IEEE 802.11x Wireless LAN Standards [Optional]
6. IETF IP Security Protocols – IP Sec

7. ITU-T V.90, V.92
8. ITU-T: T.30 T.37, T.38, Group 3 Fax
9. Lightweight Directory Access Protocol (LDAP)
10. Point to Point Tunneling Protocol (PTPP) IETF RFC 2637
11. Remote Authentication Dial Up Service (RADIUS) IETF RFC 2865
12. Secure Sockets Layer (SSL)
13. Session Initiation Protocol - IETF RFC 3261 (SIP) [Optional]
14. Wireless Application Protocol (WAP 2.0) [Optional]
15. Wired Equivalent Privacy (WEP) [Optional]
16. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially .

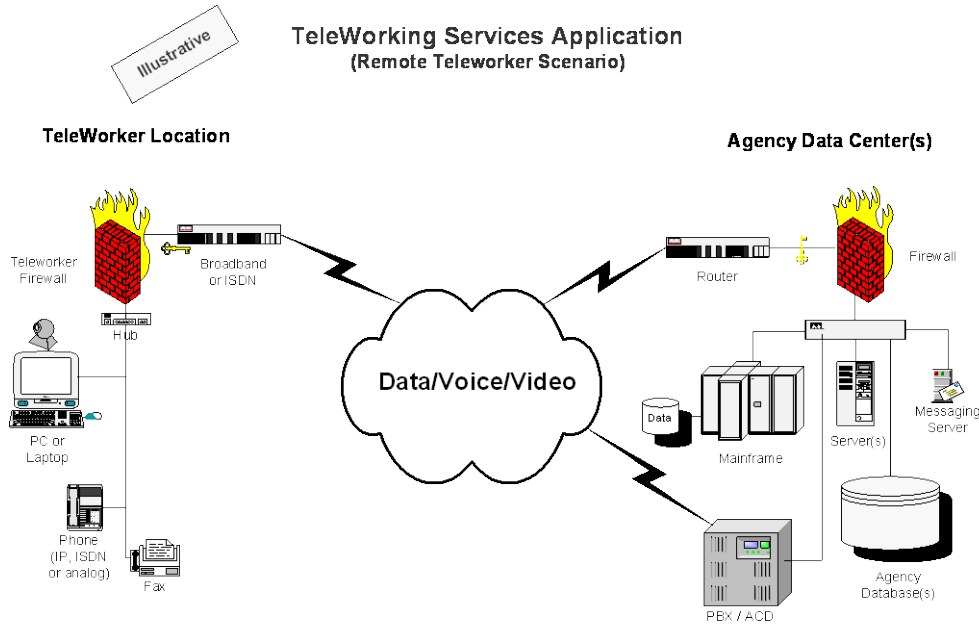
The contractor shall also comply with all applicable standards for underlying network services provided with TWS as described in section C.2.

#### **C.2.11.1.1.3 Connectivity**

Teleworking Services shall connect geographically dispersed teleworkers to and interoperate with:

1. Public Switched Telephone Network (PSTN)
2. Internet

For TWS, the contractor shall provide seamless communications from a teleworker location to an Agency. Figure C.2.12.1.1.3-1 illustrates a representative example of a TWS application for a remote teleworking scenario.



**Figure C.2.12.1.1.3-1 - TWS Application for a “Work at Home” TeleWorker**

#### C.2.11.1.1.4 Technical Capabilities

The following Teleworking Services capabilities are mandatory unless indicated otherwise:

1. TWS shall provide connectivity to enable data services and optional voice services for a remote teleworker location (or center) to communicate with Agency specified host sites and applications.
2. The contractor shall provide two different tiers of TWS.
  - a. **Tier 1 - Basic:** The contractor shall provide the basic connectivity and related components necessary to establish telework capabilities for the subscriber. The contractor shall configure and provision the TWS as part of Tier 1 service. The Agency manages the service.
  - b. **Tier 2 - Enhanced:** The contractor shall design and implement a custom service for the subscribing Agency.
3. The contractor’s TWS shall be secure and provide authentication and encryption capabilities to identify and authenticate subscribers who are authorized access to TWS before providing such access.
4. The contractor shall provide TWS service that meets the following minimum requirements:

- a. Activity log / audit trails.
  - b. Management utilities.
  - c. Class of service capabilities.
  - d. Transmission of multiple protocols.
  - e. Multiple domains and dynamic/static addressing.
5. The contractor shall provide the capability to deliver TWS to different teleworker endpoint devices. Voice service is optional. The contractor shall support the voice end point devices (a through d and f) if the contractors TWS includes a voice option. At a minimum, the following devices types shall be supported (Where applicable):
- a. Analog telephones
  - b. Facsimile devices
  - c. IP phones
  - d. ISDN telephones
  - e. Laptop or Personal Computers
  - f. Agency PBX's or ACD's
6. The contractor shall provide instructions and TWS specific training for the teleworker on how to establish and maintain TWS connections. Training shall be web based or conducted at the subscribing Agency location
7. The contractor's TWS shall have the capability to traverse and successfully interoperate with Agency firewalls and security layers.
8. The contractor shall support the transmission of any encrypted data that is generated by the subscribing Agency in a transparent manner.
9. The contractor shall provide logical isolation to protect against unauthorized modification while provisioning and testing instances of TWS service.
10. The contractor's TWS shall be compatible with Agency teleworker applications and client software including but not limited to Netscape Messenger, MS Outlook/Exchange, IBM Lotus Notes, Novell Group Wise, or MS NetMeeting.

**C.2.11.1.2 Features**

The following TWS features in Section C.2.12.1.2.1 are mandatory unless marked optional:

**C.2.11.1.2.1 Teleworking Services Features**

ID Number	Name of Feature	Description
1	Anti Virus Management	The contractor shall provide the capability to protect the TWS Agency and subscriber from a virus. Minimum

ID Number	Name of Feature	Description
		capabilities include detection, notification and removal of a virus. Refer to Section C.2.10.4.
2	Follow Me Service [Optional]	The contractor shall provide the capability to route inbound calls, at a minimum, to three alternate numbers with options for sequential or parallel routing to destination phone numbers (i.e. ring simultaneous phone numbers), or to voice mail. The subscriber shall be able to manage a "find me list" and select any combination of different phone numbers in a user defined search order to ensure delivery of important calls.
3	Instant Messaging [Optional]	The contractor shall provide Instant Messaging capabilities. Minimum requirements include providing: <ol style="list-style-type: none"> <li>1. Enable file transfer</li> <li>2. Text chat</li> <li>3. Presence information</li> <li>4. Contact lists ("buddy and group lists")</li> <li>5. User authorization</li> </ol>
4	Intrusion Detection and Prevention	The contractor shall provide monitoring, attack recognition, and response to network security threats. Refer to Section C.2.10.2.
5	Managed Firewall	The contractor shall provide a managed firewall service to protect the Agency network endpoint (s) from unauthorized inbound Internet based intrusion. Refer to Section C.2.10.1.
6	Managed Moves, Adds, Changes Support	The contractor shall provide management support and act as a single point of contact for Agency Moves, Adds, and Changes with respect to TWS service. The contractor shall perform changes including: <ol style="list-style-type: none"> <li>1. Updating router software and configuration</li> <li>2. Adding a protocol</li> <li>3. Modifying the addressing scheme</li> <li>4. Adding, moving or removing CPE</li> <li>5. Changing the network configuration</li> <li>6. Optimizing network routes</li> <li>7. Network Address Translation (NAT) or Port Address Translation (PAT) management</li> </ol>
7	Teleworker Firewall	This contractor shall protect teleworker's end point from unauthorized inbound Internet based intrusion with anti-virus protection and filtering capabilities. The Firewall is premise based and located at teleworker TWS end point.
8	Video Conferencing [Optional]	The contractor shall enable TWS subscribers to utilize point to point and multipoint desktop video conference capability.
9	Voice Mail [Optional]	The contractor shall provide a voice mail box including voice messaging transmission, reception, and storage for 24x7 except for periodic scheduled maintenance. The contractor shall provide the following minimum <ol style="list-style-type: none"> <li>1. At least thirty minutes of storage time (or 15 messages)</li> <li>2. Ability to remotely access voice mail services</li> <li>3. Secure access to voice mail via a password or PIN</li> <li>4. Automatic notification when a message is received</li> </ol>

ID Number	Name of Feature	Description
		5. Capability to record custom voice mail greetings 6. Call answering for a busy or ring no answer condition
10	Voice Service [Optional]	The contractor shall provide inbound and outbound voice calling capabilities with the following minimum capabilities: 1. Call Waiting 2. Caller ID 3. Caller ID Block (permanent or on a per call basis) 4. Three Way Conference Call
11	Vulnerability Scanning [Optional]	The contractor shall provide real time network scanning for potential entry points exposed to malicious attack through an automated scanning service that probes Internet-facing devices for vulnerability. Refer to Section C.2.10.3.

**C.2.11.1.3 Interfaces**

**C.2.11.1.3.1 Network Interface**

Teleworking Services is an application-layer service that uses underlying network service(s) to transport traffic from the service delivery points (SDP's) for teleworker endpoints such as the Agency data center or teleworker location. Please refer to the Interface requirements section for the UNI's and SDP's for the respective services listed below (Where applicable):

1. C.2.2 Voice Services [Optional]
2. C.2.4 Internet Services
3. C.2.5.1 Private Line Services [Optional]
4. C.2.6.1 Combined Services [Optional]
5. C.2.7 Virtual Private Network Services

**C.2.11.1.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI's) for Teleworking Services in Section C.2.12.1.4.1 are mandatory.

**C.2.11.1.4.1 Teleworking Services Performance Metrics**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 1
	With Dispatch	8 hours	≤ 8 hours	

The contractor shall also meet any KPI's specified in section C.2 for any underlying network service(s) provided with delivery of TWS (Where applicable).

## Note:

1. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

**C.2.12 Access Services****C.2.12.1 Reserved****C.2.12.2 Wireline Access Service (WLNAS)**

Wireline Access Service connects an Agency location with permanently-established (always on), reliable duplex (bi-directional) bandwidth to a network. The range of line speeds and reliability options provided within this service category allow Government users to satisfy their diverse needs for accessing networks.

**C.2.12.2.1 Service Description****C.2.12.2.1.1 Functional Definition**

WLNAS is an SDP to POP connecting service, i.e., it connects the SDP at the Agency location to the Point of Presence of the Agency-designated network. WLNAS connection is permanently established unless a service-request for modification, move, or disconnect is received. This service can be used for any end-user's application, such as voice, data, video, and multimedia that can be supported by WLNAS such as SONET, EthS and SS under Networx Enterprise.

**C.2.12.2.1.2 Standards**

Wireline Access Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. ANSI T1.102/107/403/503/510 for T1
2. ANSI T1.607/610 for ISDN PRI
3. Telcordia PUB GR-499-CORE for T3
4. ANSI T1.105 and 106 for SONET
5. Telcordia PUB GR-253-CORE for SONET
6. ITU-TSS G.702 and related recommendations for E1 and E3
7. Frequencies grid and physical layer parameters for Optical Wavelength
  - a. DWDM: ITU G.692 and G.694 as mandatory and G.709 and G.872 as optional
  - b. WDM: ITUG.694.2 and Telcordia GR 253
8. Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009
9. EIA/TIA-559, Single Mode Fiber Optic System Transmission Design
10. Telcordia GR-20-CORE for Generic Requirements for Optical Fiber and Optical Fiber Cable GR-253 (SONET), and GR-326 (Connector)



11. The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards when offered commercially.

#### C.2.12.2.1.3 Connectivity

Wireline Access Service will connect to and interoperate with:

1. Government specified locations (e.g., SDPs, such as PBX, Multiplexer, Router, Video codec, and Group 4 FAX)
2. Agency-designated network POP

#### C.2.12.2.1.4 Technical Capabilities

The following Wireline Access Service capabilities are mandatory unless marked optional:

1. Shall support integrated access of different services (e.g., VS, IPS)
  - a. Over pre-allocated channels for channelized transmission service (e.g., Channelized T1)
  - b. Over same channel (e.g., Unchannelized T3, SONET OC-3c) of IP packets for Converged IP Services
  - c. It shall be possible to use same access circuits (i.e., trunks) for VS and TFS.
2. Shall be transparent to any protocol used by the GFP.
3. All bit sequences transmitted by the GFP through the SDP shall be treated with data transparency
4. Shall provide network-derived clocking.
5. The following categories (i.e., data rates) of WLNAS service shall be supported:
  - (a) **T1**. This category of WLNAS service shall support a line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 service as follows:
    - (1) Channelized T1. In this mode, 24 separate DS0s clear channels of 56/64 kbps shall be supported.
    - (2) Unchannelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
  - (b) **Fractional T1**. (optional) This category of WLNAS service shall support two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps.

- (c) **ISDN PRI.** This category of WLNAS service shall support 23 separate DS0 clear channels of 56/64 kbps over an interface of ISDN PRI (23B+D) with a line rate of 1.544 Mbps.
- (d) **T3.** This category of WLNAS service shall support a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 service as follows:
  - (1) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
  - (2) Unchannelized T3. In this mode, a single 43.008 Mbps payload shall be supported.
- (e) **Fractional T3 (optional)** This category of WLNAS service shall support three, four, five, or seven adjacent DS1 clear-channels over an interface of T3.
- (f) **E1 (Optional).** This category of WLNAS service shall support a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:
  - (1) Channelized E1. In this mode, 30 separate DS0 clear channels shall be supported.
  - (2) Unchannelized E1. In this mode, a single 1.92 Mbps information payload shall be supported.
- (g) **E3 (Optional).** This category of WLNAS service shall support a line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:
  - (1) Channelized E3. In this mode, 16 separate E1 channels shall be supported.
  - (2) Unchannelized E3. In this mode, a single 30.72 Mbps information payload shall be supported.
- (h) **SONET OC-3 (Optional).** This category of WLNAS service shall support a line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c service as follows:
  - (1) Channelized OC-3. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, shall be supported.

- (2) Concatenated OC-3c. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps shall be supported.
- (i) **SONET OC-12** (Optional). This category of WLNAS service shall support a line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c service as follows:
  - (1) Channelized OC-12. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, shall be supported.
  - (2) Concatenated OC-12c. In this mode, a single channel equivalent to information payload data rate of 594.432 Mbps shall be supported.
- (j) **SONET OC-48** (Optional). This category of WLNAS service shall support a line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c service as follows:
  - (1) Channelized OC-48. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, shall be supported.
  - (2) Concatenated OC-48c. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps shall be supported.
- (k) **SONET OC-192** (Optional). This category of WLNAS service shall support a line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c service as follows:
  - (1) Channelized OC-192. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, shall be supported.
  - (2) Concatenated OC-192c. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps shall be supported.
- (l) Reserved
- (m) **DS0** This category of WLNAS service shall support informational payload data rates of 56 Kbps and 64 Kbps.
- (n) **Subrate DS0** (Optional) This category of WLNAS service shall support subrate DS0 at information payload data rates of 4.8, 9.6, and 19.2 Kbps.
- (o) **Optical Wavelength** (Optional). Bi-directional wavelengths (WDM and ASTN) connections to an optical network for the following speeds:
  - (1) OC-48
  - (2) OC-192
  - (3) OC-768 (Optional)

(p) **Dark Fiber** (Optional). Dark Fiber shall support the following capabilities:

- (1) Deployed fiber shall support both single-mode and multimode fibers
- (2) Deployed fibers shall be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1
- (3) Deployed fibers shall be capable of operating in the “C”, and “L” bands. Support for the “S” band will also be required when commercially available.

All other WLNAS data rates, including those that are available or that become available commercially from the contractor during the life of the contract [Optional].

**C.2.12.2.2 Features**

The following Wireline Access Service features in the Section C.2.13.2.2.1 below are mandatory.

**C.2.12.2.2.1 Wireline Access Service Features**

ID Number	Name of Feature	Description
1	Access Route or Path Diversity	<p>The contractor shall supply at least two physically-separated routes for access diversity with the following options:</p> <ul style="list-style-type: none"> <li>1. Between an SDP and its associated connecting network’s point, or</li> <li>2. Between an SDP and at least two connecting network points.</li> </ul> <p>These diverse routes shall:</p> <ul style="list-style-type: none"> <li>1. Not share any common telecommunications facilities or offices including common building entrance.</li> <li>2. Maintain a minimum separation of 30 feet throughout all diverse routes, except for cable crossovers, between premises/buildings where an SDP and its associated network connecting point are housed.</li> <li>3. Maintain a minimum vertical separation of two feet, with cables encased (separately) in steel or concrete for cable crossovers.</li> </ul> <p>The Government recognizes that uncompromised (i.e., adhering to the minimum separation requirements as described above) diversity may not be available in some locations. Where uncompromised diversity is not available, the contractor shall:</p> <ul style="list-style-type: none"> <li>1. Exert best efforts to propose an acceptable arrangement along with documentation describing the compromise.</li> <li>2. An acceptable alternative shall be negotiated, on an individual case basis, if diversity is not available or the compromised diversity is not acceptable to the Government.</li> </ul> <p>When access diversity has been provided by the contractor, the Government may at its discretion, elect to send telecommunications</p>

ID Number	Name of Feature	Description
		<p>traffic over:</p> <ol style="list-style-type: none"> <li>1. Only one route (i.e., the primary route) thereby keeping the second route (i.e., the diverse route) inactive until needed.</li> <li>2. Both routes on an ongoing basis, except where automatic re-routing equipment is utilized.</li> </ol> <p>The contractor shall provide the capability for the automatic switching of transmission in real-time, negotiated on an individual case basis:</p> <ol style="list-style-type: none"> <li>1. From the primary access route to the one or more diverse access routes; and,</li> <li>2. From the diverse access route to the primary access route.</li> </ol> <p>The contractor shall exercise the following control measures on the configuration or the reconfiguration of the diverse access route:</p> <ol style="list-style-type: none"> <li>1. The contractor shall provide within 30 calendar days of the implementation of access diversity and again thereafter when a change is made, a graphical representation (e.g., diagrams, maps) of access circuit routes to show where diversity has been implemented.</li> <li>2. The contractor shall provide to the Agency, with a copy to the PMO, written notification for Government approval of any proposed reconfiguration of routes, previously configured for access diversity at least 30 calendar days in advance of implementation.</li> <li>3. The contractor shall conform to the requirements for performance for each diverse route as specified in Section C.2.13.2.4.</li> <li>4. In addition, the contractor shall establish internal control (i.e., electronic flagging of routes) to prevent the accidental dismantling of diversified routes, especially during routine route optimization initiatives by the contractor.</li> </ol>
2	Access Route or Path Avoidance	<p>Between an SDP and its associated connecting network point, the contractor shall supply the capability for a customer to define a geographic location or route to avoid.</p> <p>However, the Government recognizes that avoidance may not be available in some locations. Where avoidance is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the reasons for the unavailability</p> <p>The contractor shall exercise the following control measures on the configuration or the reconfiguration of the avoidance access route:</p> <ol style="list-style-type: none"> <li>1. The contractor shall provide within 30 calendar days of the implementation of access avoidance and again thereafter when a change is made, a graphical representation (e.g., diagrams, maps) of access circuit routes to show where avoidance has been implemented.</li> <li>2. The contractor shall provide to the Agency, with a copy to</li> </ol>

ID Number	Name of Feature	Description
		<p>the PMO, written notification for Government approval of any proposed reconfiguration of routes, previously configured for access avoidance at least 30 calendar days in advance of implementation.</p> <p>3. The contractor shall conform to the requirements for performance for each avoidance route as specified in Section C.2.13.2.4.</p> <p>4. In addition, the contractor shall establish internal control (i.e., electronic flagging of routes) to prevent the accidental dismantling of avoidance routes, especially during routine route optimization initiatives by the contractor.</p>

### C.2.12.2.3 Interfaces

The user-to-network interfaces (UNIs) at the SDP, as defined in the Section C.2.13.2.3.1, are mandatory unless indicated marked optional:

#### C.2.12.2.3.1 Wireline Access Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403]	Up to 1.536 Mbps	Transparent
6	ISDN PRI [Std: ANSI T1.607/610]	Up to 1.472 Mbps	Transparent
7	T3 [Std: Telcordia GR-400-CORE]	Up to 43.008 Mbps	Transparent
8	SONET OC-3 (Std: ANSI T1.105 and 106) (Optional)	148.608 Mbps	Transparent
9	SONET OC-3c (Std: ANSI T1.105 and 106) (Optional)	148.608 Mbps	Transparent
10	E1 [ Std: ITU-TSS G.702] (Optional)	Up to 1.92 Mbps	Transparent
11	E3 [ Std: ITU-TSS G.702] (Optional)	Up to 30.72 Mbps	Transparent
12	SONET OC-12 (Std: ANSI T1.105 and 106) (Optional)	594.432 Mbps	Transparent
13	SONET OC-12c (Std: ANSI T1.105 and 106) (Optional)	594.432 Mbps	Transparent
14	SONET OC-48 (Std: ANSI T1.105 and 106) (Optional)	2.377728 Gbps	Transparent
15	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
	(Optional)		
16	SONET OC-192 (Std: ANSI T1.105 and 106) (Optional)	9.510912 Gbps	Transparent
17	SONET OC-192c (Std: ANSI T1.105 and 106) (Optional)	9.510912 Gbps	Transparent

#### C.2.12.2.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Wireline Access Service in Section C.2.13.2.4.1, are mandatory unless marked optional:

##### C.2.12.2.4.1 Wireline Access Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.8%	≥ 99.8%	See Note 1 and See Note 3
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	

Notes:

1. A service is considered unavailable when a circuit experiences 10 consecutive severely errored seconds (SES) [Standard: Telcordia PUB GR-499-CORE]. An unavailable circuit is considered available when restoration activities have been completed and 30 consecutive minutes have passed without any errored seconds, to account for stability and proving period. However, if there is no error second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time. WLNAS availability is calculated as a percentage of the total reporting interval time that WLNAS is operationally available to the Agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Refer to Section C.3.3.1.2.4 for definition and how to measure.
3. Refer to Sections C.2.5.4.1.4 and C.2.5.4.2.4 for Optical Wavelength and Section C.2.5.3.4 for Dark Fiber.

#### C.2.12.3 Broadband Access Service (BBAS)

Broadband Access Service connects an Agency location with permanently-established (always on), reliable broadband bandwidth to an Agency-designated data network or the Internet over communication facilities such as Digital Subscriber Line (DSL), Ethernet Access, Cable High-Speed Service, and Fiber-To-The-Premises (FTTP). The range of broadband line speeds (e.g., 256 kbps to up to 1Gbps) and reliability options

provided within this service will allow Agency users to satisfy their diverse needs for accessing Agency-designated data networks. With this service, end-user's applications such as desktop video conferencing, distance learning, and transferring of large files, can be realized.

### **C.2.12.3.1 Basic Service Description**

#### **C.2.12.3.1.1 Functional Definition**

Broadband Access Service includes dedicated transmission access service between an Agency location and Agency-designated network (such as transport network or the Internet). BBAS is an SDP to POP connecting service, i.e., it connects the SDP at the Agency location to the Point of Presence of the Agency-designated network. BBAS connection is permanently established unless a service request for modification, move, or disconnect is received. This service can be used for any end-user's application such as desktop video conferencing, distance learning, and transferring of large data files.

#### **C.2.12.3.1.2 Reserved**

#### **C.2.12.3.1.3 Connectivity**

Broadband Access Service shall connect to and interoperate with:

1. Agency specified locations (e.g., SDPs, such as LAN, Router, Work station, Video codec, and Group 4 FAX)
2. Agency-designated network POP

#### **C.2.12.3.1.4 Technical Capabilities**

The following Broadband Access Service capabilities are mandatory unless marked optional:

#### 1. Broadband Access Service

(a) **DSL**. This category of access service shall:

(1) Provide the following types of DSL services, at a minimum:

- i. Asymmetric DSL (ADSL). Support ADSL asymmetric data rates for upstream and downstream traffic as follows:
  - (a) Upstream: Data rates range from 128 to 640 Kbps (e.g., 256 Kbps) and optionally to 768 Kbps.
  - (b) Downstream: Data rates range from 1.5 Mbps to 6 Mbps (e.g., at 1.5, 2, 3, 4, 5, and 6 Mbps). Speeds up to 9 Mbps is optional.
- ii. Symmetric DSL (SDSL). Support SDSL symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates up to and including 1.5 Mbps. 2.3 Mbps is optional



- iii. [Optional] ISDN IDSL (IDSL). Support ISDN symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates of 144 Kbps.

(2) Comply with the following standards for ADSL and SDSL as applicable.

- i. ADSL and DSL Forums
- ii. ITU-TSS Recommendation G.992 for ADSL (interoperable DSL modem and DSLAM line card)
- iii. ANSI T1.413 (compatible DSL modem and DSLAM line card from the same manufacturer)

(3) Comply with the following standards for IDSL as applicable.

- i. ISDN Forum

(4) Split integrated voice and data traffic for ADSL and SDSL to direct voice traffic to the telephone unit/set and data traffic to the ADSL/SDSL modem.

(b) **Ethernet Access [Optional]**. If offered, this category of access service shall:

- i. Provide access to Ethernet service/network through the use of data link layer 2 protocol and be transparent to the upper layer protocols (i.e., layer 3 and above) for:

- 1. Ethernet LAN at 10 Mbps
- 2. Ethernet LAN at 100 Mbps
- 3. Ethernet LAN at 1 Gbps
- 4. Ethernet LAN at 10 Gbps (Optional).

ii. Comply with the following standards for Ethernet Access as applicable.

- i. IEEE 802.3, including 10 Base-T/TX/FX, 100 Base-TX/FX, 1000 Base-T/FX/L/LX/B/BX/PX, and 10 Gigabit Ethernet (IEEE 802.3ae and 10 GbE)

iii. Support the following payload data rates for the Ethernet Access link:

- i. 10 Mbps
- ii. 100 Mbps
- iii. 1 Gbps

- iv. 10 Gbps (Optional)

(c) **Cable High-Speed Service [Optional]**. If offered, this category of access service shall:

- (1) Provide data rates of 256 Kbps to 30 Mbps as follows:
  - i. From 256 Kbps to a maximum of 5 Mbps (Standard: DOCSIS 1.0)
  - ii. From 256 Kbps to a maximum of 10 Mbps (Standard: DOCSIS 1.1)
  - iii. From 256 Kbps to a maximum of 30 Mbps (Standard: DOCSIS 2.0) (Optional)
- (2) Comply with the following DOCSIS (Cable Labs) standards as applicable.
  - i. DOCSIS 1.0
  - ii. DOCSIS 1.1
  - iii. DOCSIS 2.0

2. **FTTP [Optional]**. If offered, this category of access service shall provide data rates over fiber as follows:

- a. 5 Mbps (downstream) and 2 Mbps (upstream)
- b. 15 Mbps (downstream) and 2 Mbps (upstream)
- c. 30 Mbps (downstream) and 5 Mbps (upstream).

**C.2.12.3.2 Features**

The following Broadband Access Service features in Section C.2.13.3.2.1 below are mandatory unless marked optional:

**C.2.12.3.2.1 Broadband Access Service Features**

ID Number	Name of Feature	Description
1 [Optional]	Customer End Bridge Management (Specific to Ethernet Access)	The contractor shall provide customers with the ability to monitor their Ethernet LANs by allowing them access to the end bridge devices that are provisioned as a part of the Ethernet Access service using SNMP management protocol for the following functions: <ul style="list-style-type: none"> <li>1. Perform visibility test on the end bridge to show connectivity between the main location and remote site</li> <li>2. Receive traps from the end bridge when error conditions occur</li> <li>3. Obtain statistical Information about the bridge and their LAN segments</li> </ul>
2 [Optional]	Specific to Cable-TV Service (for Cable High-Speed Service)	The contractor shall split integrated "Cable High-Speed Service" and "Cable-TV Service" to direct "Cable High-Speed Service" traffic to cable-modem and "Cable-TV" traffic to user's TV set and shall provide various "Cable-TV Service" channels as available commercially from the contractor.

**C.2.12.3.3 Interfaces**

The User-to-Network Interfaces (UNIs) at the SDP, as defined in the Section C.2.13.3.3.1, are mandatory unless marked optional:

### C.2.12.3.3.1 Broadband Access Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	10 Base-T/TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 10 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
2	100 Base-TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 100 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
3	1000 Base-T/LX/B/BX/PX (Std: IEEE 802.3)	Link bandwidth: Up to 1 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
4 [Optional]	10 GbE (Std: IEEE 802.3)	Link bandwidth: Up to 10 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
5	ITU-TSS V.35	Link bandwidth: Up to 1.92 Mbps	1. Transparent 2. IPv4/v6
6	USB 2.0 (Std: USB Implementers' Forum)	Link bandwidth: Up to 30 Mbps [maximum USB 2.0 bandwidth is 480 Mbps]	1. Transparent 2. IPv4/v6
7 [Optional]	T1 (Std: Telcordia SR-TSV-002275; ANSI T1.403)	Up to 1.536 Mbps	1. Transparent 2. IPv4/v6
8 [Optional]	ISDN BRI (Multirate) (Standard: ANSI T1.607 and 610)	144 Kbps	1. ITU-TSS Q.931 2. IPv4/v6

Note: IPv6 shall be supported when offered commercially by the contractor

### C.2.12.3.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Broadband Access Service in Section C.2.13.3.4.1 are mandatory unless marked optional:

#### C.2.12.3.4.1 Broadband Access Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Latency	Routine	50 ms	≤ 50 ms	See Note 2
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

## Notes:

1. A service is considered unavailable when a circuit experiences 10 consecutive Severely Errored Seconds (SES) [Standard: Telcordia PUB GR-418-CORE]. An unavailable circuit is considered available when restoration activities have been completed and 30 consecutive minutes have passed without any errored seconds, taking into account stability and proving period. However, if there is no error second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time. BBAS availability is calculated as a percentage of the total reporting interval time that BBAS is operationally available to the Agency. Availability is computed by the standard formula:  

$$\text{Availability} = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
2. Latency is defined as the sum of queuing, processing, and propagation time.
3. Refer to Section C.3.3.1.2.4 for definition and how to measure.

**C.2.12.4 Wireless Access Service (WLSAS)**

Wireless Access Service connects Agency locations with wireless access through roof-top antenna to an Agency-designated network (e.g., Networx) or the Internet over broadband wireless communication facility/network. This service can be used for any end-users' application such as voice, data, Internet, and video services. WLSAS will provide broadband wireless access to Agency locations where landline access is not available through broadband wireless technologies/networks (e.g., MMDS, LMDS, and Ultra High at 2 to 66 GHz and an optional upper limit of 90 GHz spectrum and National Guard Frequencies at 1.755 to 1.850 GHz Spectrum through roof-top antenna). This service can be used for Networx services, e.g., VS, NBIP-VPNS, and VTS.

**C.2.12.4.1 Basic Service Description****C.2.12.4.1.1 Functional Definition**

Wireless Access Service provides broadband wireless transmission access to the Internet or to an Agency-designated network from Agency locations to an Agency-designated network such as Networx. Broadband wireless supports protocol-transparent (i.e., physical level) transmission for services such as VS, NBIP-VPNS, and VTS.

WLSAS is an SDP to POP connecting service, i.e., it connects the SDP (i.e., Agency location) to the Point of Presence of the Agency-designated network or the Internet.

**C.2.12.4.1.2 Standards**

Wireless Access Service shall comply with the following standards, as applicable:

1. Standards based on IEEE 802.16 (in the future when available commercially)

2. All new versions, amendments, and modifications to the above documents and standards as they become applicable.

**C.2.12.4.1.3 Connectivity**

Wireless Access Service shall connect to and interoperate with:

1. Government specified locations (e.g., SDPs, such as LAN, Router, Work station, Video codec, and Group 4 FAX).
2. Agency-designated network POP.

**C.2.12.4.1.4 Technical Capabilities**

The following category of Wireless Access Service is mandatory unless marked optional:

- a. **Broadband Wireless.** This category of service shall provide broadband wireless point-to-point and point-to-multipoint protocol-transparent (i.e., physical level) transmission connections between two or more SDPs or to an Agency-designated network such as Networx for services (e.g., VS, NBIP-VPNS, and VTS) or to the Internet.

The following symmetric data rates shall be supported:

- a. DS1
- b. NxDS1s (where N=2 through 27)
- c. DS3
- d. E1 [Non-domestic]
- e. NxE1s (where N=2 through 15) [Non-domestic]
- f. E3 [Non-domestic]

The following capabilities are optional:

- g. Wireless access through non line of sight antenna
- h. Higher data rates (e.g., SONET OC-3).

**C.2.12.4.2 Features**

The following Wireless Access Service features in Section C.2.13.4.2.1, are mandatory unless marked optional:

**C.2.12.4.2.1 Wireless Access Service Features**

ID Number	Name of Feature	Description
1	Multipoint connection	This feature shall allow connection of three or more subscribers' premises for the same connection

### C.2.12.4.3 Interfaces

The User-to-Network Interfaces (UNIs) at the SDP, as defined in the Section C.2.13.4.3.1, are mandatory unless marked optional:

#### C.2.12.4.3.1 Wireless Access Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	ITU-TSS V.35	Up to 1.92 Mb/s	Transparent
2	EIA RS-449	Up to 1.92 Mb/s	Transparent
3	EIA RS-232	Up to 19.2 kb/s	Transparent
4	EIA RS-530	Up to 1.92 Mb/s	Transparent
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403]	Up to 1.536 Mb/s	Transparent
6	T3 [Std: Telcordia GR-400-CORE]	Up to 43.008 Mb/s	Transparent

### C.2.12.4.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance indicators (KPIs) for Wireless Access Service in Section C.2.13.4.4.1, are mandatory unless marked optional:

#### C.2.12.4.4.1 Wireless Access Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. A service is considered unavailable when a wireless connection/circuit experiences 10 consecutive Severely Errored Seconds (SES) (Standard: Telcordia PUB GR-418-CORE). An unavailable connection is considered available when restoration activities have been completed and 30 consecutive minutes have passed without any errored seconds, taking into account stability and proving period. However, if there is no error second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time.

WLSAS availability is calculated as a percentage of the total reporting interval time that WLSAS is operationally available to the Agency. Availability is

$$\text{Availability} = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

computed by the standard formula:

2. Refer to Section C.3.3.1.2.4 for definition and how to measure.

### C.2.12.5 Satellite Access Service (SatAS)

Satellite Access Service connects Agency location with dedicated and reliable satellite based transmission to the Agency-designated network or Internet where landline access facilities and/or bandwidth may not be available. The connection from satellite earth station to the SDP is also included in this service. This service could be used for access connection to voice, data, and video traffic. The service provides full-duplex and half-duplex transmissions using C-band, Ku-band, and Ka-band satellites.

#### C.2.12.5.1 Basic Service Description

##### C.2.12.5.1.1 Functional Definition

Satellite Access Service provides dedicated and adhoc (i.e., reservation-based) satellite transmission between Agency location and Agency-designated network (transport network or Internet). SatAS is an SDP to POP connecting service, i.e., it connects the SDP at the Agency location to the Point of Presence of the Agency-designated network. The connection between the locations receiving this service is permanently established unless a service request for modification, move, or disconnect is received.

This service can be used for any user applications, such as voice, data, video, and multimedia; and, may include Government end-to-end encrypted communications.

##### C.2.12.5.1.2 Standards

Satellite Access Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Satellite transponders' bands frequency allocations and channel bandwidth (FCC), as applicable:
  - a. C-Band. Uplink: 5.9 to 6.4 GHz; Downlink: 3.7 to 4.2 GHz; Bandwidth: 500 MHz
  - b. Ku-Band. Uplink: 14 to 14.5 GHz; Downlink: 11.7 to 12.2 GHz; Bandwidth: 500 MHz
  - c. Ka-band. Uplink: 30 to 31 GHz; Downlink: 20 to 21 GHz; Bandwidth: 500 MHz (when available commercially)
2. Reserved
3. Reserved
4. Transmission Performance and GFP Interfaces
  - a. ANSI T1.102/107/403/503/510 for T1 data rate
  - b. Telcordia PUB GR-499-CORE for T3 data rate
  - c. ITU-TSS G.702 and related recommendations for E1
  - d. ANSI T1.105 and 106 for SONET
  - e. USB 2.0 (USB Implementers' Forum)
  - f. IEEE 802.3, including 10 Base-T/TX/FX and 100 Base-TX/FX

5. The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards when offered commercially.

#### **C.2.12.5.1.3 Connectivity**

Satellite Access Service shall connect to and interoperate with:

1. Government specified permanent or temporary locations (e.g., SDPs, such as PBX, Multiplexer, Router, Video codec, earth station, and VSAT [e.g., 0.74, 0.98, and 1.2 to 4.5 meters; fixed and transportable/deployable])
2. Agency-designated network POP

#### **C.2.12.5.1.4 Technical Capabilities**

The following Satellite Access Service capabilities are mandatory unless marked optional:

1. Full-duplex, half-duplex, and simplex (i.e., one way) for point-to-point transmission (i.e., SDP to POP) for voice, data, and video traffic
2. Dedicated full time use of satellite link between SDP and POP or short time use between earth stations (teleport or VSAT) already connected to Government locations by advanced reservation by authorized users.
3. Reservation system shall allow:
  - a. Reservation can be placed up to a maximum of 45 days prior to service date
  - b. Reservation can be cancelled without charge no later than 5 days prior to service date
4. The contractor shall provide the access connection from the contractor's teleport or Government-premise (i.e., parking lot or roof top) based earth station to the SDP
5. The contractor shall define the contours of the SatAS coverage (i.e., footprint) maps and shall continue to provide any changes to satellite footprint for the frequency band(s) for each satellite providing the service.
6. Transparent to any protocol used by the GFP.
7. All bit sequences transmitted by the GFP through the SDP shall be treated with data transparency
8. The following categories of SatAS service shall be supported:
  - (a) **DS0**. This category of SatAS service shall support information payload data rates of 56 and 64 Kbps.



- (b) **Fractional T1.** This category of SatAS service shall support two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps.
- (c) **T1.** This category of SatAS service shall support a line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 service as follows:
  - (1) Channelized T1. In this mode, 24 separate DS0s clear channels of 56/64 Kbps shall be supported.
  - (2) Unchannelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
- (d) **E1 (For Non-domestic use).** This category of SatAS service shall support a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:
  - (1) Channelized E1. In this mode, 30 separate DS0 clear channels shall be supported.
  - (2) Unchannelized E1. In this mode, a single 1.92 Mbps information payload shall be supported.
- (e) **Fractional T3.** This category of SatAS service shall support two, three, or four adjacent DS1 clear-channels.
- (f) **T3.** This category of SatAS service shall support a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 service as follows:
  - (1) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
  - (2) Unchannelized T3. In this mode, a single 43.008 Mbps payload shall be supported
- (g) **SONET (Optional).** This category of SatAS shall support SONET data rates (e.g., SONET OC-3).
- (h) All other SatAS data rates, including those that are available or that become available during the life of the contract, are included in the scope of the contract.

#### C.2.12.5.2 Features

The following Satellite Access Service features in Section C.2.13.5.2.1 are mandatory unless marked optional:

### C.2.12.5.2.1 Satellite Access Service Features

ID Number	Name of Feature	Description
1	Low Bit Rate Voice (Optional)	The contractor shall support/provide 16 Kbps voice (Std: ITU-TSS G.728 LD-CELP voice encoding) to reduce satellite bandwidth
2	VSAT terminal (Optional)	The contractor shall provide VSAT terminals (e.g., 0.74, 0.98, and 1.2 to 4.5 meters)

### C.2.12.5.3 Interfaces

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.13.5.3.1, are mandatory unless marked optional:

#### C.2.12.5.3.1 Satellite Access Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 1.92 Mbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent
5	10 Base-T/TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 10 Mps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
6	100 Base-T/TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 100 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
7	T1 (Std: Telcordia SR-TSV-002275; ANSI T1.403)	Up to 1.536 Mbps	Transparent
8	T3 (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	Transparent
9 (Optional)	USB 2.0 (high speed) (Std: USB Implementers' Forum)	Up to 43 Mbps (Note maximum universal serial bus data rate is 480 Mbps)	Transparent
10	Air link interface (C-band, Ku-band, and Ka-band earth station)	Up to 43.008 Mbps	Transparent
11 (Optional)	SONET OC1-3 (Std: ANSI T1.105 and 106)	Up to 148.608 Mb/s	Transparent

Note: contractors are encouraged to support increased payload data rates of up to 6.6 Mbps for interface types of, RS-449/422, and V.35.

#### C.2.12.5.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Satellite Access Service (i.e., circuits) in Section C.2.13.5.4.1, are mandatory unless marked optional:

##### C.2.12.5.4.1 Satellite Access Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (severe weather conditions)	Routine	99.5%	$\geq 99.5\%$	See Note 1
Latency (one way)	Routine	400 ms	$\leq 400$ ms	See Note 2
Time to Restore	Without Dispatch	4 hours	$\leq 4$ hours	See Note 3
	With Dispatch	8 hours	$\leq 8$ hours	

Notes:

1. Availability
  - a. A service is considered unavailable
    - i. For SDP with Air link interface: when a SatAS user experiences no satellite transmission signal for more than 10 seconds due to severe weather conditions.
    - ii. For SDP with cable interface: when a SatAS circuit experiences a bit error rate (BER) of  $10 \text{ E-}7$ .
  - b. An unavailable satellite transmission is considered available when restoration activities have been completed and either (i) valid satellite signal has been received for air link interface, or (ii) there is no error-second for cable interface, for 30 consecutive minutes to account for stability and proving period. However, if there is no signal-degradation or error-second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time.
  - c. SatAS availability is calculated as a percentage of the total reporting interval time that SatAS is operationally available to the Agency. Availability is computed by the standard formula:
 
$$\text{Availability} = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
2. Latency (one way) is measured as satellite propagation delay between SDP and POP, excluding delays in the access circuits connecting to nearest earth stations (teleports or VSATs) and shall be measured via ping test.

3. Refer to Section C.3.3.1.2.4 for definition and how to measure.

## **C.2.13 Wireless Services**

### **C.2.13.1 Cellular/ Personal Communications Service (CPCS)**

Cellular/ Personal Communications Service (CPCS) provides Agency users with wireless services for their mobile terminals, such as cellular phones, notebook computers, and personal digital assistants (PDAs). This service can be used for applications, such as voice, data, short messaging services (SMS), multimedia messaging services (MMS), and Internet services.

#### **C.2.13.1.1 Service Description**

##### **C.2.13.1.1.1 Functional Definition**

Cellular/ Personal Communications Service is a wireless transmission service for mobile terminals. The contractor provides the wireless network.

The services and bandwidth provided depends on the characteristics of the mobile terminals and the technology used in the contractor's wireless network and service platforms, ranging from 2<sup>nd</sup> generation (2G) to 2.5G/3G wireless. The 2.5G/3G networks (and beyond) support IP packet-mode transmission.

Short Messaging Services (SMS), a feature of CPCS, provides the capability to send and receive text messages. The text can comprise of any alphanumeric characters; each short message may be up to 160 characters in length. Additionally, SMS supports interconnection with different message sources and public destinations including E-mail, paging, and instant messaging (IM).

Multimedia Messaging Service (MMS), a feature of CPCS, provides the capability to send and receive multimedia, such as pictures, streaming video, sound, and graphics.

##### **C.2.13.1.1.2 Standards**

Cellular/ Personal Communications Service shall comply with at least one of the following or equivalent 2.5G/3G Cellular Wireless standards:

1. 2.5G [based on General Packet Radio Service (GPRS) or Code Division Multiple Access (CDMA-2000 – 1xRTT)]
  - a. ETSI GSM-MAP or
  - b. TIA IS-41
2. 3G [based on CDMA] ITU-RTT IMT-2000
  - a. European ETSI/GSM Wideband CDMA (WCDMA) [also known as Universal Mobile Telecommunications System (UMTS)]

or

- b. US CDMA Development Group (CDG) CDMA-2000 Evolution Data Optimized (EV-DO)

CPCS shall comply with the following security standards or equivalent industry practices:

1. 3G Security: Security Threats and Requirements, 3GPP TS 21.133
2. 3G Security: Cryptographic Algorithm Requirements, 3GPP TS 33.105
3. 3G Security: Security Principles and Objectives, 3GPP TS 33.120
4. NIST FIPS Publication 140-2

CPCS shall comply with the following mobile data-related standards as applicable:

1. WAP Forum [Wireless Application Protocol (WAP 1.1 and 2.0) via WAP Gateway]
2. IP Mobility Support, IETF RFC 2002

SMS shall comply with the following standards as applicable:

1. ITU-T Q.700 – Q.774 Signaling System No. 7
2. ANSI T1.114 Signaling System Number 7 – Transaction Capabilities Application Part
3. 3GPP TS 03.40: “Digital cellular telecommunications system (Phase 2+) technical realization of the Short Message Service (SMS) Point-to-Point (PP)”
4. GSM 03.41: “Digital cellular telecommunication system (phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB).”
5. Mobile Applications Part (MAP)
  - a. GSM MAP 3.04, 9.4
  - b. ANSI-41 MAP Rev. B
6. Simple Message Transfer Protocol (SMTP)
7. Short Message Peer to Peer (SMPP)
8. Computer Access Protocol Number II (CAP II)
9. Telocator Alphanumeric Protocol (TAP)

MMS shall comply with the following standards as applicable:

1. Multimedia Messaging Service (MMS), 3GPP Technical Specification 23.140
2. Open Mobile Alliance

### 3. Wireless Application Protocol (WAP) Forum

The contractor shall comply with new versions, amendments, and modifications made to the above listed documents/standards, including beyond 3G, when offered commercially.

#### **C.2.13.1.1.3 Connectivity**

Cellular/ Personal Communications Service shall connect Agency mobile terminals (such as, but not limited to cellular phones, wireless-enabled Notebook and Laptop PCs, and PDAs) to the contractor's wireless network.

The contractor's wireless network shall interoperate with:

1. The Public Switched Telephony Network (PSTN) and the world wide dialing plan per ITU Recommendation E.164
2. Users of satellite-based services
3. The Internet
4. contractor's network providing Network-Based IP-VPN services (see Section C.2.7.3)
5. (Optional) contractor's network providing Premises-Based IP-VPN services (see Section C.2.7.2).

#### **C.2.13.1.1.4 Technical Capabilities**

The following Cellular/ Personal Communications Service capabilities are mandatory unless indicated otherwise:

1. CPCS shall have the capability to originate and receive voice calls from mobile phones, fixed wireline networks, and satellite-based networks.
2. CPCS shall allow the user to roam between compatible wireless (e.g., CDMA, GSM, etc.) networks
3. Packet-mode data transfer shall support a data rate in the range of 128 Kbps to 384 Kbps or higher while indoors or traveling at up to 65 miles per hour. This category of service shall provide "always on" connections. Offerings may include data optimized capabilities including EV-DO, High Speed Downlink Packet Access (HSDPA), or equivalent standards.
4. The contractor shall comply with Wireless Enhanced 911 (E911) Rules including Phases I and II as stipulated by the Federal Communications Commission. Refer to <http://www.fcc.gov/911/enhanced/>
5. Wireless Priority Service (WPS) shall allow authorized National Security and Emergency Preparedness (NS/EP) personnel to gain access to the next available wireless radio channel in order to initiate calls during an emergency when channels may be congested. WPS is invoked by dialing \*272 prior to the destination number on wireless terminals that have subscribed to WPS. Refer to

<http://wps.ncs.gov/>. Also refer to Section C.5 of the contract for NS/EP requirements.

6. The contractor shall provide wireless modem cards for mobile terminals if required by an Agency. The cards provided shall support the mobile terminals needed by the Agency, and shall include but not be limited to Type II PCMCIA and those required for PDAs.
7. If required by an Agency, the contractor shall provide and support commercially available mobile terminals with the characteristics and features needed.
8. If required by an Agency, the contractor shall provide commercially available mobile terminals that support device access control and data protection, including but not limited to:
  - a. Integrated authentication
  - b. Authorization
  - c. Virus scanning
  - d. Encryption capabilities (resident on terminal device)
9. (Optional) The contractor's wireless network performance (including but not limited to maximum latency and bit error rate [BER]) shall enable the use of National Security Agency-approved Type 1 encryption devices.

**C.2.13.1.2 Features**

The following CPCS features in the Section C.2.14.1.2.1 are mandatory unless indicated otherwise:

**C.2.13.1.2.1 Cellular/Personal Communications Service Features**

ID Number	Name of Feature	Description
1	Caller ID	Caller ID shall display the name and number (when available) of the person calling. It may also display the name of the person if stored <i>a priori</i> in the wireless terminal memory. Call can usually be returned by pressing one button.
2	Caller ID Blocking	Caller ID Blocking shall prevent the subscriber's wireless phone number from being transmitted. This shall be supported in two ways: a) Block on a per-call basis, or b) Block all calls (with the option to de-activate on a per-call basis).
3	Call Forwarding – Busy or No Answer Condition	This feature shall forward incoming calls to another phone number whenever the subscriber is busy or no answer occurs after a specified time. When forwarding calls to destinations outside of calling plan area (e.g. international numbers), additional charges may apply.
4	Call Forwarding - Unconditional	This feature shall automatically forward incoming calls to another phone number until deactivated. When forwarding calls to destinations outside of calling plan area (e.g. international numbers), additional charges may apply.

ID Number	Name of Feature	Description
5	Call Waiting	This feature shall alert the subscriber of another incoming call while currently engaged with an active call. The subscriber shall hear a short tone indicating that a call is waiting.
6	In-building Repeaters	The contractor shall provide in-building repeaters (or other solutions) as required by Agencies to improve wireless capacity and coverage in in-door facilities.
7	Information Services	<p>The contractor shall provide information services including – but not limited to:</p> <ol style="list-style-type: none"> <li>1. Weather reports (Optional)</li> <li>2. News summaries (Optional)</li> <li>3. Traffic advisory (Optional)</li> <li>4. Directory assistance (Optional)</li> <li>5. Web browsing</li> </ol>
8	Reserved	Reserved
9	International Wireless Voice Service Roaming (Optional)	The contractor shall support voice service roaming internationally between different service provider wireless networks to include GSM, and CDMA networks. The contractor shall specify the necessary mobile terminals needed.
10	International Wireless Data Service Roaming (Optional)	The contractor shall support data service roaming internationally between different service provider wireless networks to include GSM, and CDMA networks. The contractor shall specify the necessary mobile terminals needed.
11	Multimedia Messaging Service (MMS) (Optional)	<p>MMS shall provide mobile terminal-originated and mobile terminal-terminated point-to-point multimedia messaging:</p> <p>MMS shall support content types including – but not limited to:</p> <ol style="list-style-type: none"> <li>1. Text in Unicode format</li> <li>2. Speech in Adaptive Multirate format</li> <li>3. Pictures in Joint Photographic Experts Group (JPEG)</li> <li>4. Pictures in Graphics Interchange Format (GIF)</li> <li>5. Video Streaming in ITU Recommendation H.263 format</li> </ol> <p>The contractor shall propose, describe, and provide MMS of likely interest to Agencies.</p>
12	Short Messaging Services (SMS) – Basic Functionality	<p>SMS shall provide:</p> <ol style="list-style-type: none"> <li>1. Mobile terminal-originated and mobile terminal-terminated point-to-point short messaging</li> <li>2. Group Messaging to allow a subscriber to specify as many as 25 members comprising a SMS mailing list. Furthermore, a subscriber can specify up to 10 different Group Messaging lists.</li> <li>3. Support for broadcast services. [For example, an Agency may send broadcast messages to large, targeted audiences who subscribe to specific information, such as government economic data, and regulatory news.]</li> </ol> <p>SMS shall provide support the following capabilities relevant to the reception and submission of short messages:</p> <ol style="list-style-type: none"> <li>1. Message Expiration – Message delivery re-attempts and storage for unavailable recipients shall be</li> </ol>



ID Number	Name of Feature	Description
		supported. A message expiration time will govern how many re-attempts will be made. The expiration time shall be set on a per-
		<p>message or per-account basis.</p> <ol style="list-style-type: none"> <li>1. Priority – A priority scheme allowing urgent messages to be differentiated from normal messages shall be supported. Urgent messages shall take priority over normal messages, regardless of the arrival time at the SMS Center (SMSC).</li> <li>2. Message Escalation – The SMSC stores the message for a period no longer than the expiration time (it is assumed that the escalation time is smaller than the expiration time associated with the message), and after said escalation time expires, the message will be sent to an alternate message system such as a paging network or e-mail server.</li> <li>3. Message Acknowledgement/Delivery Confirmation</li> </ol> <p>SMS shall:</p> <ol style="list-style-type: none"> <li>1. Support an Interworking and Interoperability Function (IIF) to allow the sending/receiving of short messages between subscribers served by ANSI-41 (e.g., TDMA and CDMA) and GSM networks.</li> <li>2. Interwork with Internet E-mail (SMTP/MIME) to allow SMS subscribers to send and receive postings from any Internet mail address, e.g. subscriber@gsa.gov.</li> <li>3. Interwork with paging services to allow SMS subscribers to be accessible via existing paging interfaces.</li> </ol> <p>SMS shall support notification services. The contractor shall propose, describe, and provide notification services of likely interest to Agencies. [Examples of notification services include:</p> <ol style="list-style-type: none"> <li>1. E-mail notification, which indicates that e-mail messages are present in an e-mail mailbox.</li> <li>2. Reminder/calendar services, which enable reminders for meetings and scheduled appointments.</li> <li>3. Voice notification, which indicates that voice mail and/or facsimile messages are present in a voice mailbox.]</li> </ol>
13	SMS - Interworking with Instant Messaging (IM)	<p>The contractor shall provide interworking with Instant Messaging (IM). This capability entails using a current instant messaging screen name and sending instant messages with a 2-way text messaging device. This feature supports the portability of a "buddy list" permitting the subscriber to see who's online and then getting alerts when other colleagues or associates sign on.</p> <p>This feature is an add-on to SMS-Basic Functionality.</p>
14	Three-way Calling	Three-way Calling shall enable a subscriber to conduct a three-way conversation using the wireless terminal.
15	Voice-Activated Dialing (Network-hosted)	Voice-activated dialing shall initiate outgoing calls via voice commands.

ID Number	Name of Feature	Description
	(Optional)	Feature shall support: <ol style="list-style-type: none"> <li>1. Storage of up to 1000 contacts</li> </ol>
		<ol style="list-style-type: none"> <li>2. Addition and editing of contact via service provider Web site</li> <li>3. Importing contacts as needed from Agency applications such Microsoft Outlook Express or Lotus Notes</li> </ol>
16	Voice Mail	Voice mail features shall include – but not limited to: <ol style="list-style-type: none"> <li>1. Personal voice mail greeting – in the recorded words of the subscriber.</li> <li>2. Security features including an access code required to retrieve messages.</li> <li>3. Recorded messages can be up to three (3) minutes in length.</li> <li>4. New and not-yet-retrieved messages are stored for a minimum of 72 hours.</li> <li>5. Stores up to 20 saved messages for up to 14 calendar days.</li> <li>6. Toll-free access to voice mail system for subscribers.</li> <li>7. A notification is sent to wireless terminal as soon as a message is left in subscriber's mailbox.</li> </ol>
17	Walkie-talkie functionality (Optional)	Walkie-talkie functionality shall enable subscribers to connect directly with other users by pressing a button on their wireless terminal. The service shall indicate via an icon on their handset whether a user on their calling list is available  Business colleagues or work teams shall be able to set-up and manage group calling lists. This feature shall support groups of up to 10 participants. Users shall be able to create up to 50 group lists and store 100 individual contacts.

### C.2.13.1.3 Interfaces

The contractor shall support the following interfaces at the SDP, as defined in the Section C.2.14.1.3.1, for the provisioning of CPCS.

#### C.2.13.1.3.1 Cellular/Personal Communications Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
Specific to 2.5G and 3G			
1	Air Link for mobile phone: (Std: GSM and IS-136 TDMA)	Up to 116 Kbps	<ol style="list-style-type: none"> <li>1. Transparent</li> <li>2. IP v4</li> <li>3. IP v6 when offered commercially by the contractor</li> </ol>
2	Air Link: (Std: CDMA 1xRTT)	Up to 144 Kbps	<ol style="list-style-type: none"> <li>1. Transparent</li> <li>2. IP v4</li> <li>3. IP v6 when offered commercially by the contractor</li> </ol>
3	Air link: 1.8-2.5 GHz (Std: 3G WCDMA)	Up to 384 Kbps	<ol style="list-style-type: none"> <li>1. Transparent</li> <li>2. IP v4</li> </ol>

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
			3. IP v6 when offered commercially by the contractor
Specific to 2.5G and 3G			
4	Air Link: (Std: CDMA EVDO)	Up to 500 Kbps	1. Transparent 2. IP v4 3. IP v6 when offered commercially by the contractor
5	Air link: (Std: WCDMA-High Speed Downlink Packet Access (HSDPA) [Optional])	Up to 14.4 Mbps	1. Transparent 2. IP v4 3. IP v6 when offered commercially by the contractor

#### C.2.13.1.4 Performance Metrics

The Agencies recognize that the radio access network performance is likely to vary depending on location (e.g., urban, suburban, or rural), as well as the technical specifications and capabilities of the deployed infrastructure (such as the radio access equipment).

The contractor shall comply with the requisite geographic coverage for Cellular/Personal Communications Service as specified in Section J.2. The contractor shall provide the Key Performance Indicators (KPIs) which shall govern the service offered to Agencies. The KPIs shall include (but not be limited to) service availability.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (Voice Service)	Routine	99.5%	≥ 99.5%	See Note 1
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Notes:

- Voice Service availability is calculated as the average voice service availability for the contractor's network.
- See C.3.3.1.2.4 for the TTR definitions and measurement guidelines.

#### C.2.13.2 Cellular Digital Packet Data

Cellular Digital Packet Data (CDPD) provides wireless access to the Internet and other packet-switched networks over the AMPS and TDMA cellular network systems. CDPD was the first wireless packet data standard; it was specified in 1992 and initial commercial service was launched in 1995.

**C.2.13.2.1 Service Description****C.2.13.2.1.1 Functional Definition**

Cellular Digital Packet Data provides an “always on” wireless connection to the Internet. It is secure owing to support of encryption and channel hopping, which makes it difficult to intercept and interpret. CDPD packets also use forward error correction to reduce the effects of noise and radio frequency interference. CDPD service supports a data rate of 19.2Kps; however some of this capacity is used for error correction and other overhead.

**C.2.13.2.1.2 Standards**

Cellular Digital Packet Data services shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Cellular Digital Packet Data System Specification, Release 1.1 1995 CDPD Forum
2. IP Mobility Support, IETF RFC No. 2002
3. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards when offered commercially.

**C.2.13.2.1.3 Connectivity**

Cellular Digital Packet Data Systems shall connect and interoperate with:

1. Public Switched Telephone Network (PSTN)
2. Internet.

CDPD subscribers shall be accessible via E-mail and the telephone.

**C.2.13.2.1.4 Technical Capabilities**

The following Cellular Digital Packet Data capabilities are mandatory:

1. Radio Channel Data Rate at 19.2Kps
2. Full duplex radio link
3. Connectionless, “always on” access
4. Security including:
  - a. User authentication
  - b. Air-link encryption using RSA 128-bit RC4 Symmetric Stream Cipher
5. Host connectivity including:
  - a. Internet Protocol

b. Direct 56Kps access

6. The contractor shall provide CDPD-compliant modems to meet Agency needs. The modems shall include Type II PCMCIA, such as for laptop computers, and also those compatible with Personal Digital Assistants (PDAs) (See Section B.4).

**C.2.13.2.2 Features**

The following Cellular Digital Packet Data features in Section C.2.14.2.2.1 below are mandatory unless indicated otherwise:

**C.2.13.2.2.1 CDPD Features**

ID Number	Name of Feature	Description
1	Mobile Office (Optional)	In addition to digital wireless access via CDPD, the Mobile Office shall support voice telephony. This feature shall allow a subscriber to transform a laptop, PDA, or data-capable digital phone into a mobile office, supporting both voice and data communications from a single device.

**C.2.13.2.3 Interfaces**

The principal interface for CDPD is a laptop computer or PDA equipped with a CDPD modem. Other interfaces include point-of-sales terminal or telemetry sensors.

**C.2.13.2.4 Performance Metrics**

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Cellular Digital Packet Data are defined in Section C.2.14.2.4.1.

**C.2.13.2.4.1 Performance Metrics for Cellular Digital Packet Data**

Key Performance Indicator (KPI)	Service Type	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 1
	With Dispatch	8 hours	≤ 8 hours	

Notes

1. See C.3.3.1.2.4 for the TTR definitions and measurement guidelines.

**C.2.13.3 Multimode/Wireless LAN Service (MWLANS)**

Multimode/Wireless LAN Service (MWLANS) enables Agency users to securely access Agency networks from outside the Agency firewall. Such Agency users are increasingly accessing the Internet and Government intranets via Wireless Fidelity (Wi-Fi) hotspots rather than traditional dial-up connections.

### **C.2.13.3.1 Service Description**

#### **C.2.13.3.1.1 Functional Definition**

Multimode/Wireless LAN Service provides Agency users with wireless access points, i.e., Wi-Fi hotspots with connections to the Internet and/or to the contractor's IP network. These wireless access points are at locations such as hotels, airports, convention/conference centers, or other public establishments. In addition, Agencies may need contractor-provided wireless access points dedicated for Agency use at various Agency locations.

MWLANS is a wireless transmission service for mobile terminals. Agency personnel using Wi-Fi-enabled notebook computers or personal digital assistants (PDAs), when they are located within the Wi-Fi coverage areas or hotspots of the service, can access E-mail, government intranets, and the Internet.

MWLANS supports IP packet-mode transmission.

#### **C.2.13.3.1.2 Standards**

Multimode/Wireless LAN Service shall comply with the following standards as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. IEEE 802.11b (Wi-Fi at 2.4 GHz with data rates of up to 11 Mbps)
2. IEEE 802.11g (Wi-Fi at 2.4 GHz with data rates of up to 54 Mbps)
3. IEEE 802.11a (Wi-Fi at 5 GHz with data rates of up to 54 Mbps) –Applicable only to dedicated Agency “hot spots.”
4. IEEE 802.1x Extensible Authentication Protocol (EAP) for authentication.
5. IEEE 802.11i with Advanced Encryption Standard (AES) for encryption between the mobile terminal and the access point, when available
6. IEEE 802.11e Media Access Control Enhancements for Quality of Service (QoS), when available

The contractor shall comply with new versions, amendments, and modifications made to the above listed documents/standards, when offered commercially.

#### **C.2.13.3.1.3 Connectivity**

Multimode/Wireless LAN Service shall interoperate with:

- Agency mobile terminals (that include but are not limited to wireless-enabled Notebook and Laptop PCs, and PDAs) to the wireless access points.
- The contractor's wireless access points to the Internet and to the contractor's networks providing IP-VPN services (see Sections C.2.7.2 and C.2.7.3).

The SDP shall be at the mobile terminal.

**C.2.13.3.1.4 Technical Capabilities**

The following Multimode/Wireless LAN Service capabilities are mandatory unless indicated otherwise:

- Wireless access in packet-mode to mobile terminals shall be supported. Mobile terminals shall include but not be limited to wireless-enabled Notebooks, Laptops and PDAs. Access coverage shall include wireless LAN “hot spots” such as hotels, airports, convention/conference centers, or other public establishments.
- Access shall only be provided after authentication by user-id and password by the contractor. The user shall be able to change password as often as deemed necessary.
- The contractor shall support dynamic IP address as well as single or multiple static IP address(es).- Applicable only to dedicated Agency “hot spots.”
- The contractor shall provide a public Domain Name Service (DNS) for users to access the Internet.
- The contractor shall have established roaming agreements with public hotspot providers and aggregators so that users can roam globally.
- The contractor shall provide private hotspots (i.e. dedicated network infrastructure) at government locations as required by an Agency.
- The contractor shall provide commercially available Wireless Network Interfaces Cards (NICs) for mobile terminals as required by an Agency.
- Support for IEEE 802.11e for Agency applications such as, but not limited to transport of voice, audio and video over 802.11 wireless networks, video conferencing, media stream distribution, enhanced security applications, and mobile and nomadic access applications. [Optional]

**C.2.13.3.2 Features**

None.

**C.2.13.3.3 Interfaces**

The User-to-Network Interfaces (UNIs) at the SDP, as defined in the Section C.2.14.3.3.1 are mandatory.

### C.2.13.3.3.1 Multimode/Wireless LAN Service User-to-Network Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	Air link: 2.4 GHz (Physical interface is Type II PCMCIA card of handheld computers and card/chip in PDA)	Up to 11 Mbps for IEEE 802.11b	1. IP v4 2. IP v6 when offered commercially by the contractor
2	Air link: 2.4 GHz (Physical interface is Type II PCMCIA card of handheld computers and card/chip in PDA)	Up to 54 Mbps for IEEE 802.11g	1. IP v4 2. IP v6 when offered commercially by the contractor
3	Air link: 5 GHz (Physical interface is Type II PCMCIA card of handheld computers and card/chip in PDA)	Up to 54 Mbps for IEEE 802.11a	1. IP v4 2. IP v6 when offered commercially by the contractor

### C.2.13.3.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Multimode/Wireless LAN Service in Section C.2.14.3.4.1 are mandatory for contractor-provided wireless access points dedicated for Agency use.

#### C.2.13.3.4.1 Multimode/Wireless LAN Service Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Level/threshold)	Acceptable Quality Level (AQL)	How Measured
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 1
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. See C.3.3.1.2.4 for the TTR definitions and measurement guidelines.

### C.2.13.4 Reserved

### C.2.13.5 Paging Service (PagS)

Paging service traditionally consists of one-way data communications sent to a mobile device that alerts the user when it arrives. The communication could consist of a phone number for the user to call, a short message, or an information update. Recently, more advanced two-way paging services have been introduced.



### C.2.13.5.1 Service Description

#### C.2.13.5.1.1 Functional Definition

Paging is a radiotelephony service provided by firms authorized by the FCC. Commercial paging services operate in the 35-36, 43-44, and 152-159, and 454-460 MHz bands (referred to as the “Lower Band”) and 929 and 931 MHz bands (referred to as “Upper Band”). Paging systems use store-and-forward technology, accepting messages for delivery to paging devices, and storing them for a brief period prior to delivery. The primary elements of a paging system are:

1. Input source – the telephone, personal computer, personal digital assistants (PDAs such as BlackBerry, Palm Pilot, etc.), desktop entry device, or an operator dispatch
2. Public Switched Telephone Network – pages are sent over the local/national/international phone systems (PSTN)
3. Paging Terminals and Transmitter Equipment – or radio frequency (RF) link systems – typically provided by paging service Contractor
4. Pager Unit – small radio receiver carried by the subscriber

#### C.2.13.5.1.2 Standards

Paging services shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Protocols between the Paging Infrastructure and Subscriber Devices
  - a. Advanced Paging Operators Code (APOC)
  - b. Post Office Standardization Advisory Group (POSAG)
  - c. Radio Access Mail Protocol (RAMP) – and upgrade to APOC offering direct two-way access to the Internet.
  - d. Mobitex
  - e. One or more of the following FLEX<sup>6</sup> Protocols
    - i. FLEX: 16-64Kps one-way paging protocol
    - ii. ReFLEX: enables throughput of 44-192Kps with acknowledgement paging and interactive messaging
    - iii. InFLEXion Voice – supports digital voice compression
    - iv. InFLEXion Data – intended for high-speed data applications supporting speeds of 28 – 112Kps
2. Protocols between the Paging Infrastructure and other Networks

---

<sup>6</sup>.These are licensed protocols that have become the *de facto* standards in the USA

- a. Telocator Network Paging Protocol (TNPP)
- b. Telocator Alphanumeric Protocol (TAP)

The rules governing commercial paging in the USA are found in Code of Federal Regulations, Volume 47, Part 1 and Part 22 (and Part 90 for 929 MHz channels).

#### **C.2.13.5.1.3 Connectivity**

Paging Systems support interoperability and interworking with the a) Public Switched Telephone Network and b) Internet; paging subscribers are accessible via E-mail and the telephone.

#### **C.2.13.5.1.4 Technical Capabilities**

The following Paging capabilities are mandatory unless indicated otherwise:

1. Two basic paging services shall be offered: one-way and two-way.

##### **C.2.13.5.1.4.1 One-Way Paging**

The requisite technical capabilities for one-way paging shall include:

1. Display text messages up to 240 characters in length.
2. Receive numeric messages originating from the PSTN via dual tone multi-frequency.
3. Support the assignment of an e-mail address, e.g. [customer@paging-service.com](mailto:customer@paging-service.com), to a paging device.
4. Receive messages sent from Internet e-mail.
5. Message recall via telephone and Internet – allows retrieval of messages when subscriber does not have paging device or is outside coverage area.
6. Personal phone greetings for telephone number assigned to the pager unit.
7. Messaging software for Windows and Macintosh environments allowing the sending of pages from personal computers; software shall be distributed via Internet downloading with a browser.
8. The Contractor shall provide one-way pager devices compatible with the paging service and features offered.

##### **C.2.13.5.1.4.2 Two-way Paging**

The requisite technical capabilities for two-way paging shall include:

1. Display text messages up to 240 characters in length.
2. Receive numeric messages originating from the PSTN via dual tone multi-frequency.

3. Guaranteed Message Delivery – when out of range (e.g. on an airplane) or when unit is turned off, the paging system shall store incoming messages for no less than 48 hours, automatically delivering them when unit returns to service.
4. Originate and send messages from pager unit.
5. Reply to messages from pager unit including preprogrammed replies such “Yes”, “No”, and “Thank You.”
6. Receive messages sent from Internet e-mail.
7. Support the assignment of an e-mail address, e.g. [customer@paging-service.com](mailto:customer@paging-service.com), to a paging device.
8. Originate and reply to e-mail using pager.
9. Receive news updates from leading information sources.
10. Message recall via telephone and Internet – allows retrieval of messages when subscriber does not have paging device or is outside coverage area.
11. Text-to-Speech Messaging – i.e., entering a text message on a paging device for speech synthesis and transmittal via the PSTN. In this manner, one can send a message to any telephone number using only the pager.
12. Personal phone greetings for telephone number assigned to the pager unit.
13. Messaging software for Windows and Macintosh environments allowing the sending of pages from personal computers; software shall be distributed via Internet downloading with a browser.
14. The contractor shall provide two-way pager devices compatible with the paging service and features offered.

**C.2.13.5.2 Features**

The following Paging features in Section C.2.14.5.2.1 below are mandatory unless indicated otherwise:

**C.2.13.5.2.1 Paging Features**

ID Number	Name of Feature	Description
1	Caller ID	The contractor shall provide Caller ID. When receiving a numeric page or a voice-message notification, the recipient shall be presented with the caller identification on the pager.
2	Group and Broadcast Messaging	<p>The contractor shall provide Group and Broadcast Messaging. This feature shall allow the sending of a single message to 500 (or greater) recipients quickly and easily. Set up and managed through a web interface, the distribution list can contain any combination of:</p> <ul style="list-style-type: none"> <li>• One-Way and Two-Way PINs</li> <li>• Email addresses</li> </ul>

ID Number	Name of Feature	Description
		<ul style="list-style-type: none"> <li>• Cell SMS addresses</li> <li>• U.S. Telephone Numbers</li> </ul> <p>Restrict access to the Group and Broadcast Messaging by specifying the PINs that can send messages, and the times when messages will be accepted.</p>
3	Information Services	<p>The contractor shall provide Information Services. This feature shall allow subscription and receipt of periodic updates from major information services including:</p> <ul style="list-style-type: none"> <li>• Weather</li> <li>• News Summaries</li> <li>• Finance</li> <li>• Technology</li> </ul>
4	Interoperability with Short Messaging Service (SMS)	<p>The contractor shall provide Interoperability with SMS. Send, receive, and reply to messages to and from SMS-enabled cell phones shall be supported.</p>
5	Operator Dispatch	<p>Operator Dispatch lets callers send complete text messages to subscriber alphanumeric paging device, even if they don't have PC, Internet or email access. Callers dictate their message to an operator who immediately transmits the message to paging unit.</p>
6	Read Acknowledgement	<p>Read Acknowledgement shall allow the sender to know whether a message was actually read or not. (This is <i>in addition</i> to message delivery acknowledgement.)</p>
7	Toll-free Personal Access Number	<p>Toll-free access permits others to send messages without charge to paging subscribers via the PSTN.</p>
8	Voice Mail	<p>Voice mail features shall include – but not limited to:</p> <ul style="list-style-type: none"> <li>• Personal voice mail greeting – in the words of the subscriber.</li> <li>• Security features including an access code required to retrieve messages.</li> <li>• Recorded messages can be up to three (3) minutes in length.</li> <li>• New and not-yet-retrieved messages are stored for a minimum of 72 hours.</li> <li>• Stores up to 20 saved messages for up to 14 days.</li> <li>• Toll-free access to voice mail system for subscribers.</li> <li>• A notification is sent to pager unit as soon as a message is left in subscriber's mailbox.</li> </ul>

### C.2.13.5.3 Interfaces

The principal user interface shall be the pager – a small radio receiver designed to be carried by the subscriber and activated by the reception of a radio signal containing its

specific code. There are several ways a pager can receive a message including: tone only – the pager alerts only; numeric – the pager alerts the subscriber of an incoming message and a phone number appears on the pager (requires a touch tone phone); alphanumeric – text and numbers appear on the pager either in real time or retrieved from memory like an answering message; and voice – the message is heard audibly from the pager. The subscriber can often select the method of alerting, whether it is via visual stimuli (a message indicator or LED flashes), audible stimuli, or a more discrete stimuli such as vibrate mode.

**C.2.13.5.4 Performance Metrics**

The Performance Levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Paging are defined in Section C.2.14.5.4.1

**C.2.13.5.4.1 Performance Metrics for Paging**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 1
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. See C.3.3.1.2.4 for the TTR definitions and measurement guidelines.

**C.2.13.6 Land Mobile Radio Service (LMRS)**

LMRS connects Agency locations and mobile equipment (e.g., commercially available mobile and portable two-way half-duplex radio systems) with wireless Radio Frequency (RF) access to public and private network resources or to other LMRS users. An LMRS system typically consists of a combination of a command/control/dispatch center, remote fixed Radio Frequency (RF) facilities, mobile and portable radios, and the system infrastructure to operate the network and interface to external communications systems. Since all LMRS communication is via RF, the Service Delivery Points (SDP) consist of a combination of portable handheld radios, mobile vehicular mounted radios, and/or fixed base station radios or consoles.

**C.2.13.6.1 Service Description**

**C.2.13.6.1.1 Functional Definition**

The LMRS is a two-way wireless transmission service using the contractor’s wireless network to communicate between mobile terminals using half duplex radio frequency transmissions.

LMRS is an SDP to SDP connecting service, i.e., it connects the SDP (i.e., Agency location or the mobile terminal) to another SDP on the LMRS system. The connected

SDPs form a local RF network to meet Agency requirements. In addition, an Agency may use end-to-end encrypted communications over the contractor's wireless network.

An optional feature of LMRS provides SDP to Point of Presence (POP) connection, i.e., it connects the SDP to the POP of the contractor's network. For this feature, the contractor provides: (a) wireless RF coverage for local access to the LMRS as needed by an Agency, and (b) connectivity to other voice and data Network services (i.e., Voice Services, Internet Protocol Service, and Network-Based IP VPN Service).

#### **C.2.13.6.1.2 Standards**

Land Mobile Radio Service shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions or standards listed below.

1. Compatible with ANSI/TIA/EIA 102 Series APCO Project 25 (P25) Common Air Interface:
  - a. Digital Conventional
  - b. Digital Trunked
2. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management.
3. NTIA Narrowband (12.5 KHz channel spacing) Operation Directive for operations below 512MHz.
4. The contractor shall meet the NTIA Narrowbanding Mandate for operation. [Note. NTIA requires that all Federal users move to more efficient 12.5 KHz equipment for mobile communications by 2005 or 2008, depending on the frequency bands in which they operate. After Jan 1, 2005, all Federal systems in the 162- 174 MHz band must be capable of operating within a 12.5 kHz channel. In addition, after Jan 1, 2008, all Federal systems in the 138-162 MHz and 406-420 MHz band must be capable of operating within a 12.5 kHz channel.]
5. TIA TSB88-A and TIA TSB88-A-1 Wireless Communications Systems- Performance in Noise and Interference Limited Situations
6. Numbering and Addressing Plan (Optional)
  - a. Voice:
    - i. North American Numbering Plan (NANP)
    - ii. ITU-TSS ISDN E.164
  - b. Data:
    - i. IPv4/v6
      1. IPv4 Specification

2. IPv6 Specification (IETF RFC 2460)
3. IP 6 Addressing Architecture (IETF RFC 2373)
7. All new versions, amendments, and modifications to the above documents and standards when offered commercially.

#### **C.2.13.6.1.3 Connectivity**

Land Mobile Radio Service shall connect the following:

1. Agency's two-way mobile terminals (e.g., P25 compatible portable and mobile radios or data terminals) to each other through a digital RF system.
2. Agency specified locations (i.e., SDPs, such as Command and Dispatch Centers) to each other and with the two-way mobile terminals through a digital RF system.

#### **C.2.13.6.1.4 Technical Capabilities**

The following Land Mobile Radio Service capabilities are mandatory unless marked optional:

##### **C.2.13.6.1.4.1 Design and Engineering Services**

1. The contractor shall determine the Agency's functional and performance requirements for Land Mobile Radio (LMR) systems and equipment. This task includes determination of the Concept of Operational for LMR within the Agency's telecommunications operations. The requirements also may include the identification of necessary interfaces between the Agency's wireline and wireless systems and LMR.
2. The contractor shall conduct site surveys.
3. The contractor shall develop a detailed system design. The system design shall address network topology, configuration, addressing (fleet mapping), bandwidth and frequency requirements, RF coverage, availability, reliability, scalability, security, SEDs, and disaster recovery requirements.
4. The contractor shall assist Agencies in obtaining the radio frequency spectrum authorizations needed to implement the LMRS network. Radio frequency spectrum authorizations must be secured by the Agency from either the National Telecommunications and Information Administration (NTIA) or the Federal Communications Commission (FCC).

##### **C.2.13.6.1.4.2 Implementation**

1. The contractor shall manage the SEDs required for the installation and operation of the LMRS. The contractor shall ensure that SEDs are transported to appropriate site of deployment and/or stored until installation is completed.

2. The contractor shall perform testing of the delivered LMR system to verify system performance. Tests shall verify the connectivity between the dispatch and control center and mobile assets, and verify connectivity with other wireless/wireline services as required.
3. At a minimum, the contractor shall support the following Land Mobile Radio Service capabilities:
  - a. Push to Talk. Half-Duplex (walkie-talkie) communications operation.
  - b. Conferencing/Talk Groups. Definition and subscription of users to 'channels' or talk groups serving specific missions or groups of users.
  - c. Broadcast. Ability to send and receive broadcast transmissions.
  - d. Fixed Frequency Operation. Capability to connect mobile terminal users to the network or each other using fixed RF frequencies as needed.
  - e. Trunking. Ability to share multiple frequencies or frequency pairs between the subscribing mobile terminal users on an as required basis.
  - f. P25 compatibility/interoperability. Compatibility and interoperability with systems meeting EIA/TIA 102 Standards.
  - g. Data Transmission. Ability to send and receive text, graphics, and video transmissions.
  - h. The contractor shall support the following categories of Land Mobile Radio Service:
    - a. **Analog.** This category of service shall offer limited capability access to existing legacy analog systems using dedicated fixed frequencies for each communications channel.
    - b. **Digital.** This category of service shall provide digital wireless access using a non-P25 system using either dedicated fixed frequencies or trunked access using a control methodology to manage on-demand sharing of multiple frequencies among multiple users.
    - c. **P25.** This category of service shall provide P25 compatible digital non-trunked access using dedicated fixed frequencies for each communications channel, or trunked access using a control methodology to manage on-demand sharing of multiple frequencies among multiple users.

#### **C.2.13.6.1.4.3 Management**

The contractor shall provide overall management of an Agency's LMRS network to include operational support on a per node basis. This may include managing services delivered to the Agency by other contractors. For LMRS, nodes include command centers and fixed RF sites.



**C.2.13.6.2 Features**

The following Land Mobile Radio Service features in the Section C.2.14.6.2.1 are mandatory unless marked optional:

**C.2.14.6.2.1. Mobile Radio Service Features**

ID Number	Name of Feature	Description
1	OTAR	The contractor shall support Over- the-Air-Rekeying encryption capabilities.
2	System Specifications Document	The contractor shall provide data collection and analysis resulting in a System Specifications Document. The document may include concepts of operation, functional and performance requirements and interface definition as needed by the Agency.
3	Site Survey Report	The contractor shall provide a site survey report delivered after the completion of physical site visits to potential operational locations to collect and validate floor plans, physical measurements, building power capacity, and external ingress/egress factors.
4	System Design Document	The contractor shall provide a detailed system design specific to Agency requirements.
5	System Frequency Authorizations	The contractor shall provide assistance to the Agency in the acquisition of frequency use authorization.
6	Test Documentation	The contractor shall provide test plans and procedures for functional verification, performance validation, security test and evaluation.
7	Training	The contractor shall provide training classes and documentation for users and system maintainers.
8	Dialing Capability (Optional)	The contractor shall provide the ability to originate and terminate dialable voice and data (IP) connections.
9	Extended Connectivity (Optional)	The contractor shall enable an Agency's two-way mobile terminals to connect to a Network POP so that users can access Network services, such as, but not limited to, Voice Services, Internet Protocol Service, and Network-Based IP VPN Service. The contractor shall provide connectivity to the PSTN, Internet, and private network resources as needed by the Agency. The contractor shall enable the Agency command/control/dispatch center(s) to control the extended connectivity provided to individual users.

**C.2.13.6.3 Interfaces**

The following interfaces for Land Mobile Radio Service in Section C.2.14.6.3.1 below shall be supported:

**C.2.13.6.3.1 Land Mobile Radio Service Interfaces**

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	Narrowband compatibility	12.5 KHz channels maximum bandwidth	Operation below 512 MHz
2	Interoperability	Defined by P25 Common Air Interface	P25 Common Air Interface
3	Voice to Data coding	P25 A/D	Improved Multi-Band

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
	standard	conversion/coding standard	Excitation (IMBE) vocoder [Std: P25]
4	Encryption	Note 1	Note 1

Notes:

1. The Payload Data Rate and Protocol Type are highly dependent upon the Agency's requirement. Exact Payload Data Rate and Protocol Types will be defined and agreed upon as part of each service delivery order.

#### C.2.13.6.4 Performance Metrics

The performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Land Mobile Radio Service in Section C.2.14.6.4.1 are mandatory unless marked optional.

##### C.2.13.6.4.1 Performance Metrics for LMRS

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(LMRS)	Routine	99.5%	≥ 99.5%	See Note 1
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that LMRS is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(LMRS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section C.3.3.1.2.4 for the definitions and measurement guidelines.

#### C.2.14 Reserved

#### C.2.15 Access Arrangements [As Applicable]

Access Arrangements provide the convention to specify and price the originating and/or terminating access component required to connect the SDP to the contractor's POP when that access component is required to deliver a Telecommunications Service. The contractor shall provide the following types of access arrangements:

1. Circuit-Switched Access Arrangements
2. Dedicated Access Arrangements

These access arrangement types are described in following subsections

C.2.15.1 Circuit-Switched Access Arrangement

The contractor shall provide circuit-switched access arrangements from the serving local central office for SDPs with Presubscribed Interexchange Carriers (PICs) service for VS, CSDS, TFS, and CS.

C.2.15.2 Dedicated Access Arrangements

The contractor shall provide the following types of dedicated access arrangements:

1. Wireline Access Arrangement (WLNAA)
2. Broadband Access Arrangement (BBAA)
3. Wireless Access Arrangement (WLSAA) (Optional)
4. Satellite Access Arrangement (SatAA) (Optional)

A user shall be able to select a dedicated access arrangement for a particular telecommunications service type (e.g., VS, ATMS, L2VPNS) from the above access arrangement types as specified in Table C.2.16.2-1 and Attachment J.2.

**Table C.2.14.6.4-1 Minimum Dedicated Access Arrangements  
[Services and Access Arrangements – As Applicable]**

	Access from SDP to contractor's POP																		
	PLS	VS	CSDS	TFS	FRS	IPS	NBIP-VPNS	PBIP-VPNS	CIPS	ATMS	EthS	L2-VPNS	SONETS	OVS	DFS	CDNS	IP-TelS	IP-VTS	
WLNAA	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
BBAA																			
DSL					[x]	x	x	x	x		x	x					x	x	x
Ethernet Access						x	x	x	x		x	x					x	x	x
FTTP		x				x	x	x	x		x	x					x	x	x
Cable High-speed Service																			
WLSAA						x	x	x	x		x	x					x	x	x
Broadband Wireless	x	x	x	x	x	x	x	x	x	x	x	x					x	x	x
SatAA	x	x	x	x	x	x	x	x	x	x							x	x	x

Legend:

x: Denotes a valid access arrangement	
[x] Denotes an access arrangement that is (Optional)	
PLS: Private Line Service	OWS: Optical Wavelength Service
CSDS: Circuit-Switched Data Service	FTTP: Fiber-to-the-premises
FRS: Frame Relay Service	L2VPNS: Layer 2 VPN Service
ATMS: ATM Service	SONETS: SONET Service
VS: Voice Services	CDNS: Content Delivery Network Service
CIPS: Converged IP Services	IPTelS: IP Telephony Service
TFS: Toll Free Service	IPVTS: IP Video Transport Service
IPS: Internet Protocol Service	WLNAA: Wireline Access Arrangement
NBIP-VPNS: Network based IP VPN service	BBAA: Broadband Access Arrangement
PBIP-VPNS: Premise based IP VPN service	WLSAA: Wireless Access Arrangement
EthS: Ethernet Services	SatAA: Satellite Access Arrangement
DSL: Digital Subscriber Line	DFS: Dark Fiber Service

## Note:

1. Combined Services (CS) will utilize the same access arrangement as for VS, TFS, and IPS.

**C.2.15.2.1 Wireline Access Arrangement (WLNAA)**

Wireline Access Arrangement connects an Agency location with dedicated, reliable bandwidth to contractor's network. The range of line speeds and reliability options provided within this access arrangement category allow Agency users to satisfy their diverse needs for accessing contractor's networks. The following sections provide the requirements for WLNAA.

**C.2.15.2.1.1 Basic Access Arrangement Description****C.2.15.2.1.1.1 Functional Definition**

Wireline Access Arrangement includes dedicated transmission access arrangement between Agency location and contractor's network (i.e., transport network). WLNAA is an SDP to POP connecting access arrangement, i.e., it connects the SDP at the Agency location to the POP of the contractor's network. This access arrangement can be used for any application, such as voice, data, video, and multimedia.

**C.2.15.2.1.1.2 Standards**

Wireline Access Arrangement shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. ANSI T1.102/107/403/503/510 for T1
2. ANSI T1.607/610 for ISDN PRI
3. Telcordia PUB GR-499-CORE for T3
4. ANSI T1.105 and 106 for SONET
5. Telcordia PUB GR-253-CORE for SONET
6. ITU-TSS G.702 and related recommendations for E1 and E3
7. Frequencies grid and physical layer parameters for Optical Wavelength

- a. DWDM: ITU G.692 and G.694 as mandatory and G.709 and G.872 as optional
- b. WDM: ITUG.694.2 and Telcordia GR 253
- 8. Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009
- 9. EIA/TIA-559, Single Mode Fiber Optic System Transmission Design
- 10. Telcordia GR-20-CORE for Generic Requirements for Optical Fiber and Optical Fiber Cable GR-253 (SONET), and GR-326 (Connector)
- 11. The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards when offered commercially.

**C.2.15.2.1.1.3 Connectivity**

Wireline Access Arrangement shall connect to and interoperate with:

- 1. Agency specified locations (i.e., SDPs, such as PBX, Centrex, Multiplexer, Router, Video codec, and Group 4 FAX)
- 2. POPs of the contractor's network

**C.2.15.2.1.1.4 Technical Capabilities**

The following Wireline Access Arrangement capabilities are mandatory unless marked optional:

- 1. Integrated access of different services (e.g., VS, IPS, and CS)
  - a. Over pre-allocated channels for channelized transmission service (e.g., Channelized T1)
  - b. Over the same channel (e.g., Unchannelized T3, SONET OC-3c) of IP packets for Converged IP Services
  - c. Over the same access circuits for both VS and TFS.
- 2. Transparent to any protocol used by the Government Furnished Property (GFP).
- 3. Transparent to all bit sequences transmitted by the GFP
- 4. Network-derived clocking.

The following categories of WLNAA access arrangement shall be supported:

- a. **T1**. This category of WLNAA access arrangement shall support a line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 access arrangement as follows:
  - (1) Channelized T1. In this mode, 24 separate DS0s clear channels of 56/64 kb/s shall be supported.

- (2) Unchannelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
- b. **Fractional T1**. This category of WLNAAs shall support two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps.
- c. **ISDN PRI**. This category of WLNAAs shall support 23 separate DS0 clear channels of 56/64 kbps over an interface of ISDN PRI (23B+D) with a line rate of 1.544 Mbps. (Optional)
- d. **T3**. This category of WLNAAs shall support a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 access arrangement as follows:
  - (1) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
  - (2) Unchannelized T3. In this mode, a single 43.008 Mbps payload shall be supported.
- e. **Fractional T3**. This category of WLNAAs shall support three, four, five, or seven adjacent DS1 clear-channels.
- f. **E1 (Non-domestic)**. This category of WLNAAs shall support a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:
  - (1) Channelized E1. In this mode, 30 separate DS0 clear channels shall be supported.
  - (2) Unchannelized E1. In this mode, a single 1.92 Mbps information payload shall be supported.
- g. **E3 (Non-domestic)**. This category of WLNAAs shall support a line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:
  - (1) Channelized E3. In this mode, 16 separate E1 channels shall be supported.
  - (2) Unchannelized E3. In this mode, a single 30.72 Mbps information payload shall be supported.

- h. **SONET OC-3.** (Optional) This category of WLNA shall support a line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c access arrangement as follows:
- (1) Channelized OC-3. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, shall be supported.
  - (2) Concatenated OC-3c. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps shall be supported.
- i. **SONET OC-12** (Optional). This category of WLNA shall support a line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c access arrangement as follows.
- (1) Channelized OC-12. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, shall be supported.
  - (2) Concatenated OC-12c. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps shall be supported.
- j. **SONET OC-48** (Optional). This category of WLNA shall support a line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c service as follows:
- (1) Channelized OC-48. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, shall be supported.
  - (2) Concatenated OC-48c. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps shall be supported.
- k. **SONET OC-192** (Optional). This category of WLNA shall support a line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c service as follows:
- (1) Channelized OC-192. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, shall be supported.
  - (2) Concatenated OC-192c. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps shall be supported.
- (l) **Dial Access Line.** (Optional) This category of WLNA shall support 2 wire analog lines and trunks without access integration for voice service (VS).
- (m) **DS0.** This category of WLNAS shall support information payload data rates of 56 Kbps and 64 Kbps.
- (n) **Subrate DS0 (optional).** This category of WLNA shall support subrate DSO at information payload data rates of 4.8, 9.6, and 19.2 Kbps.

- (o) **Optical Wavelength (Optional).** Bi-directional wavelengths (WDM and ASTN) connections to an optical network for the following speeds:
  1. OC-48
  2. OC-192
  3. OC-768 (Optional)
  
- (p) **Dark Fiber (Optional):** Dark Fiber shall support the following capabilities:
  1. Deployed fiber shall support both single-mode and multimode fibers
  2. Deployed fibers shall be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1
  3. Deployed fibers shall be capable of operating in the "C", and "L" bands. Support for the "S" band will also be required when commercially available.

All other WLNA data rates, including those that are available or that become available commercially from the contractor during the life of the contract [Optional].

**C.2.15.2.1.2 Features**

The following Wireline Access Arrangement features in Section C.2.16.2.1.2.1 are mandatory:

**C.2.15.2.1.2.1 Wireline Access Arrangement Features**

ID Number	Name of Feature	Description
1	Access Route or Path Diversity	<p>The contractor shall supply at least two physically-separated routes for access diversity with the following options:</p> <ol style="list-style-type: none"> <li>1. Between an SDP and its associated connecting network's POP, or</li> <li>2. Between an SDP and at least two connecting network POPs.</li> <li>3. Access from the same or different access providers (e.g., ILEC and a CLEC) for two separate routes, using any mix of access arrangements, such as wireless access (e.g., Broadband Wireless) and satellite access.</li> </ol> <p>These diverse routes shall:</p> <ol style="list-style-type: none"> <li>4. Not share any common telecommunications facilities or offices including common building entrance.</li> <li>5. Maintain a minimum separation of 30 feet throughout all diverse routes, except for cable crossovers, between premises/buildings where an SDP and its associated network connecting point are housed.</li> <li>6. Maintain a minimum vertical separation of two feet, with cables encased (separately) in steel or concrete for cable crossovers.</li> </ol> <p>Where uncompromised diversity is not available, the contractor shall:</p> <ol style="list-style-type: none"> <li>7. Exert best efforts to propose an acceptable arrangement along with documentation describing the</li> </ol>



ID Number	Name of Feature	Description
		<p>compromise.</p> <p>8. An acceptable alternative shall be negotiated, on an individual case basis, if diversity is not available or the compromised diversity is not acceptable to the Agency.</p> <p>When access diversity has been provided by the contractor, the Agency may at its discretion, elect to send telecommunications traffic over:</p>
		<p>9. Only one route (i.e., the primary route) thereby keeping the second route (i.e., the diverse route) inactive until needed</p> <p>10. Both routes on an ongoing basis, except where automatic re-routing equipment is utilized.</p> <p>The contractor shall provide the capability for the automatic switching of transmission in real-time, negotiated on an individual case basis:</p> <p>11. From the primary access route to the one or more diverse access routes, including satellite connection, and</p> <p>12. From the diverse access route to the primary access route.</p> <p>The contractor shall exercise the following control measures on the configuration or the reconfiguration of the diverse access route:</p> <p>13. The contractor shall provide within 30 calendar days of the implementation of access diversity and again thereafter when a change is made, a graphical representation (e.g., diagrams, maps) of access circuit routes to show where diversity has been implemented.</p> <p>14. The contractor shall provide to the Agency, with a copy to the PMO, written notification for Agency approval of any proposed reconfiguration of routes, previously configured for access diversity at least 30 calendar days in advance of implementation.</p> <p>15. In addition, the contractor shall establish internal control (i.e., electronic flagging of routes) to prevent the accidental dismantling of diversified routes, especially during routine route optimization initiatives by the contractor.</p>
2	Access Route or Path Avoidance	<p>Between an SDP and its associated connecting network point, the contractor shall supply the capability for a customer to define a geographic location or route to avoid.</p> <p>Where avoidance is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the reasons for the unavailability</p> <p>The contractor shall exercise the following control measures on the configuration or the reconfiguration of the avoidance access route:</p> <p>1. The contractor shall provide within 30 calendar days of the implementation of access avoidance and again thereafter when a change is made, a graphical representation (e.g., diagrams, maps) of access circuit routes to show where avoidance has been implemented.</p> <p>2. The contractor shall provide to the Agency, with a copy to the PMO, written notification for GSA approval of any</p>

ID Number	Name of Feature	Description
		<p>proposed reconfiguration of routes, previously configured for access avoidance at least 30 calendar days in advance of implementation.</p> <p>3. In addition, the contractor shall establish internal control (i.e., electronic flagging of routes) to prevent the accidental dismantling of avoidance routes, especially during routine route optimization initiatives by the contractor.</p>

### C.2.15.2.1.3 Interfaces

The User-to-Network Interfaces (UNIs) at the SDP, as defined in the Section C.2.16.2.1.3.1, are mandatory unless indicated otherwise:

#### C.2.15.2.1.3.1 Wireline Access Arrangement Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403]	Up to 1.536 Mbps	Transparent
6 [Optional]	ISDN PRI [Std: ANSI T1.607/610])	Up to 1.472 Mbps	Transparent
7	T3 [Std: Telcordia GR-400-CORE]	Up to 43.008 Mbps	Transparent
8 [Optional]	E1 (Std: ITU-TSS G.702) (Non-domestic)	Up to 1.92 Mbps	Transparent
9 [Optional]	E3 (Std: ITU-TSS G.702) (Non-domestic)	Up to 30.72 Mbps	Transparent
10 [Optional]	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
11 [Optional]	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
12 [Optional]	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
13 [Optional]	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
14 [Optional]	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
15 [Optional]	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
16 [Optional]	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
17	SONET OC-192c	9.510912 Gbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
17 [Optional]	(Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent

### C.2.15.2.2 Broadband Access Arrangement (BBA)

Broadband Access Arrangement connects an Agency location with dedicated, reliable broadband bandwidth to the contractor's data network over communication facilities, such as Digital Subscriber Line (DSL), Ethernet Access, Cable High-Speed Service, and Fiber-To-The-Premises (FTTP) service. The range of broadband line speeds (e.g., 256 kbps to up to 1Gbps) and reliability options provided within this access arrangement category will allow Government users to satisfy their diverse needs for accessing contractor's data networks. With this access arrangement, applications such as desktop video conferencing, distance learning, and transferring of large files can be realized.

#### C.2.15.2.2.1 Basic Access Arrangement Description

##### C.2.15.2.2.1.1 Functional Definition

Broadband Access Arrangement includes dedicated transmission access between Agency location and contractor's transport network. BBA is an SDP to POP connecting access arrangement, i.e., it connects the SDP at the Agency location to the Point of Presence of the contractor's network. This access arrangement can be used for any end-user's application, such as desktop video conferencing, distance learning, and transferring of large files.

##### C.2.15.2.2.1.2 Reserved

##### C.2.15.2.2.1.3 Connectivity

Broadband Access Arrangement shall connect to and interoperate with:

1. Government specified locations (e.g., SDPs, such as LAN, Router, Work station, Video codec, and Group 4 FAX)
2. POPs of contractor's network

##### C.2.15.2.2.1.4 Technical Capabilities

The following Broadband Access Arrangement capabilities are mandatory unless marked optional:

1. Broadband Access Arrangements.
  - a. **DSL**. This category of access arrangement shall be offered as required by Section J.2.3.1.2:
    - (1) Provide the following types of DSL services, at a minimum:
      - i. Asymmetric DSL (ADSL). Support ADSL asymmetric data rates for upstream and downstream traffic as follows:

2. Upstream: Data rates range from 16 to 640 Kbps (e.g., 256 Kbps) and optionally to 768 Kbps.
  3. Downstream: Data rates range from 1.5 Mbps to 6 Mbps (e.g., at 1.5, 2, 3, 4, 5, and 6 Mbps). Speeds up to 9 Mbps is optional.
  - ii. Symmetric DSL (SDSL). Support SDSL symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates up to and including 1.5 Mbps. 2.3 Mbps is optional
  - iii. [Optional] ISDN IDSL (IDSL). Support ISDN symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates of 144 Kbps.
- (2) Comply with the following standards for ADSL and SDSL as applicable.
- a. ADSL and DSL Forums
  - b. ITU-TSS Recommendation G.992 for ADSL (interoperable DSL modem and DSLAM line card)
  - c. ANSI T1.413 (compatible DSL modem and DSLAM line card from the same manufacturer)
- (3) Comply with the following standards for IDSL as applicable
- (d) ISDN Forum
- (4) Split integrated voice and data traffic for ADSL and SDSL to direct voice traffic to the telephone unit/set and data traffic to the ADSL/SDSL modem.
- b. **Ethernet Access [Optional]**. If offered, this category of access arrangement shall:
- i. Provide access to Ethernet service/network through the use of data link layer 2 protocol and be transparent to the upper layer protocols (i.e. layer 3 and above) for:
    - d. Ethernet LAN at 10 Mbps
    - e. Ethernet LAN at 100 Mbps
    - f. Ethernet LAN at 1 Gbps
    - g. Ethernet LAN at 10 Gbps (Optional)
  - ii. Comply with the following standards for Ethernet Access as
    - d. IEEE 802.3, including 10 Base-T/TX/FX, 100 Base-TX/FX, 1000 Base-T/FX/L/LX/B/BX/PX, and 10 Gigabit Ethernet (IEEE 802.3ae and 10 GbE)
  - iii. Support the following payload data rates for the Ethernet Access link:

- 2. 10 Mbps
- 3. 100 Mbps
- 4. 1 Gbps
- 5. 10 Gbps (Optional)

c. **Cable High-Speed Service [Optional]**. If offered, this category of access arrangement shall:

i. Provide data rates of 256 Kbps to 30 Mbps as follows:

- 38. From 256 Kbps to a maximum of 5 Mbps (Standard: DOCSIS 1.0)
- 39. From 256 Kbps to a maximum of 10 Mbps (Standard: DOCSIS 1.1)
- 40. From 256 Kbps to a maximum of 30 Mbps (Standard: DOCSIS 2.0) (Optional)
  - ii. Comply with the following DOCSIS (Cable Labs) standards as applicable.
    - 3. DOCSIS 1.0
    - 4. DOCSIS 1.1
    - 5. DOCSIS 2.0

1. **FTTP [Optional]**. If offered, this category of access arrangement shall provide data rates over fiber as follows:

- 1. 5 Mbps (downstream) and 2 Mbps (upstream)
- 2. 15 Mbps (downstream) and 2 Mbps (upstream)
- 3. 30 Mbps (downstream) and 5 Mbps (upstream).

**C.2.15.2.2.2 Features**

The following Broadband Access Arrangement features in the Section C.2.16.2.2.2.1 are mandatory unless marked optional:

**C.2.15.2.2.2.1 Broadband Access Arrangement Features**

ID Number	Name of Feature	Description
1 [Optional]	Specific to Cable-TV Service (for Cable High-Speed Service)	The contractor shall split integrated "Cable High-Speed Service" and "Cable-TV Service" to direct "Cable High-Speed Service" traffic to cable-modem and "Cable-TV" traffic to user's TV set and shall provide various "Cable-TV Service" channels as available commercially from the contractor.

**C.2.15.2.2.3 Interfaces**

The User-to-Network Interfaces (UNIs) at the SDP as defined in the Section C.2.16.2.2.3.1, are mandatory unless marked optional:



UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
6	USB 2.0 (Std: USB Implementers' Forum)	Link bandwidth: Up to 30 Mbps [maximum USB 2.0 bandwidth is 480 Mbps]	c. Transparent d. IP (v4/v6)
7 [Optional]	T1 [Std: Telcordia SR-TSV-002275; ANSI T1.403]	Up to 1.536 Mbps	1. Transparent 2. IP (v4/v6)
8 [Optional]	ISDN BRI (Multirate) [Standard: ANSI T1.607 and 610]	144 kbps	a. ITU-TSS Q.931 b. IP (v4/v6)

Note: IPv6 shall be supported when offered commercially by the contractor.

**C.2.15.2.3 Wireless Access Arrangement (WLSAA) [Optional]**

Wireless Access Arrangement connects Agency locations to contractor's network through broadband wireless communication facilities/networks (e.g., MMDS, LMDS, and Ultra High at 2 to 66 GHz and an optional upper limit of 90 GHz spectrum; and, National Guard Frequency at 1.755 to 1.850 GHz spectrum through a roof-top antenna). This access arrangement can be used for Network services, e.g., VS, NBIP-VPNS, and VTS.

**C.2.15.2.3.1 Basic Access Arrangement Description**

**C.2.15.2.3.1.1 Functional Definition**

Wireless Access Arrangement is a wireless transmission access arrangement to the contractor's network from Agency locations. Broadband Wireless supports protocol-transparent (i.e., physical level) transmission for services, such as VS, NBIP-VPNS, and VTS.

WLSAA is an SDP to POP connecting access arrangement, i.e., it connects the SDP (i.e., Agency location or the mobile terminal) to the POP of the contractor's network.

**C.2.15.2.3.1.2 Standards**

Wireless Access Arrangement shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

- Standards based on IEEE 802.16 (when available commercially)
- The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards when offered commercially.

**C.2.15.2.3.1.3 Connectivity**

Wireless Access Arrangement shall connect to and interoperate with:

1. Government specified locations (i.e., SDPs, such as LAN, Router, Work station, Video codec, and Group 4 FAX) through Broadband Wireless.
2. POPs of contractor's network

**C.2.15.2.3.1.4 Technical Capabilities**

The following Wireless Access Arrangement categories are mandatory unless marked optional:

1. **Broadband Wireless.** This category of access arrangement shall provide broadband wireless point-to-point protocol-transparent (i.e., physical level) transmission connection between an SDP and the contractor's POP for Network services (e.g., VS, NBIP-VPNS, and VTS).

The following symmetric data rates shall be supported:

- a. DS1
- b. NxDS1s (where N=2 through 27)
- c. DS3
- d. E1 [Non-domestic]
- e. NxE1s (where N=2 through 15) [Non-domestic]
- f. E3. [Non-domestic]

The following capabilities are optional:

1. Wireless access through non line of sight antenna
2. Higher data rates (e.g., SONET).

**C.2.15.2.3.2 Features**

None

**C.2.15.2.3.3 Interfaces**

The User-to-Network Interfaces (UNIs) at the SDP, as defined in the Section C.2.16.2.3.3.1, are mandatory unless marked optional:

**C.2.15.2.3.3.1 Wireless Access Arrangement Interfaces**

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	ITU-TSS V.35 (Specific to Broadband Wireless)	Up to 1.92 Mbps	Transparent
2	EIA RS-449 (Specific to Broadband Wireless)	Up to 1.92 Mbps	Transparent
3	EIA RS-232 (Specific to Broadband Wireless)	Up to 19.2 kbps	Transparent
4	EIA RS-530 (Specific to	Up to 1.92 Mbps	Transparent



UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
	Broadband Wireless)		
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403] (Specific to Broadband Wireless)	Up to 1.536 Mbps	Transparent
6	T3 [Std: Telcordia GR-400-CORE] (Specific to Broadband Wireless)	Up to 43.008 Mbps	Transparent
7	E1 (Std: ITU-TSS G.702) (Non-domestic)	Up to 1.92 Mbps	Transparent
8	E3 (Std: ITU-TSS G.702) (Non-domestic)	Up to 30.72 Mbps	Transparent

#### C.2.15.2.4 Satellite Access Arrangement (SatAA) [Optional]

Satellite Access Arrangement connects Agency location with dedicated and reliable satellite based transmission to the contractor's network. The connection from satellite earth station to the SDP is also included in this access arrangement. This access arrangement could be used for voice, data, and video traffic. The access arrangement provides full-duplex and half-duplex transmissions using C-band, Ku-band, and Ka-band satellites.

##### C.2.15.2.4.1 Basic Access Arrangement Description

###### C.2.15.2.4.1.1 Functional Definition

Satellite Access Arrangement includes satellite transmission access arrangement between Agency location and contractor's transport network. SatAA is an SDP to POP connecting access arrangement, i.e., it connects the SDP at the Agency location to the Point of Presence of the contractor's network. This access arrangement can be used for any application, such as voice, data, video, and multimedia; and, may include Government end-to-end encrypted communication.

###### C.2.15.2.4.1.2 Standards

Satellite Access Arrangement shall comply with the following standards, as applicable. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the standards listed below.

1. Satellite transponders' bands frequency allocations and channel bandwidth (FCC) as applicable:
  - C-Band. Uplink: 5.9 to 6.4 GHz; Downlink: 3.7 to 4.2 GHz; Bandwidth: 500 MHz
  - Ku-Band. Uplink: 14 to 14.5 GHz; Downlink: 11.7 to 12.2 GHz; Bandwidth: 500 MHz

- Ka-band. Uplink: 30 to 31 GHz; Downlink: 20 to 21 GHz; Bandwidth: 500 MHz (when available commercially)
- 2. Reserved
- 3. Reserved
- 4. Transmission Performance and GFP Interfaces
  - 6. ANSI T1.102/107/403/503/510 for T1 data rate
  - 7. Telcordia PUB GR-499-CORE for T3 data rate
  - 8. ITU-TSS G.702 and related recommendations for E1
  - 9. ANSI T1.105 and 106 for SONET
  - 10. USB 2.0 (USB Implementers' Forum) [Optional]
  - 11. IEEE 802.3, including 10 Base-T/TX/FX and 100 Base-TX/FX
- 5. The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards when offered commercially.

**C.2.15.2.4.1.3 Connectivity**

Satellite Access Arrangement shall connect to and interoperate with:

- Government specified permanent or temporary locations (i.e., SDPs, such as PBX, Multiplexer, Router, Video codec, earth station, and VSAT [1.2 to 4.5 meters; fixed and transportable/deployable])
- POP of contractor's network

**C.2.15.2.4.1.4 Technical Capabilities**

The following Satellite Access Arrangement capabilities are mandatory unless marked optional:

- Full-duplex, half-duplex, and simplex (i.e., one way) for point-to-point transmission (i.e., SDP to POP) for voice, data, and video traffic and for simplex egress connection (i.e., POP to SDP), the contractor shall support broadcast transmission at the airlink interface of Agency VSATs that are within the foot-print of the same satellite.
- The contractor shall define the contours of the SatAA coverage (i.e., foot print) maps and shall continue to provide any changes to satellite foot print for the frequency band(s) for each satellite providing the access arrangement.
- Transparent to any protocol used by the GFP.
- All bit sequences transmitted by the GFP through the SDP shall be treated with data transparency.

The following categories (i.e., data rates) of SatAA access arrangement shall be supported:

- a. **Fractional T1**. This category of SatAA shall support two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps.

- b. **T1**. This category of SatAA shall support a line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 access arrangement as follows:
  - (1) Channelized T1. In this mode, 24 separate DS0s clear channels of 56/64 kbps shall be supported.
  - (2) Unchannelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
- c. **E1 (Non-domestic)**. This category of SatAA shall support a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:
  - (1) Channelized E1. In this mode, 30 separate DS0 clear channels shall be supported.
  - (2) Unchannelized E1. In this mode, a single 1.92 Mbps information payload shall be supported.
- d. **Fractional T3**. This category of SatAA shall support two, three, or four adjacent DS1 clear-channels over an interface of T1 or T3.
- e. **T3**. This category of SatAA shall support a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 as follows:
  - (1) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
  - (2) Unchannelized T3. In this mode, a single 43.008 Mbps payload shall be supported.
- f. **SONET (Optional)**. This category of SatAA shall support SONET data rates (e.g., SONET OC-3).

All other SatAA data rates, including those that are available or that become available during the life of the contract, are included in the scope of the contract.

#### C.2.15.2.4.2 Features

None

#### C.2.15.2.4.3 Interfaces

The User-to-Network Interfaces (UNIs) at the SDP, as defined in Section C.2.16.2.4.3.1 are mandatory unless marked optional:

### C.2.15.2.4.3.1 Satellite Access Arrangement Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 Kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent
5	T1 [Std: Telcordia SR-TSV-002275; ANSI T1.403]	Up to 1.536 Mbps	Transparent
6	T3 [Std: Telcordia GR-499-CORE]	Up to 43.008 Mbps	Transparent
7	E1 (Std: ITU-TSS G.702) (Non-domestic)	Up to 1.92 Mbps	Transparent
8	USB 2.0 (high speed) (Optional)	Up to 43 Mbps (Note maximum serial bus speed is limited to 480 Mbps)	Transparent
9	Air link interface (C-band, Ku-band, and Ka-band earth station)	Up to 43.008 Mbps	Transparent

Note: The contractors are encouraged to support increased data rates above 1.92 Mbps for RS-449/422, and V.35 interfaces

## C.3 Management and Operation

### C.3.1 General Information

Management and Operations encompass the essential activities and requirements necessary to provide quality services to the Government throughout the life cycle of the contract. It begins with the overarching program management that puts the appropriate resources, systems, and processes in place with leadership to balance contract compliance, the needs of the Government, and the contractor's business approach. GSA Federal Technology Service (FTS) is the responsible Program Management Office (PMO) for the contract, and the Networx PMO will be the Government's primary point of contact with the contractor for program activities, in conjunction with the Contracting Officer (CO) for contract matters. However, this contract is open to all authorized Government Agencies who have their own unique environments and will need to access services on the contract in ways that meet Agency requirements. The Agencies may interface directly with the contractor for ordering, billing, inventory management, service management, training, and customer support. Furthermore, many Government organizations are decentralized, so multiple entities within a Department or an independent Agency may perform the functions of an "Agency." The Agency's responsibilities and functions may be delegated to another Agency, to a Sub-Agency or an Agency component, or to a contractor authorized to act on behalf of the Agency. Given this multi-faceted relationship, therefore, effective communication is critical to the

success of the program to ensure requirements, expectations, and solutions are clear and consistent.

The responsibilities of the contractor commence at contract award and apply through transition and life-cycle service delivery and management, including assisting GSA and Agencies with transitioning to the next contract. The contractor ensures that all service offerings under this contract comply with and are delivered according to the Management and Operations requirements.

To minimize the cost burden to the contractor, the sections for deliverable reports describe the required contents of the reports and do not prescribe a format; the format of the reports is left to the judgment or standard practice of the contractor.

NOTE: Land Mobile Radio Service (LMRS) has unique requirements outlined in Section C.2, Technical Requirements, for training, trouble handling, and network management. As such, those portions of the Management and Operations requirements DO NOT apply to LMRS (that is, Sections C.3.3.1, Network Management, C.3.4.2, Trouble and Complaint Handling, and C.3.7, Training).

#### **C.3.1.1 Section Format**

The Management and Operations section outlines the Government's role as well as that of the contractor. Each section begins with a definition of the process for the functional area it covers then steps through detailed activities and requirements for performing the process and meeting expected service levels. It identifies the contractor's requirements to provide data access, reports, systems access, and other information to GSA's Network PMO and other Government Agencies subscribing to the contractor's services.

Specific C.3 Management and Operations deliverables are identified within each section, detailed formatting and delivery requirements are provided at the end of each section, and a reference list of all deliverables is in Section F.2, contractor Deliverables.

Each section that follows in C.3.2 through C.3.9 is generally structured according to the sequence that follows:

#### C.3.X Functional Area

##### C.3.X.1 Process Definition

C.3.X.1.1 Process Description: a summary description of the process for which the requirements are defined

C.3.X.1.2 Process Narrative: a table showing the steps in the process and the party responsible for performing the steps

##### C.3.X.2 Functional Requirements:

C.3.X.2.1-n Step 1-Step n: detailed statement of work requirements for the contractor's role in the process containing only the steps in the Process Narrative for which the contractor is a responsible party; omitted steps are Government-only and are not contained in the Section.

C.3.X.3 Data Requirements: data that supports the process to be shared between GSA, the Agencies, and the contractor

C.3.X.4 Report Requirements: the deliverables required as outputs of the process

### C.3.1.2 Data and Report Requirements

Information deliverables and communication from the contractor to the Government is expected to be in the form of data, reports and unstructured communications such as telephone or e-mail contact for immediate notifications. The following definitions apply to the management and operations deliverables:

- Report – A type of written document providing information as specified by the Government
- Data – Information that is structured into fields or otherwise delimited so that it can be readily processed by an automated system as well as by a human
- Media – Type of package or storage of a report or data such as a file for purposes of delivery
- Transport – Method by which a report or data is transported or delivered
- Data Format – Structure or organization of data elements in a data file
- Report File Format – The application file type used to generate or store the report

Management and operations data and report deliverables will be specified using four elements that define the Deliverable Item Description.

- a. Frequency - when a deliverable is due. It will address the initial delivery as well as updates as necessary
- b. Deliver To – to whom the deliverable is provided. It may have more than one deliverable point
- c. Media/Transport/Format –the type of storage package, transport method, and format of the deliverable
- d. Content or Record Elements –the data or information elements for the deliverable

The contractor shall send to and shall receive from GSA and the Agencies data and reports, as specified by the Deliverable Item Description elements defined above and used in the Data Requirements (C.3.X.3, C.3.n.X.3, or C.4.X.3) and Report Requirements (C.3.X.4, C.3.n.X.4, or C.4.X.4) sections of C.3, Management and Operations and C.4, Transition.

In regard to media, transport and format, the Government requires that data and report deliverables be provided in ways that are compatible with ways the various Government recipients receive and process them. Many deliverables contain information segmented by Agency but delivered to GSA in aggregate for a complete set of the required elements for all Agencies the contractor serves. For designated deliverables, the contractor shall provide the Agency with its individual report in addition to the aggregated deliverable for GSA. In these cases, GSA's requirements for receipt are described separately from the Agency's requirements. At the time it requests a

deliverable, the Agency will specify which of the media/transport/format choices it requires.

The following paragraphs cite requirements for contractor reports and data that will be provided to the Agencies.

**Media/Transport/Format Requirements for Reports from the Contractor to the Agencies:**

The contractor shall be capable of providing reports to the Agencies as specified in the following table:

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**Media/Transport/Format Requirements for Data from the Contractor to the Agencies:**

The contractor shall be capable of providing data to the Agencies as specified in the following table:

Data		
Media	Transport	Data Format
Paper	<ul style="list-style-type: none"> <li>• Fax</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	

As existing media types become unsupported as an industry standard, the contractor shall notify the GSA Contracting Officer and all affected agencies. The contractor shall communicate with the affected agencies and migrate to a mutually agreed upon alternative media type that is equal to or more advanced than the unsupported or expiring media type. Such mutually agreed upon alternative media type shall be provided by the contractor at no cost for the media to the Government. Any costs associated with hardware or software required to read the alternative media type shall be borne by the affected agency. Until such time as the unsupported or expiring media type is removed from the list above, the contractor shall continue to use it if required by an agency.

As new media types emerge and become recognized industry standards the contractor shall notify the GSA Contracting Officer prior to adding it to the available options to agencies.



### C.3.1.3 Section Outline

The Management and Operations Section has been divided into major categories to facilitate the presentation of Government requirements and to delineate the contractor's roles and responsibilities to perform daily operational activities and support PMO program management and contract administration.

This section also defines the detailed requirements for the following functional areas:

- network management, security management, and disaster recovery
- customer service;
- service ordering;
- billing and invoicing, including disputes and adjustments;
- training
- inventory management and
- operational support system.

Program Management (Section C.3.2) presents the Government's requirements of the contractor for management and administration of the program. These activities include: comprehensive planning and control throughout the life-cycle of the contract, specific project planning for delivery of complex services or unique circumstances, establishing and maintaining various contact points, providing periodic reports for statistical and performance monitoring, presenting contract kickoff and monthly reviews, and supporting user forums. As part of this section the Networx PMO is defined and the Government's requirements of the contractor are identified for support of the PMO.

Service Management (Section C.3.3) presents the Government's requirements for managing, maintaining, and reporting on services provided to Agencies. These activities include: network management, security management, and disaster recovery.

Customer Service (Section C.3.4) presents the Government's requirements of the contractor to establish and operate a Customer Support Office (CSO) for providing high-quality support to the Government. This section defines the Government's requirements for the contractor to provide an automated system for recording and handling trouble reports, complaints, and general inquiries. It also presents requirements for escalating the resolution of troubles and complaints. Furthermore, Customer Service discusses requirements for the contractor to maintain an effective business relationship with the Government users and support the Government's efforts through sales forecasting and optimization of service configurations.

Service Ordering (Section C.3.5) contains the Government's requirements for a user-to-contractor ordering process and an automated system to facilitate it. The process must support standardized electronic transactions, order tracking and inquiry, and retaining and processing data between the automated service ordering and billing systems.

Billing (Section C.3.6) addresses the Government's requirements of the contractor to use an automated billing system, to support delivery of data and invoices using

standard elements, and to provide a process for disputes and adjustments. Detailed billing activities include: direct billing, centralized billing, billing inquiries and disputes, and shared-tenant billing.

Training (Section C.3.7) describes the Government's requirements of the contractor to provide training to various levels of Government staff and Agency personnel. Training is either technical or non-technical in nature and may be delivered through a variety of methods.

Inventory Management (Section C.3.8) establishes the Government's requirement for the contractor to maintain current inventories and to make them available to both Agencies and GSA. The contractor provides inventory data for a given Agency only to that Agency and to GSA. Inventory data is to be available throughout the entire period of this contract. Operational Support Systems (Section C.3.9) describes the Government's requirement for the contractor's operational support systems to perform billing, service ordering, customer service, service management, inventory management, and program management.

### C.3.2 Program Management

#### C.3.2.1 Program Management Process Definition

##### C.3.2.1.1 Program Management Process Description

This section describes the requirements for management at the program level and establishment of the Contractor's Program Organization (CPO). These contractor program management responsibilities shall remain in effect through the duration of the Networkx contract.

The CPO interfaces directly with Agencies subscribing to services and GSA's Networkx Program Management Office (PMO). The Networkx PMO is accountable for technical performance of the Networkx contractors. As such, the PMO will direct and monitor the work of the contractor as well as serve as liaison to the subscribing Agencies to ensure their requirements are met and resolve any issues that require PMO attention. The CPO is the primary interface to the Government for program management activities, including but not limited to program control, planning at the program level, planning at the Agency level, contractor performance, resource management, revenue management, reporting and reviews, and senior-level communications.

##### C.3.2.1.2 Program Management Process Narrative

Step Number	Description	Executing Entities
1	The contractor establishes a "Contractor's Program Organization (CPO).	Contractor
2	The contractor develops a Program Management Plan (PMP).	Contractor
3	The CPO develops a project plan, which includes schedule and resource allocation, for program management activities.	Contractor

Step Number	Description	Executing Entities
4	The CPO performs financial management activities, including tracking billed revenue for Networx, reporting, and supporting the Government's process for comparing contract prices to those available elsewhere (refer to Section H.7, Price Management Mechanism).	Contractor
5	GSA provides contractor a list of Networx PMO contacts, Contracting Officer Representatives (CORs) for the contract and customer service representatives for each Agency.	GSA
6	The contractor hosts a program launch meeting with the PMO, Agencies, and associated CORs, DARs, customer service representatives and others as determined by the Government.	Contractor
7	The contractor delivers Program Monthly Status Reports and leads Quarterly Program Management Reviews to the Networx PMO and supports ad hoc user forums and other meetings.	Contractor
8	The contractor creates and executes against Service Delivery Project Plans for fulfilling orders that constitute a project.	Contractor
9	The contractor provides data and reports. The Government retains rights to all data contained within reports and to formats the Government provides. The contractor owns the intellectual property associated with formats the contractor provides.	Contractor/ Agency/ GSA
10	The contractor manages its assigned numbers, Internet Protocol (IP) addresses, and domain names to ensure no duplication of assignments.	Contractor
11	The contractor provides Networx Inventory Codes. Input provided from Telcordia.	Contractor
12	The contractor supports the Government in transitioning at Networx contract expiration or another contract.	Contractor

### C.3.2.2 Program Management Functional Requirements

#### C.3.2.2.1 Step 1--Contractor's Program Organization

##### C.3.2.2.1.1 General Description

ID Number	Description
1	The contractor shall maintain a Contractor's Program Organization (CPO) for program control and management of the Networx contract. The CPO shall provide effective and efficient program management through the application of support tools and industry best practices. The CPO shall be led by the Networx program director and generally be comprised of leads from each functional area of the contractor's company that have a role in executing against the contract.
2	The contractor's CPO shall not be housed in Government space.
3	The contractor's CPO shall support a Government PMO and subscribing Agencies that are dispersed domestically and non-domestically.

##### C.3.2.2.1.2 Quality Assurance and Contract Compliance

ID Number	Description
-----------	-------------

ID Number	Description
1	The contractor's performance shall be measured against the set of SLAs established by the Networx contract
2	The contractor's CPO shall be the single point of interface for SLA information the Government requires. The CPO will deliver SLA data and reports to the Networx PMO and others in accordance with the Networx contract
3	The contractor shall establish a process for detailed, monitoring and reporting to enable an accurate assessment of performance against SLAs
4	The contractor's CPO shall resolve all issues concerning SLAs, including those that pertain to subcontractors. Issues concerning SLAs include but are not limited to items such as missing data, data reported in the wrong format or units, late submission from subcontractors, etc.
5	The contractor shall compile the SLA data from all sources, including subcontractors, into a single SLA Compliance Report, which shall be in a "scorecard" format to allow quick review of all SLAs.
6	The contractor shall deliver to individual Agencies an Agency-Specific SLA Monthly Compliance Report that contains only the SLA performance data for that Agency.
7	The CPO shall be responsible for monitoring and managing the contractor's performance against all contract performance requirements.

#### C.3.2.2.1.3 Human Resource Management

ID Number	Description
1	Contractor shall have in place a methodology for determining staffing levels required to complete the work under this contract and for assessing the skills and competence of staff to perform the functions required.
2	Contractor shall have in place a disciplinary and removal process for its employees.

#### C.3.2.2.1.4 Contractor Policies and Procedures

ID Number	Description
1	The contractor shall develop, implement, and update a Policies and Procedures (P&P) document(s) that provide direction to staff on the methods of performing their Networx responsibilities.

ID Number	Description
2	The contractor's P&P shall outline contractor and subcontractor procedures regarding performance of functions under this contract, including, but not limited to: (a) Network management, including security (b) Inventory management (c) Billing (d) Customer Support (e) Account management (f) Order Processing and Fulfillment (g) Training Development and Delivery (h) Analysis and Reporting (i) Network Augments for Infrastructure as well as Customer Orders (j) Document change control (k) Network configuration control (l) OSS change control

**C.3.2.2.1.5 Document Change Control**

ID Number	Description
1	The contractor shall manage changes to versions of all documentation required in the contract. Documentation change control includes: (a) Tracking versions (b) Tracking history of changes (c) Retrieving previous versions of files

**C.3.2.2.1.6 Coordination and Communication**

ID Number	Description
1	The contractor shall implement consistent and effective communications between management and technical personnel as indicated in Section C.3.2.2.2, Program Management Plan.
2	The CPO shall manage the customer relationship, including, but not limited to: (a) Government PMO-to-CPO communications (b) Resolution of Trouble Reports and Complaints (c) Resolution of Issue calls (d) Resolution of Billing Disputes and Inquiries (e) Resolution of Schedule issues (f) Resolution of Reporting Discrepancies
3	The CPO shall provide technical expertise associated with the contractor's network management center, help desk, management chain of command, and all other contractor organizations used to provide service and support to the Government.
4	The CPO shall answer questions and address issues from the Network PMO regarding the contractor's network management activities, particularly those that have not been resolved to the Government's satisfaction through the standard trouble handling process according to Section C.3.4.2, CSO - Trouble and Complaint Handling.
5	The CPO shall provide the means by which the contractor or the Government can

ID Number	Description
	escalate issues to the appropriate levels of the contractor's management in order to resolve disputes and issues.
6	<p>At a minimum the CPO shall have the capability and authority to:</p> <ul style="list-style-type: none"> <li>(a) Support disaster recovery planning and execution</li> <li>(b) Resolve interoperability problems</li> <li>(c) Respond to escalation of service concerns</li> <li>(d) Participate in contract performance reviews</li> <li>(e) Participate in contract modification negotiations</li> <li>(f) Perform basic network management functions in support of the Government's requirements in Section C.3.3, Service Management</li> <li>(g) Help resolve billing queries and reconciliation issues</li> <li>(h) Support NS/EP requirements</li> <li>(i) Provide the Networx PMO with information on customer requirements and customer demographics</li> </ul>
7	<p>The contractor shall identify as contractor Points of Contact employees and at least two levels of management escalation contacts who are responsible for, but not limited to the functions that follow (see Section C.3.2.3, Program Management Data Requirements):</p> <ul style="list-style-type: none"> <li>(a) Networx program management</li> <li>(b) Provisioning Orders</li> <li>(c) Identifying and resolving service troubles and complaints</li> <li>(d) Providing customers with status of troubles and resolution</li> <li>(e) Developing and delivering training</li> <li>(f) Conducting billing inquiries</li> <li>(g) Transition project management</li> <li>(h) Finance</li> <li>(i) Contracting</li> <li>(j) Account Management (business development and sales)</li> <li>(k) Security and National security/emergency planning (NS/EP)</li> <li>(l) Technicians who perform work at Government sites.</li> </ul>
8	<p>The contractor shall identify to the Government contractor Points of Contact who have passed national Agency checks or background investigations and the security clearance levels held by these individuals. At the Government's discretion, higher clearances and access authorization will be required. See Section C.3.3.2, Security Management.</p>
9	<p>Contractor Points of Contact technicians assigned to perform work at Government sites will be, at the Government's discretion, required to pass a national Agency check prior to their assignment. See Section C.3.3.2, Security Management. The contractor shall initiate requests for background investigations of personnel, as identified by the Government, requiring national Agency checks. Failure to secure the proper clearances for personnel within a reasonable amount of time (as determined by the Government based on recent similar requests) may result in unexcused delays in or inability to perform in accordance with the contract.</p>
10	<p>The contractor shall have a point of contact available for each Agency and GSA on a full-coverage basis (24x7).</p>

**C.3.2.2.2 Step 2--Program Management Plan (PMP)**

ID Number	Description
1	<p>The contractor shall deliver a Program Management Plan (PMP), in accordance with Section C.3.2.4, Program Management Report Requirements that details its program management method and implementation plan at a level sufficient to give the Government an understanding of the program management approach. The PMP</p>

ID Number	Description
	<p>shall address, at a minimum, the following:</p> <p>Summary of Contract Requirements, including Government dependencies and assumptions regarding Government services, facilities, and personnel</p> <p>Summary Description of Service Solution, including methodology to comply with Service Ordering, Billing, Inventory Management, and Service Management requirements</p> <p>Program Management Schedule</p> <p>Resource Plan: Management approach to</p> <p>Financial Resources: budgeting, tracking, and controlling costs</p> <p>Human Resources: identifying and retaining qualified personnel and making effective use of their skills</p> <p>Equipment: managing hardware and software assets</p> <p>Quality Assurance Program: Management approach to formulating and enforcing work and quality standards, ensuring compliance with contractual Service Level Agreements (SLAs), reviewing work in progress, and providing Customer Support services</p> <p>Technology Plan: Approach to managing the network or service infrastructure, providing recommendations for optimization of services and policies, and procedures to improve service or refresh technology</p> <p>Communication Plan: Approach to communicating individual task requirements, resolving technical, service and personnel issues and risks between the contractor's key personnel and the Government, managing communications between the contractor and the Government, including contractor points of contact, and processing lessons learned</p> <p>Subcontractor Management and Vendor/Carrier Relations: Approach to managing teaming relationships with all subcontractors, effective relations with vendors and other service providers, and meeting the requirements of Section H.19.</p> <p>Organizational Structure: Management structure, organizations, and roles and responsibilities of each function performing work under this contract; key personnel and subject matter experts.</p> <p>Risk Management Plan: Process for identifying program risks, including risks identified in this statement of work, and actions to mitigate them.</p> <p>Information Systems: Description of OSS employed to implement the requirements of the contract consistent with security plans for precluding unauthorized access to the Government's data and an Agency's access to data belonging to any other Agency, and describing how the contractor shall ensure those systems are available immediately upon Notice to Proceed to meet the requirements of Section C.3.9, Operational Support Systems.</p>

**C.3.2.2.3 Step 3: Develop Project Plan for Program Management Activities**

ID Number	Description
1	<p>The contractor, through the CPO, shall effectively and responsively plan, control, and execute against this contract. This includes all activities related to contract compliance and all entities supporting the CPO, including, but not limited to, subcontractors, vendors, other service providers, and internal departments such as marketing, legal, finance, sales, provisioning, network management, billing, engineering, and program control.</p>

ID Number	Description
2	The contractor shall establish a master Project Plan for all program milestones and deliverables required to comply with the contract throughout its life. The Project Plan shall provide a means of scheduling and directing work, defining predecessor relationships for tasks, determining required human resources, and tracking variance to a baseline and current schedule. The Project Plan shall also allow for reporting on these functions.

#### C.3.2.2.4 Step 4: Financial Management

ID Number	Description
1	The contractor shall furnish the PMO and the GSA Contracting Officer (CO) with a Monthly Financial Status Report.
2	The contractor shall support the Government's efforts for price management in accordance with the requirements in Section H.7, Price Management Mechanism

#### C.3.2.2.5 Step 6: Program Launch Meeting

In order to familiarize the Government with the contractor's proposed solution and services, the contractor hosts a Program Launch Meeting.

ID Number	Description
1	The contractor shall schedule the Program Launch Meeting with the Network PMO after Notice to Proceed and announce the meeting to the Government users of this contract on its website
2	The contractor shall introduce the CPO and other functional team leads and present plan for delivering services to Agency and interfacing with COR and others.
3	The contractor shall give an overview of the services it has available under the contract.
4	The contractor shall explain the schedule for providing training to Agencies and describe processes for receiving orders, delivering services, and managing them through the life-cycle.
5	The contractor shall perform the Program Launch Meeting within one month of Notice to Proceed and may be delivered through on-site attendance as well as a conference call. The contractor shall deliver the on-site Program Launch Meeting within the Washington DC metropolitan area.

#### C.3.2.2.6 Step 7: Deliver Program Reviews and Support User Forums

ID Number	Description
1	The contractor shall support periodic meetings and user forums based on program needs to discuss topics of interest and answer questions. Meeting and forums are intended to provide both the Government and the contractor an equal opportunity to exchange information
2	The contractor shall make its representatives available at user forums to: (a) Answer questions and document issues raised by Agencies



ID Number	Description
	(b) Report on completed contract modifications and the resolution of outstanding actions from previous meetings and user forums
3	The contractor shall provide demonstrations of new technology recently added to the Networx contract
4	The contractor shall issue a User Forums Issues Report documenting issues that were identified in the forums.
5	The contractor shall deliver monthly Program Monthly Status Reports according to Section C.3.2.4, Program Management Report Requirements.
6	The contractor shall lead Quarterly Program Management Review meetings. Program Reviews shall include a roll-up of information contained in the Program Monthly Status Reports
7	The contractor shall present the SLA Compliance Report as individual months with the trend from previous months. For measures not in compliance with SLAs, the contractor shall describe the root cause and remedy

#### C.3.2.2.7 Step 8: Service Delivery Project Plans

ID Number	Description
1	When an Agency has a need for Networx services that involve multiple sites or complex or mission-critical requirements, the Agency may request the contractor to fulfill the need by approaching it as a project. Service Delivery Projects may include adding multiple services at a single location, adding new services to multiple locations, implementing a private network, or migrating services from an existing provider or contract (other than FTS contracts, transitioning from an existing FTS contract is covered in Section C.4, Transition). In these cases flowing orders through the routine service delivery process will not adequately address the special requirements for coordinating activation of service.
2	For Service Delivery Projects requested by the Government, the contractor shall develop and implement a Service Delivery Project Plan (SDPP) that complies with Section C.3.2.4, Program Management Report Requirements
3	The contractor shall describe the organizational structure and identify lead points of contact for each functional area associated with the project in the SDPP.
4	The contractor shall identify in the SDPP any unique factors of each work effort in a project and the solution for ensuring that adequate resources are available to perform each.
5	The contractor shall coordinate the completion and acceptance criteria for the Service Delivery Project with the ordering Agency and establish the point at which billing will commence.
6	In the case of moving from existing contracts (other than FTS contracts), the ordering Agency will be responsible for interaction with the incumbent contractor, including placing any necessary orders, initiating any required contractual action, and coordinating schedules with the Networx provider.
7	For Service Delivery Projects involving moving from existing contracts (other than transition), the contractor shall complete an inventory of incumbent contractor services being replaced as part of the project as an attachment to the SDPP. This inventory shall contain data elements sufficient to comply with standard ordering and billing requirements of this contract.

ID Number	Description
8	At the request of the ordering Agency, the contractor shall accept bulk orders for multiple instances of the same service within the project, in addition to individual orders, in accordance with Section C.3.5.1, Direct Ordering. For projects involving more than one kind of service, the contractor shall accept and manage multiple bulk orders within the project.
9	The contractor shall complete Service Delivery Projects by the baseline completion dates of the SDPP mutually agreed upon with the Agency at the time orders are placed and acknowledged by the contractor. The baseline dates will be the Firm Order Commitment dates for each order within the project, which shall meet the provisioning objectives in Attachment J.12.3, Service Provisioning Intervals, for routine or Class B expedited orders unless the Agency otherwise agrees to different intervals.
10	For all other order-fulfillment activities, the contractor shall proceed according to routine ordering process. This includes site visits the contractor requires, orders to local exchange carriers, test and acceptance of service, and training as required.
11	The Agency will monitor contractor's project management performance and coordinate corrective action with GSA if required.
12	GSA will monitor and facilitate coordination and issue resolution between the contractor, Agencies, and other GSA FTS contractors.
13	If the Agency chooses to identify all orders within the project using a single Agency Service Request Number (ASRN), the contractor shall accept a single ASRN for the project orders and include that ASRN on all documents and acknowledgements wherever it is a required data element, as specified in Attachment J.12, Ordering and Billing Data Elements.
14	If the Agency chooses to identify all orders within the project using a single project name or number, the contractor shall accept that project identifier and include it in any documents relating to the project, particularly the SDPP.

**C.3.2.2.8 Step 9: Government Rights to Data and Reports**

ID Number	Description
1	The contractor shall, upon request, describe to the direct billed Agencies and GSA the derivation of data and information provided by the contractor at no additional cost to the Government
2	The contractor shall provide, as requested by the Government, additional information necessary to permit the Government to conduct contract administration and to manage the Network program

**C.3.2.2.9 Step 10:--Manage Network Numbering, Naming, and Addressing**

ID Number	Description
1	The contractor shall administer the numbering, addressing, and naming plans associated with its network(s).
2	The contractor shall ensure that the same identifier is not assigned to any other user or any other contractor's network.
3	The contractor shall maintain and make available for GSA review a list of assigned: On-net numbers including NANP

ID Number	Description
	Non-commercial Agency-specific private numbers Non-domestic numbers Other individual network contractor assigned numbers that are utilized for specific network functions such as security, customer assistance, and other situations where assignment of an NANP or non-domestic number is not appropriate IP Addresses of elements providing Networkx services under this contract Domain names of web sites delivered under this contract
4	In the event of a duplicate assignment, the contractor shall resolve the duplication and any resulting service outage at no cost to the Government. Service performance requirements, KPIs, and SLAs within this contract shall apply as well as credits to the Government for failure to meet SLAs.

**C.3.2.2.10 Step 11: Networkx Inventory Codes**

This step describes the requirements for assigning Networkx Inventory Codes, Network Sites Codes, and Serving Wire Centers (SWC)s associated with orders placed by the Agencies.

The contractor shall subscribe to Telcordia’s Common Language Location Identifier (CLLI™) system to generate both the Networkx Inventory Code and the Network Site Code.

For those locations where dedicated access is required for the service ordered, the Network Site Code is used to determine the SWC that serves the SDP. GSA will maintain and provide to the contractor a mapping of Network Site Codes to SWCs. The Network Site Code uses geographical and geopolitical codes to represent buildings, structures, enclosures or other fixed, physical locations. The Network Site Code has eight alphanumeric characters. The first four are the Geographical representation of the city, the next two are the Geopolitical representation of the state or country, and the final two represent the building associated with that Geographical/Geopolitical pair.

The Networkx Inventory Code is to be used for several purposes: Ordering, Billing, Inventory Management, Service Management and reporting. The Networkx Inventory Code is eleven alphanumeric characters, the first eight of which are the Network Site Code, and the last three represent the contract and the service ordered by the Agency at the Network Site Code.

The contractor shall follow the conventions in this section when validating an address for the SDP(s) for each order. If the contractor determines the Agency has not provided the correct address, the contractor shall obtain the correct address through the order validation process in C.3.5.1, Direct Ordering before completing the order.

The conventions to determine which address to use for defining the Network Site Code are as follows:

Rule Number	Rule
1	If a dedicated access circuit is ordered with the service, the contractor shall enter into Telcordia's system the address where the circuit terminates and retrieve the Network Site Code assigned by the system.
2	If a Service Enabling Device is delivered and installed at a fixed, physical location for a service order, the contractor shall enter into Telcordia's system the address of the building where the SED is installed and retrieve the Network Site Code assigned by the system.
3	In all other cases the contractor shall enter into Telcordia's system the address of the Agency representative accepting the service, as indicated on the order (typically the Local Government Contact).
4	The Network Inventory Code shall be defined by the Network Site Code, the contract, and the service ordered. The contractor shall retrieve the Network Inventory Code from Telcordia's system after identifying in the system the contract and service for the order the contractor is processing.

The remaining functional requirements are detailed below.

ID Number	Description
1	The contractor shall establish an account with Telcordia to receive Network Inventory Codes and Network Site Codes.
2	The contractor shall retrieve from Telcordia's Common Language Location Identifier (CLLI™) system a Network Inventory Code and accept it as a required data element for pricing, ordering, billing, inventory, and service management to identify a physical address for the service, as well as the service and the contract under which it is provided.
3	The contractor shall select a Network Inventory Code that already exists, rather than creating a new code, wherever an existing code will accurately define the location, service, and contract.
4	The contractor shall support Government-conducted audits as they occur and make corrections as required to ensure accuracy of the Network Inventory Code assignments.
5	The contractor shall provide the Network Inventory Code as required by Attachment J.12, Ordering and Billing Data Elements.
6	Using the Network Site Code, the contractor shall use Table B.6.5-9 Domestic Site to SWC Relationship to determine the SWC for pricing those locations that require dedicated access.
7	The contractor shall not deliver a Service Order Confirmation for any order that requires dedicated access unless the mapping between the Network Site Code and the SWC is in Table B.6.5-9 Domestic Site to SWC Relationship.
8	The contractor shall work with GSA or its representative to determine the SWC for those Network Site Codes that are not in Table B.6.5-9.
9	The contractor shall provide the SWC in the Ordering, Acknowledgement, and Billing data elements as required by Attachment J.12, Ordering and Billing Data Elements.
10	The contractor shall not deliver a Service Order Confirmation for any orders to locations for which the contractor does not have a price at the assigned SWC.
11	The contractor shall submit modifications to add prices for new SWCs at which the Government requires service.

ID Number	Description
12	The contractor shall submit modifications that include both Table B.6.5-2 Domestic Serving Wire Center to Point of Presence Relationship and Table B.3.1-1 Domestic Wireline Access Prices (MRC) whenever the contractor submits pricing for SWCs it does not have on contract for Wireline Access.
13	The contractor shall submit modifications that include both Table B.6.5-2 Domestic Serving Wire Center to Point of Presence Relationship and Table B.3.2.1-1 Domestic Broadband DSL Access Prices (MRC) whenever the contractor submits pricing for SWCs it does not have on contract for Broadband DSL Access.

**C.3.2.2.11 Step 12: Support Transition at Contract Expiration**

When this contract is nearing expiration, GSA will begin planning for transitioning services to a follow-on vehicle to ensure service continuity. In support of that planning, the contractors will provide information to and coordinate with the Government to ensure no services are abandoned, expiring services are disconnected and billing terminated, and the Government has accurate and current data to make decisions on how to configure, enhance, or optimize services for the future contract.

ID Number	Description
1	The contractor shall provide requesting Agencies with traffic and utilization reports in accordance with Section C.3.3, Service Management.
2	The contractor shall provide the Government with accurate and current inventories of services in accordance with Section C.3.8, Inventory Management
3	The contractor shall disconnect services and terminate billing within service level intervals, following procedures in Section C.3.5, Service Ordering and terms in Attachment J.12.3, Service Provisioning Intervals.

**C.3.2.3 Program Management Data Requirements**

**C.3.2.3.1 GSA Data Provided to Contractors**

**C.3.2.3.1.1 GSA Program Contacts**

GSA will provide the contractor with the names of contacts within the PMO, the COR, and the customer service representative.

**C.3.2.3.1.1.1 Frequency – GSA Program Contacts**

- i. Initial: At Notice to Proceed
- j. Updated: As changes occur

**C.3.2.3.1.1.2 Media/Transport/Format – GSA Program Contacts**

Data		
Media	Transport	Data Format
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other unsecured transport methods as mutually agreed between GSA and</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed</li> </ul>

Data		
Media	Transport	Data Format
	contractor	Record <ul style="list-style-type: none"> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

### C.3.2.3.1.1.3 Record Elements – GSA Program Contacts

ID Number	Data Elements	Description
1	Name	Name of GSA employee or agent
2	Office Phone	Business phone number
3	E-mail Address	Business e-mail address
4	Facsimile Number	Business facsimile number
5	Mobile Phone	Cellular phone or device number (optional)

### C.3.2.3.2 Agency Data Provided to Contractors

#### C.3.2.3.2.1 Agency Network Management Contact

The Agency will provide the contractor with points of contact for the program.

##### C.3.2.3.2.1.1 Frequency - Agency Network Management Contacts

- Initial: At Agency's Selection of Contractor
- Updated As changes occur

##### C.3.2.3.2.1.2 Media/Transport/Format – Agency Network Management Contacts

The Agency will provide and deliver the Agency Network Management Contacts to the contractor in accordance with the procedures and in any of the media, transport, and format types described in the Data table in Section C.3.1.2, Data and Report Requirements.

##### C.3.2.3.2.1.3 Record Elements – Agency Network Management Contacts

ID Number	Data Elements	Description
1	Name	Agency Network Management Contact's Name
2	Office Phone	Business phone number
3	E-mail Address	Business e-mail address
4	Fax Number	Business fax number
5	Mobile Phone	Cellular phone or device number (optional)
6	Agency Name	Name of Agency or Sub-Agency

### C.3.2.3.3 Contractor Provided Data to GSA

#### C.3.2.3.3.1 Contractor Points of Contact List for GSA

The contractor shall provide the contractor Points of Contact for GSA, in accordance with C.3.2.2, Functional Requirements. The contractor shall mark changes to the contractor Points of Contact list in each update.

**C.3.2.3.3.1.1 Frequency – Contractor Points of Contact List for GSA**

- Initial: Within 15 business days of Notice to Proceed
- Updated: Within 5 days after changes are made

**C.3.2.3.3.1.2 Deliver To - Contractor Points of Contact List for GSA**

- Contractor's Network public website (all information required in Section C.3.2.3.3.1.4 except information regarding the POC's security clearance).
- GSA COR

**C.3.2.3.3.1.3 Media/Transport/Format – Contractor Points of Contact List for GSA**

Data		
Media	Transport	Data Format
File Server	Internet Hypertext Transfer Protocol (HTTP)	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.2.3.3.1.4 Record Elements – Contractor Points of Contact List for GSA**

ID Number	Data Elements	Description
1	Name	Employee's or Subcontractor's Name
2	Completed Investigation	List whether national Agency check or background investigation has been completed; if none, indicate "None"
3	Security Clearance	Active Security Clearance, if any; if none, indicate "None"
4	Office Phone	Business phone number
5	E-mail Address	Business e-mail address
6	Role	Description of role and responsibilities on the Network program
7	Facsimile Number	Office facsimile number
8	Address	Business Mailing Address

**C.3.2.3.4 Contractor Data Provided to Agency**

**C.3.2.3.4.1 Contractor Points of Contact List for Agency**

The contractor provides the contractor Points of Contact (POCs) for the Agencies, in accordance with C.3.2.2, Functional Requirements. The contractor shall mark changes to the contractor POC list in each update. If POCs are the same as those for GSA, the contractor may provide the Agency a link or URL for that list on the contractor's Network public website.

**C.3.2.3.4.1.1 Frequency – Contractor Points of Contact List for Agency**

- Initial: Within 15 days after Agency's selection of contractor
- Updated: Within 5 days after changes are made

**C.3.2.3.4.1.2 Deliver To - Contractor Points of Contact List for Agency**

- To be designated by Agency after Agency's selection of contractor

- Contractor's Network public website

**C.3.2.3.4.1.3 Media/Transport/Format – Contractor Points of Contact List for Agency**

The contractor shall provide and deliver the contractor Points of Contact List to the Agencies in accordance with the procedures and in any of the media, transport, and format types described in the Data table in Section C.3.1.2, Data and Report Requirements.

**C.3.2.3.4.1.4 Record Elements – Contractor Points of Contact List for Agency**

ID Number	Data Elements	Description
1	Name	Employee's Name
2	Completed Investigation	List whether national Agency check or background investigation has been completed; if none, indicate "None"
3	Security Clearance	Active Security Clearance, if any; if none, indicate "None"
4	Office Phone	Business phone number
5	E-mail Address	Business e-mail address
6	Role	Description of role and responsibilities on the Network program
7	Facsimile Number	Office facsimile number
8	Address	Business Mailing Address
9	Contractor Name	Prime, and Subcontractor, if appropriate

**C.3.2.4 Program Management Report Requirements**

**C.3.2.4.1 Contractor Reports Provided to GSA**

**C.3.2.4.1.1 Program Management Plan (PMP)**

**C.3.2.4.1.1.1 Frequency – PMP**

- Initial: Included at Contract Award
- Revised: Reply within 15 business days after receiving GSA comments, or if no comments, within 15 days after Notice to Proceed
- Updated: Annually, 30 business days after the end of each contract year

**C.3.2.4.1.1.2 Deliver To – PMP**

- GSA COR
- GSA CO

**C.3.2.4.1.1.3 Media/Transport/Format – PMP\***

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Other secured or unsecured transport</li> </ul>	



Report		
Media	Transport	File Format
	methods as mutually agreed between GSA and contractor	
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

\*Media type changes per section C.3.1.2

#### C.3.2.4.1.1.4 Content – PMP

ID Number	Information Elements	Description
1	Title	Program Management Plan
2	Contractor	Name of contractor
3	Date	Date of Report
4	Length	100 pages or fewer
5	Contents	Program Management information required in Section C.3.2.2.1 and Section C.3.2.2.2: Summary of Customer Requirements Summary Description of Service Solution Project Plan for Program Management Activities Resource Plan Quality Assurance Plan Technology Plan Communication Plan Subcontractor Management and Vendor/Carrier Relations Organizational Structure Risk Management Plan Information Systems

#### C.3.2.4.1.2 Policies and Procedures (P&P)

The contractor's P&P may, at the contractor's discretion, be delivered in separate volumes. The contractor's P&P shall, if delivered in volumes, be clearly marked and referenced so as to create a single document set.

##### C.3.2.4.1.2.1 Frequency – P&P

1. Initial: Included at contract award
2. Revised: Reply within 15 business days after receiving GSA comment. If no comments are received, within 15 business days of Notice to Proceed
3. Updated: Semi-annually, 30 business days after the end of each period

##### C.3.2.4.1.2.2 Deliver To – P&P

4. GSA COR

##### C.3.2.4.1.2.3 Media/Transport/Format – P&P

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97</li> </ul>

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>Postal Service</li> </ul>	through2003
Magnetic Tape	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through</li> <li>PDF</li> <li>ASCII Text</li> <li>HTML</li> <li>Visio 2000</li> <li>Power Point 2000</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
File Server	<ul style="list-style-type: none"> <li>Internet File Transfer Protocol (FTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>Visio 2000</li> <li>Power Point 2000</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>Flow charts in Visio 2000 or MS PowerPoint 2000</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

\*Media type changes per section C.3.1.2

#### C.3.2.4.1.2.4 Content – P&P

ID Number	Information Elements	Description
1	Title	Policies and Procedures
2	Contractor	Name of contractor
3	Date	Date of Report
4	Contents	P&P documentation per Section C.3.2.2.1.4. One-page process diagrams are desired to represent each procedure and text description of each step.

#### C.3.2.4.1.3 Program Monthly Status Report

##### C.3.2.4.1.3.1 Frequency- Program Monthly Status Report

- Initial Format: Included at contract award
- Revised Format: Reply within 15 business days after receiving GSA comment. If no comments are received, within 15 business days of Notice to Proceed
- Initial report: 5 business days after the first complete calendar month
- Updated: 5 business days after the end of each calendar month

##### C.3.2.4.1.3.2 Deliver To – Program Monthly Status Report

- GSA COR
- GSA CO

##### C.3.2.4.1.3.3 Media/Transport/Format - Program Monthly Status Report

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> </ul>

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>Courier</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> </ul>
File Server	<ul style="list-style-type: none"> <li>Internet File Transfer Protocol (FTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

#### C.3.2.4.1.3.4 Content - Program Monthly Status Report

ID Number	Information Elements	Description
1	Title	Program Monthly Status Report
2	Contractor	Name of Contractor
3	Date	Date of Report
4	Contents	Status of Project Plan for Program Management Activities using either a tabular or graphical representation, including bar, GANTT and PERT charts. Status of projects Orders entered and completed Backlog, aging, and pipeline of orders Summary of trouble reports Current risk assessment and mitigation strategies Issues and resolution SLA Compliance Report: list of each SLA by name, required performance target, actual performance for the reported calendar month, and indication of trend from previous report SLA Corrective Actions for any measures failing SLAs Technical accomplishments and plans Sales and marketing calls.

#### C.3.2.4.1.4 Quarterly Program Management Review

##### C.3.2.4.1.4.1 Frequency - Quarterly Program Management Review

- Initial: Within 30 business days after the third complete calendar month
- Updated: 30 business days after the end of each calendar quarter
- Slides: 2 business days prior to presentation
- Content Information may be presented as cumulative for the quarter, with the exception of the SLA Compliance Report, which the contractor shall present as individual months with the trend from previous months and root cause analysis

##### C.3.2.4.1.4.2 Deliver To – Quarterly Program Management Review

- GSA COR
- GSA CO

**C.3.2.4.1.4.3 Media/Transport/Format - Quarterly Program Management Review**

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• MS PowerPoint 2000</li> <li>• PDF</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Oral Presentation	<ul style="list-style-type: none"> <li>• On-site meeting</li> <li>• Video-teleconference</li> <li>• Web-conference</li> <li>• Audio-teleconference</li> </ul>	

**C.3.2.4.1.4.4 Content - Quarterly Program Management Review**

ID Number	Information Elements	Description
1	Title	Quarterly Program Management Review
2	Contractor	Name of contractor
3	Date	Date of Review
4	Contents	Status of Project Plan for Program Management Activities using either a tabular or graphical representation, including bar, GANTT and PERT charts. Status of projects Orders entered and completed Backlog, aging, and pipeline of orders Summary of trouble reports Current risk assessment and mitigation strategies Issues and resolution SLA Compliance Report: list of each SLA by name, required performance target, actual performance for the preceding quarter, and indication of trend from previous report Root Cause Analysis: identification of measures failing SLAs, root cause of the failure, and corrective action to remedy Technical accomplishments and plans Sales and marketing calls.

**C.3.2.4.1.5 Monthly Financial Status Report**

**C.3.2.4.1.5.1 Frequency - Monthly Financial Status Report**

- Initial Format: Included at contract award

- Revised Format: Reply within 15 business days after receiving GSA comment. If no comments are received, within 15 business days of Notice to Proceed
- Initial report: 15 business days after the first complete billing cycle
- Updated: No later than the tenth business day of each calendar month and reflect those charges invoiced during the previous billing cycle.
- Changes: No later than two billing cycles from the date of Government's request for change

**C.3.2.4.1.5.2 Delivery To - Monthly Financial Status Report**

- GSA COR

**C.3.2.4.1.5.3 Media/Transport/Format - Monthly Financial Status Report**

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> </ul>
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.2.4.1.5.4 Content - Monthly Financial Status Report**

ID Number	Information Elements	Data Elements
1	Title	Monthly Financial Status Report
2	Contractor	Name of contractor
3	Date	Date of Report
4	Contents	<p>The total dollar activity (a through d below) for the month shall be broken down by the service types and services as outlined in Section B (Note: the contractor shall update the list of service types and services with proposals for new or improved services or according to any contract action that deletes services from the list.)</p> <p>The total billed charges for all Agencies invoiced during the monthly reporting period (for both centralized and direct</p>

ID Number	Information Elements	Data Elements
		billing accounts) The remaining dollar obligation under the minimum revenue guarantee (MRG) The remaining amount of unspent dollars under the maximum contract dollar limitation. (d) Total billed charges to be reconciled with the minimum revenue guarantee shall not include any GSA management service fee or tax figures.

**C.3.2.4.1.6 User Forums Issues Report**

**C.3.2.4.1.6.1 Frequency - User Forums Issues Report**

- Initial: Within 10 business days of first user forum
- Updated: Monthly, until all items are resolved

**C.3.2.4.1.6.2 Deliver To - User Forums Issues Report**

- GSA COR

**C.3.2.4.1.6.3 Media/Transport/Format - User Forums Issues Report**

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.2.4.1.6.4 Content - User Forums Issues Report**

ID Number	Information Elements	Description
1	Title	User Forums Issues Report
2	Contractor	Name of contractor
3	Date	Date of Report
4	Contents	Issues that were gathered in the previous User Forums and proposed resolutions, where available

**C.3.2.4.2 Contractor Reports Provided to Agency**

**C.3.2.4.2.1 Service Delivery Project Plan (SDPP)**

**C.3.2.4.2.1.1 Frequency – SDPP**

- Initial: As requested by Agency, no later than 30 calendar days prior to the earliest customer want date
- Updated: As requested by Agency, typically weekly or monthly through duration of project

**C.3.2.4.2.1.2 Deliver To – SDPP**

To be designated by the requesting Agency. If not specified, sent to the Agency DAR for the project

**C.3.2.4.2.1.3 Media/Transport/Format – SDPP**

The contractor shall provide and deliver the SDPP to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.2.4.2.2 Content – SDPP**

ID Number	Information Elements	Description
1	Title	Service Delivery Project Plan (SDPP)
2	Contractor	Name of contractor
3	Date	Date of Project Plan
4	Project Identifier	(Required if indicated by the ordering Agency) ASRN, Project Name or Project Number assigned by Agency as identified on the order
5	Description	Description of project, including Agency, scope of services, and approach to delivering services ordered
6	Contents	Tasks, Schedule, Processes, and Resources to Complete Project. Schedule must reflect baseline due dates (Firm Order Commitment dates) agreed to with Agency as well as current schedule dates for the completion of each individual service to each location.

**C.3.2.4.2.3 Agency-Specific SLA Monthly Compliance Report**

**C.3.2.4.2.3.1 Frequency – Agency-Specific SLA Monthly Compliance Report**

- Initial Format: Included at contract award
- Updated Format: within 15 business days after receiving GSA comment. If no comments are received, within 15 business days of Notice to Proceed
- Initial report: 5 business days after the first complete calendar month after Agency requests report
- Updated: 5 business days after the end of each calendar month

**C.3.2.4.2.3.2 Deliver To – Agency-Specific SLA Monthly Compliance Report**

- To be designated by the requesting Agency. If not specified, sent to the Agency DAR

**C.3.2.4.2.3.3 Media/Transport/Format – Agency-Specific SLA Monthly Compliance Report**

The contractor shall provide and deliver the Agency-Specific SLA Monthly Compliance Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.2.4.2.3.4 Content - Agency-Specific SLA Monthly Compliance Report**

ID Number	Information Elements	Description
1	Title	[Name of Agency] SLA Monthly Compliance Report
2	Period	Period covered by report
3	Contractor	Name of contractor
4	Date	Date of Report
5	Contents	List of each SLA by name, required performance target, actual performance, and indication of trend from previous 3 reports Corrective Actions for any measures failing SLAs

**C.3.3 Service Management**

Service Management encompasses the processes, systems, and data required for the contractor to ensure the quality of services delivered to the Government. This section defines network management, security management, and disaster recovery requirements for operational integrity of the contractor’s network infrastructure, from the backbone to the demarcation of service delivery to the customer.

**C.3.3.1 Network Management**

While the contractor is solely responsible for the management, performance, and maintenance of its service offering, GSA and Agencies must have the ability to monitor the contractor service for contract compliance and Agency operational requirements. In addition, GSA must have the ability to ensure that the contractor has in place adequate capabilities to operate and manage the service to the level of performance required by the Government. Furthermore, GSA and Agencies need to be informed of planned and unplanned service impacting events so that proper action is taken as required. NOTE: Land Mobile Radio Service (LMRS) has unique requirements outlined in Section C.2, Technical Requirements, for training, trouble handling, and network management. As such, those portions of the Management and Operations requirements DO NOT apply to LMRS (that is, Sections C.3.3.1, Network Management, C.3.4.2, Trouble and Complaint Handling, and C.3.7, Training).

**C.3.3.1.1 Network Management Process Definition**

**C.3.3.1.1.1 Network Management Process Description**

This section specifies the process by which the contractor will ensure the quality operations of services provided under this contract. Network management addresses all five areas of the International Organization for Standardization (ISO) network management model, including Fault, Configuration, Accounting, Security, and Performance management. The process begins with security management. Through configuration management, the contractor ensures changes to the network are made



under a controlled environment and that the Government users are aware of impacts to them as those changes are made. Accounting and performance management allow for collection and reporting of network data the Government needs for its administration of this Network contract and to optimize network services. Surveillance and repair manages network faults.

**C.3.3.1.1.2 Network Management Process Narrative**

Step Number	Description	Executing Entities
1	The contractor provides network security management.	Contractor
2	The contractor provides notification and coordination with the GSA Network Program Management Office (PMO) and affected Agencies on any network configuration changes.	Contractor
3	The contractor provides network accounting management.	Contractor
4	The contractor provides notification and information regarding faults and troubles as well as electronic, on-line access, with appropriate security controls, to progress status on restoration of faults and troubles.	Contractor
5	The contractor provides access to all available customer performance reporting capabilities.	Contractor
6	The contractor provides an optional service for Network Monitoring and Management	Contractor

**C.3.3.1.2 Network Management Functional Requirements**

**C.3.3.1.2.1 Step 1--Network Security Management**

ID Number	Description
1	The contractor shall provide network security and fraud prevention, detection, and reporting as specified in Section C.3.3.2 security Management

**C.3.3.1.2.2 Step 2-- Configuration Management**

ID Number	Description
1	The contractor shall provide notification to the PMO of any changes to the contractor's network components or configuration when those changes affect or are likely to affect users' services and resources. The change notification shall include at minimum: a high-level description of the configuration change, scheduled change date and time, Network services affected by the change, and impacted Agencies.
2	The contractor shall notify and coordinate with the PMO and affected Agencies regarding planned network maintenance activity for shared facilities supporting the subscribed services that likely could affect users' services.
2.1	The contractor shall notify the PMO and affected Agencies at least 10 business days prior to a scheduled (non-emergency) network configuration change or planned maintenance activity as described in items 1 and 2 above. The Government retains the right to have the contractor reschedule with 5 business days' prior notice when the change or activity impacts only Government customers served under this contract; for changes or activities that impact other customers as well, the contractor shall make best efforts accommodate the Government's request to reschedule.
2.2	The contractor shall open a trouble report for any emergency changes that may

ID Number	Description
	impact network services for which 10 business days notice to the Government is not feasible due to the nature of the emergency.
2.3	The contractor shall notify the PMO and affected Agencies of such emergency events adhering to the same notification requirements of service-affecting faults stipulated in Section C.3.3.1., Network Management.
3	The contractor shall notify the PMO and affected Agencies at least 20 business days prior to the scheduled date of a large-project network change or maintenance activity as described in items 1 and 2 above. Example of a large project is replacement of multiple routers as part of a change in business strategy. The Government retains the right to have the contractor reschedule with 15 business days' notice.
4	The contractor shall perform configuration changes in a standard maintenance window as stated in the contract to minimize service impact to the Government.
5	The contractor shall submit change notices to the PMO and the Network Management Contact for affected Agencies by E-Mail, facsimile, or other mutually agreed method.
6	The contractor shall maintain and provide PMO and Agency Network Management Contacts access to a network configuration database to include contractor facility maps and node geographical information. This database shall enable the Government to assess how network changes may impact services to Agencies.
7	This database shall enable the Government to perform impact analyses on services during outages.

#### C.3.3.1.2.3 Step 3--Accounting Management

ID Number	Description
1	The contractor's network accounting management system shall provide for the generation and distribution of usage data to support the contractor's detection, resolution, and reporting of network fraud, and abuse as well as optimization activity defined in Section C.3.4, Customer Service.
2	The contractor shall provide the Government with ad hoc traffic and usage reports to support the Government's telecommunications planning and avoidance of fraud, waste, and abuse.
3	The contractor shall provide at a minimum Voice Traffic and Data Traffic reports. See Sections C.3.3.1.4.1.3, Voice Traffic Report and C.3.3.1.4.1.4, Data Traffic Report for report requirements.
4	The contractor shall sample the data link at minimum 2 times per hour to capture data link utilization information for Data Traffic Reports.
5	The contractor's network accounting management system shall capture data for all network service components employed to provide service to the SDP. This includes facilities the contractor may lease from other providers to complete service delivery.

#### C.3.3.1.2.4 Step 4--Fault Management

ID Number	Description
1	On a 24x7 basis, the contractor shall detect, prioritize, isolate, diagnose, and repair faults affecting contract services to restore them to meet specifications.
2	On a 24x7 basis, the contractor shall capture, track, analyze, and report faults as trouble reports in a Trouble Management System.
3	The contractor shall log the fault in its Trouble Management System and adhere to the

ID Number	Description
	same reporting requirements as described in Section C.3.4.2, Trouble and Complaint Handling.
4	The contractor shall implement a process for Government-driven escalations as well as contractor-driven escalations to succeeding levels of management when a fault is not resolved within the required performance target or when the Government has indicated dissatisfaction with the way the contractor has handled the issue. Requirements for the contractor's escalation contacts are in Section C.3.2, Program Management.
5	The contractor shall post and make accessible to the Government via its Network Website its documented contacts and procedures for escalating faults.
6	The contractor shall provide the affected Agencies' Network Management Contacts notification of service-affecting faults and updated status of progress on service restoration regarding the service-affecting fault types listed below in item 8.
7	The contractor shall provide the PMO notification of service-affecting faults and updated status of progress on service restoration if such fault impacts, or has the potential of affecting, multiple Agencies.
8	Faults considered to be service-affecting include the following: <ul style="list-style-type: none"> <li>(a) Outages of contractor network switches or facilities</li> <li>(b) Outages causing Agency site impairments and/or isolations from service</li> <li>(c) Faults/failures of other contractor network elements, such as routers and multiplexers</li> <li>(d) Outages/failures of major access facilities</li> <li>(e) Any hazardous condition that has the potential for major service impact (e.g., fire in a node)</li> <li>(f) Network controls initiated by the contractor</li> <li>(g) Outages of services provided by other vendors to the contractor that the contractor has employed to deliver service end-to-end to the Government</li> <li>(h) Failure of network management system that results in loss of visibility to network and telemetry data</li> <li>(i) Failure of one path of a diverse route at OC-3 bandwidth or above</li> <li>(j) Any other event type that, through the duration of the Network contract, the Government determines must be included as a service-affecting fault and for which mutual agreement for implementation and monitoring has been reached with the contractor</li> </ul>
9	The service-affecting fault information shall contain, at minimum, the following types of data: <ul style="list-style-type: none"> <li>• Trouble tracking number</li> <li>• Fault description and definition of problem</li> <li>• Fault date and detected time</li> <li>• Identification of Agencies affected by the fault</li> <li>• Network service(s) and locations affected by the fault</li> <li>• Information about detection of Network service-affecting faults for peripheral network resources indicating whether the fault is internal or external to the contractor's network.</li> <li>• Estimated time to resolve, if known</li> <li>• TSP or Non-TSP service</li> <li>• Critical or Routine service level</li> </ul>
10	The contractor shall provide the PMO and impacted Agencies' Network Management Contact with E-Mail or telephonic notification within 15 minutes upon service-affecting fault detection and isolation.
11	The contractor shall post notifications and progress status of service-affecting faults on the restricted area of its Network services Website.

**GS00T07NSD0038**  
**Modification No. PS661**

ID Number	Description
12	The contractor shall enable the Government to view Network service-affecting faults notifications and progress status from the PMO and at subscribing Agencies using a Web browser.
13	The contractor shall implement appropriate security and access controls so that only authorized personnel can view notifications and progress status information on service-affecting faults.
14	The contractor shall provide the PMO the capability to view information on all service-affecting faults.
15	The contractor shall restrict the Agencies to be able to view only data that provides information on impacts to their service(s).
16	The contractor shall update progress status information every 30 minutes until the service-affecting fault is resolved.
17	The contractor shall post the date and time-to-restore as the last progress status update on the service-affecting fault.
18	The contractor shall keep the final status update of a service-affecting fault on line for at least 24 hours.
19	The contractor shall resolve 90% of all monthly service outages that do not require dispatching of personnel within 4 hours as measured at the Agency level, that is, 90% of all service outages that affect a particular customer Agency during the month. This aggregate level monthly performance metric for resolution is intended to be independent and complement, but not replace, the incident level performance target as defined in ID # 22 below.
20	The contractor shall resolve 90% of all monthly service outages that require dispatching of personnel within 8 hours as measured at the Agency level. This aggregate level monthly performance metric for resolution is intended to be independent and complement, but not replace, the incident level performance target as defined in ID # 23 below.
21	The contractor shall calculate Time to Restore (TTR) as the elapsed time between the time a service outage is recorded in the Trouble Management System and the time the service is restored minus any (1) time due to scheduled network configuration change or planned maintenance or (2) time, as agreed to by the Government, that the service restoration of the service cannot be worked due to Government caused delays. Examples of Government caused delays include: 1) the customer was not available to allow the contractor to access the Service Delivery Point or other customer-controlled space or interface; 2) the customer gave the contractor an incorrect address for the SDP; 3) the customer failed to inform the contractor that a security clearance was required to access the SDP or customer-controlled space; 4) or the Government required service at a remote site and agreed that a longer transit time was required.
22	The contractor shall resolve each service outage for any Network service within 4 hours for restoration not requiring dispatching of personnel. See Attachment J.13.4, for Service Level Agreements associated with service outage incidents.
23	The contractor shall resolve each service outage for any Network service within 8 hours for restoration requiring dispatching of personnel except for non-domestic SDPs. See Attachment J.13.4, for Service Level Agreements associated with service outage incidents.
24	The contractor shall produce and deliver to the PMO and customer Agencies a monthly Trouble Management Performance Summary report for the calendar month that itemizes trouble management performance by Agency and by service within an Agency, and includes a grand total for all services within an Agency. See Section C.3.3.1.4.1.1, Trouble Management Performance Summary Report for report requirements.
25	The contractor shall produce and deliver to the PMO and customer Agencies a monthly

ID Number	Description
	Trouble Management Incident Performance report that itemizes by Agency each trouble report for service outage that failed to meet service restoration SLA as defined in this table and in Attachment J.13, Service Level Agreements. See Section C.3.3.1.4.1.2, Trouble Management Incident Performance Report for report requirements.

**C.3.3.1.2.5 Step 5--Performance Management**

GSA will manage the contractor's performance through reports provided by the contractor as well as through the Government's own records.

ID Number	Description
1	The contractor shall deliver reports of performance against requirements defined throughout Section C, in accordance with instructions in Sections C.2, Technical Requirements, and C.3, Management and Operations.
2	Any credits associated with performance that does not meet requirements are established in Section H, Type and Terms of Contract.
3	The contractor shall provide the PMO and all subscribing Agencies with access to all available customer performance reporting capabilities for subscribed services on the same basis (that is, means of delivery, frequency, and content) that they are available to other customers.
4	For subscribing Agencies, the contractor shall make only the information applicable to that Agency available to that Agency.

**C.3.3.1.2.6 Step 6 -- Network Services Monitoring and Management**

Network Services Monitoring and Management is an optional capability, provided at additional cost to an Agency (see Section B.6.4) who requires real-time performance information related to the health of the contractor's services for which the subscribing Agency has selected this optional capability.

The contractor shall also provide real time informational updates on the status of particular problem resolution efforts as a product of interfaces to the contractor's Trouble Management System. These updates will provide information appropriate to the service, such as test results (e.g. trace route, latency, bit error rate, and ping), technician log entries, and current status, from within the contractor's Trouble Management System.

ID Number	Description
1	The contractor shall provide a Network Services Monitoring and Management capability to provide real-time information regarding the health of the contractor's network as it applies specifically to the services the Agency has selected for this option.
2	The contractor shall provide a Network Services Monitoring and Management capability to provide real time informational updates of the status of problem resolution efforts within the contractor's Trouble Management System as it applies specifically to the services for which the Agency has selected this option.
3	The contractor shall provide additional hardware, software, and other means of access as determined by the contractor to provide this capability.
4	In the Network Services Monitoring and Management capability, the contractor shall provide information that includes its measurement of KPIs described in Section C.2 (Technical Requirements) for each service for which the Agency has selected this

ID Number	Description
	option.
5	In the Network Services Monitoring and Management capability, the contractor shall provide the Agency the capability to conduct its own measurement of KPIs described in Section C.2 (Technical Requirements) for each service for which the Agency has selected this option.
6	The contractor shall restrict Agency's access to information within the Network Monitoring and Management capability to only the information that applies to the Agency's own selected services.

**C.3.3.1.3 Network Management Data Requirements**

None

**C.3.3.1.4 Network Management Report Requirements**

**C.3.3.1.4.1 Contractor Reports Provided to Government**

**C.3.3.1.4.1.1 Trouble Management Performance Summary Report**

For reports sent to GSA, the contractor shall include data for all customer Agencies and shall produce and deliver the Trouble Management Performance Summary report to GSA according to the frequency, media, transport, file format and content as specified in this section.

For reports sent to the Agencies, the contractor shall include only Agency-specific data. The contractor shall generate and deliver the Trouble Management Performance Summary report to Agencies according to the frequency, media, transport, file format and content as specified in this section.

**C.3.3.1.4.1.1.1 Frequency - Trouble Management Performance Summary Report**

- Initial:
  - Sent to GSA: Within 15 business days from the end of the first calendar month in which a SOCN is delivered
  - Sent to Agency: Within 15 business days after end of calendar month in which Agency requests report and first SOCN is delivered
- Updated:
  - Monthly within 15 business days after end of calendar month

**C.3.3.1.4.1.1.2 Deliver To –Trouble Management Performance Summary Report**

- GSA COR
- Agency Network Management Contract or as determined by each Agency

**C.3.3.1.4.1.1.3 Media/Transport/Format –Trouble Management Performance Summary Report**

**C.3.3.1.4.1.1.3.1 Media/Transport/Format –Trouble Management Performance Summary Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Excel 97 through 2003</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.1.4.1.1.3.2 Media/Transport/Format –Trouble Management Performance Summary Report sent to Agency**

The contractor shall provide and deliver the Agency Trouble Management Performance Summary report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements

**C.3.3.1.4.1.1.4 Content –Trouble Management Performance Summary Report**

The contractor shall include in the Trouble Management Performance Summary report at minimum the information described in the table below.

ID Number	Information Elements	Description
1	Report Title	Trouble Management Performance Summary
2	Agency and Agency hierarchy code	Name of Government Agency/entity and Agency hierarchy code to which service is being provided.
3	Reporting Period	The period covered by the report.
4	Service	Service provided to the Agency.
5	Non-Dispatch Services Trouble Reports Created	Total number of Non-Dispatch trouble reports opened during the reporting period by an Agency or the contractor for service outages by service.
6	Non-Dispatch Services Trouble Reports Resolved w/in 4 Hours	Total number of Non-Dispatch trouble reports resolved and closed within 4 hours during the reporting period for service outages by service.
7	% Non-Dispatch Services Trouble Reports Resolved w/in 4 Hours	Percent of Non-Dispatch trouble reports resolved and close within 4 hours during the reporting period by service.
8	Dispatch Services Trouble Reports Created	Total number of Dispatch trouble reports opened during the reporting period by an Agency or the contractor for service outages by service .
9	Dispatch Services Trouble Reports Resolved w/in 8 Hours	Total number of Dispatch trouble reports resolved and closed within 8 hours during the reporting period for service outages by service.
10	% Dispatch Services Trouble Reports Resolved w/in 8 Hours	Percent of Dispatch services fault/trouble reports resolved and close within 8 hours during the reporting period by service.
11	Total Non-Dispatch Services Trouble	Total number of Non-Dispatch trouble reports opened during the reporting period by an Agency or the contractor for service

ID Number	Information Elements	Description
	Reports Created	outages for all services.
12	Total Non-Dispatch Services Trouble Reports Resolved w/in 4 Hours	Total number of Non-Dispatch trouble reports resolved and closed within 4 hours during the reporting period for service outages for all services.
13	% of Total Non-Dispatch Services Trouble Reports Resolved w/in 4 Hours	Percent of Non-Dispatch trouble reports resolved and close within 4 hours during the reporting period for service outages for all services.
14	Total Dispatch Services Trouble Reports Created	Total number of Dispatch trouble reports opened during the reporting period by an Agency or the contractor for service outages for all services.
15	Total Dispatch Services Trouble Reports Resolved w/in 8 Hours	Total number of Dispatch trouble reports resolved and closed within 8 hours during the reporting period for service outages for all services.
16	% of Total Dispatch Services Trouble Reports Resolved w/in 8 Hours	Percent of Dispatch trouble reports resolved and close within 8 hours during the reporting period for service outages for all services.
17	Contractor	Contractor's Name

**C.3.3.1.4.1.2 Trouble Management Incident Performance Report**

The contractor shall include data for all customer Agencies and shall produce and deliver the Trouble Management Incident Performance report to GSA and Agencies according to the frequency, media, transport, file format and content as specified in this section.

**C.3.3.1.4.1.2.1 Frequency - Trouble Management Incident Performance Report**

- Initial:
- Sent to GSA: Within 15 business days from the end of the first calendar month in which a SOCN is delivered
- Sent to Agency: Within 15 business days after end of calendar month in which Agency requests report
- Updated:
- Monthly within 15 business days after end of calendar month

**C.3.3.1.4.1.2.2 Deliver To –Trouble Management Incident Performance Report**

- GSA COR
- Agency

**C.3.3.1.4.1.2.3 Media/Transport/Format – Trouble Management Incident Performance Report**

**C.3.3.1.4.1.2.3.1 Media/Transport/Format –Trouble Management Incident Performance Report sent to GSA**



Report		
Media	Transport	File Format
E-mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Excel 97 through 2003</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.1.4.1.2.3.2 Media/Transport/Format – Trouble Management Incident Performance Report sent to Agency**

The contractor shall provide and deliver the Agency Trouble Management Incident Performance Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.3.1.4.1.2.4 Content – Trouble Management Incident Performance Report**

The contractor shall include in the Trouble Management Incident Performance report, at minimum, the information described in the table below.

ID Number	Information Elements	Description (repeat for each Service Outage that failed the SLA)
1	Report Title	Trouble Management Incident Performance
2	Agency and Agency hierarchy code	Name of Government Agency/entity and Agency Hierarchy Code to which service is being provided.
3	Reporting Period	The period covered by the report.
4	Trouble Tracking Number	Identifier that uniquely identifies the trouble report within the contractor's trouble management system.
5	Service Level Category	Either "Routine" or "Critical" based on the service level that was ordered by the customer Agency.
6	Services Category	Service that was affected by the service outage.
7	UBI	Unique Billing Identifier
8	Date/Time Trouble Report Opened	Date and time the trouble report was opened.
9	Date/Time Trouble Resolved	Date and time the service outage was cleared and service restored.
10	Total Time to Restore	Total duration of the service outage, in hours and fraction of hours.
11	Contractor	Contractor's Name
12	Dispatch Required	(Yes or no) Indication of whether dispatch was required to restore service

**C.3.3.1.4.1.3 Voice Traffic Report**

The contractor shall summarize all daily voice traffic and shall produce and deliver the GSA Voice Traffic report according to the frequency, media, transport, file format and content as specified in this section.

**C.3.3.1.4.1.3.1 Frequency - Voice Traffic Report**

- GSA Report: When requested by the PMO, not to exceed two times per Government fiscal year

- Agency Report: When requested by the Agency, not to exceed twelve times per Government fiscal year per Agency

**C.3.3.1.4.1.3.2 Deliver To –Voice Traffic Report**

- GSA COR
- Agency

**C.3.3.1.4.1.3.3 Media/Transport/Format –Voice Traffic Report**

**C.3.3.1.4.1.3.3.1 Media/Transport/Format –Voice Traffic Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Excel 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.1.4.1.3.3.2 Media/Transport/Format –Voice Traffic Report sent to Agency**

The contractor shall provide and deliver the requesting Agency's Voice Traffic Report in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.3.1.4.1.3.4 Content -- Voice Traffic Report**

The contractor shall include in the Voice Traffic report at minimum the information described in the table below.

ID Number	Information Elements	Description
1	Report Title	Voice Traffic
2	Trunk Group ID or as requested by Agency	Character string that uniquely identifies the trunk group for which the daily data is summarized.
3	Date	Day for which the data is summarized.
4	Incoming Attempts	Total number of incoming calls that were attempted on the particular day.
5	Outgoing Attempts	Total number of outgoing calls that were attempted on the particular day.
6	Incoming Abandoned	Total number of incoming calls that were abandoned on the particular day.
7	Failure Count	Total number of calls that failed on the particular day.
8	Total Minutes	Total number of minutes that the trunk group was utilized on the particular day.
9	Total Outgoing Answered	Total number of outgoing call that were answered.
10	Percent Answered	Percent of outgoing calls that were answered.
11	Busy Calls	Total number of daily busy calls.
12	Busy Hour Traffic	The amount of traffic in the trunk group during the Busy Hour (the busiest, one-hour period in the day) represented in call

ID Number	Information Elements	Description
		minutes.

**C.3.3.1.4.1.4 Data Traffic Report**

The contractor shall produce a Data Traffic report that summarizes Agency specific daily data network traffic. The contractor shall produce and deliver the Data Traffic report according to the frequency, media, transport, file format and content as specified in this section

**C.3.3.1.4.1.4.1 Frequency - Data Traffic Report**

- GSA Report: When requested specifically by the PMO, not to exceed two times per Government fiscal year
- Agency Report: When requested by the Agency, not to exceed twelve times per Government fiscal year per Agency

**C.3.3.1.4.1.4.2 Deliver To – Data Traffic Report**

- GSA COR
- Agency

**C.3.3.1.4.1.4.3 Media/Transport/Format – Data Traffic Report**

**C.3.3.1.4.1.4.3.1 Media/Transport/Format – Data Traffic Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Excel 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.1.4.1.4.3.2 Media/Transport/Format – Data Traffic Report sent to Agency**

The contractor shall provide and deliver the requesting Agency's Data Traffic Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.3.1.4.1.4.4 Content GSA Data Traffic Report**

The contractor shall include in the Data Traffic report at minimum the information described in the table below.

ID Number	Information Elements	Description
1	Report Title	Data Traffic

ID Number	Information Elements	Description
2	Data Link Connection Identifier or similar as appropriate to the service and as requested by the Agency	A data link identifier that identifies the particular data link for which the daily data is summarized.
3	Date	Day for which the daily data is summarized.
4	Peak utilization	Utilization rate of the highest sample taken during the day.
5	Average Peak Hourly Utilization	Utilization rate for the hour in the day that had the highest average utilization rate of all samples taken during that hour.

### C.3.3.2 Security Management

Services under this contract will carry non-sensitive programmatic and administrative traffic, Sensitive but Unclassified (SBU) traffic, and higher levels of sensitive and/or classified traffic that has been encrypted, either by Agency users or by the contractor, for a fee, at Agency request. Therefore, the contractor is required to follow Federal Government generally accepted security principles and practices or better, and to employ adequate and reasonable means to ensure and protect the integrity, confidentiality, and availability of Networx services, OSS, and Government information transported or stored in the contractor's Networx services infrastructure.

#### C.3.3.2.1 Security Management Process Definition

The Security Management process entails the steps and activities required to ensure that Government security requirements and needs are met; to ensure and maintain the confidentiality, integrity, and availability of Networx services, information, and operational support systems; and to prevent fraudulent use of Networx services.

##### C.3.3.2.1.1 Security Management Process Narrative

Step Number	Description	Executing Entities
1	The contractor maintains and implements a Security Plan that meets Government security requirements.	Contractor
2	The contractor conducts a yearly risk analysis and produces a Security Risks Assessment Report that identifies security vulnerabilities and risks and defines steps that the contractor will take to mitigate identified security risks.	Contractor
3	The contractor implements security risk mitigation measures defined in the Networx Risks Assessment Report.	Contractor
4	The contractor implements information security policies, procedures, and capabilities that meet Government information security requirements.	Contractor
5	The contractor implements information assurance policies, procedures, and capabilities that meet Government information assurance requirements.	Contractor
6	The contractor implements policies, processes, procedures, systems, and other capabilities to prevent and detect security violations, and to notify the Government of suspected or actual security breaches.	Contractor

Step Number	Description	Executing Entities
7	The contractor logs alarms and security breach events and makes this information available to the Government when requested.	Contractor
8	The contractor obtains personnel and facilities clearances as requested by the Government.	Contractor
9	The contractor protects its facilities against unauthorized access.	Contractor
10	The contractor establishes security procedures and provides such procedures to the Government.	Contractor
11	The contractor performs on-going security refreshments.	Contractor
12	The contractor implements and manages security of non-domestic services.	Contractor
13	The contractor proactively develops and implements methods to prevent and detect fraudulent use of Network services.	Contractor

### C.3.3.2.2 Security Management Functional Requirements

#### C.3.3.2.2.1 Step 1--Security Plan

ID Number	Description
1	A Security Plan shall be included in the contract at award and updated annually.
2	The contractor's Security Plan shall describe in detail how the contractor shall satisfy the security requirements as identified in Sections C.3.3.2, Security Management, and all its subsections, including how improved security-related processes and technologies are to be incorporated into the contract as they become commercially available. See Section C.3.3.2.4.2.1, Security Plan and Risks Assessment for report requirements.
3	The contractor's Security Plan shall include a description of the approach, scope, and methodology of Network services security risk analyses that shall be undertaken by the contractor throughout the life of the contract. See Section C.3.3.2.2.2, Security Risk Analysis.
4	The contractor's Security Plan shall comply with the requirements of Section C.2.1.11, Network Security
5	The contractor shall describe in the Security Plan its Network security management organization, and how it will interface and coordinate with suppliers, vendors, partners, and Government to address Network security related matters.
6	The contractor shall describe in the Security Plan the management, technical and operational controls as defined in NIST SP 800-18 that will be employed to ensure the integrity, confidentiality, and availability of Government information and data that is transported and/or stored by Network services, Network OSS, databases, or handled manually at contractor's facilities.
7	The contractor shall describe in the Security Plan how it will communicate and educate its employees, vendors, and Government users its Network security policies, practices, and procedures, and how it plans to develop and maintain overall security awareness among Network stakeholders.
8	Upon PMO approval, the contractor shall implement the Security Plan.
9	The contractor shall adhere to Federal Government accepted security principles and practices, or better, as defined in NIST Special Publication 800-14 in addressing all security requirements in Section C.3.3.2, Security Management.

#### C.3.3.2.2.2 Step 2--Security Risk Analysis

ID Number	Description
-----------	-------------

ID Number	Description
1	The contractor shall conduct a yearly security risk analysis, making a good faith effort to identify all risks regardless of severity, and shall prepare and submit to the Government for approval a Security Risks Assessment Report describing the results of such analysis. See Section C.3.3.2.4.2.1, Security Plan and Risks Assessment for report requirements.
2	The contractor shall address and include in the yearly security risk analysis all aspects of security, including but not limited to those described within the entirety of Section C.3.3.2, Security Management
3	The contractor shall assess and include as part of the yearly security risk analysis security vulnerabilities of all Networx services as they pertain to confidentiality of the services and Government information that may be stored or transported by such services
4	The contractor shall assess and include as part of the yearly security risk analysis security vulnerabilities of all Networx services as they pertain to integrity of the services and Government information that may be stored or transported by such services.
5	The contractor shall assess and include as part of the yearly security risk analysis security vulnerabilities of all Networx services as they pertain to availability of the services and Government information that may be stored or transported by such services.
6	The contractor shall assess and include as part of the yearly security risk analysis security vulnerabilities of all Networx OSS as they pertain to confidentiality of the OSS and Government information that may be stored and made available by the OSS.
7	The contractor shall assess and include as part of the yearly security risk analysis security vulnerabilities of all Networx OSS as they pertain to integrity of the OSS and Government information that may be stored and made available by the OSS.
8	The contractor shall assess and include as part of the yearly security risk analysis security vulnerabilities of all Networx OSS as they pertain to availability of the OSS and Government information that may be stored and made available by the OSS.
9	The contractor shall adhere to NIST SP 800-30 guidelines and include in the yearly Security Risks Assessment Report at a minimum a description of threats, security vulnerabilities identified and their associated risks, likelihood that the risks will occur, impact of the risks to the Government, severity of the risks, mitigation strategy, and commercially reasonable measures that the contractor will take to mitigate the risks.
10	The contractor shall categorize risk severity based on the potential impact that the security risk has to the Government as defined on "Potential Impact" categorization described in the latest issue, updates, and amendments of the Federal Information Processing Standards (FIPS) Publication 199, at the time the risk analysis is conducted.

### C.3.3.2.2.3 Step 3--Security Risk Mitigation

ID Number	Description
1	The contractor shall implement, within 60 calendar days of PMO approval of the yearly Security Risk Assessment Report, the risk mitigation measures identified in the yearly Security Risk Assessment Report.
2	If the contractor determines that it will take more than 60 days to implement risk mitigation measures identified in the Security Risk Assessment Report, the contractor shall notify the PMO and request, in writing with appropriate justification, an extension. The Government reserves the right to deny an extension.
3	The contractor shall implement any additional measures that the PMO determines are

ID Number	Description
	required to mitigate security risks of the Network services and OSS, that are above and beyond Federal Government accepted security principles and practices per NIST SP 800-14, as mutually agreed with the contractor.
4	The contractor shall provide the PMO with evidence that all risk mitigation measures were taken and the risks have been reduced or eliminated.

**C.3.3.2.2.4 Step 4--Information Security**

ID Number	Description
1	The contractor shall provide protection consistent with Federal Government accepted security principles and practices per NIST SP 800-14, or better, of Government information, including confidentiality, data integrity, and authentication for all its Network services.
2	The contractor shall support the Government to comply with FISMA requirements, in accordance with National Institute of Standards (NIST), Federal Information Processing Standards (FIPS) Publication 199 , <i>Standards for the Security Categorization of Federal Information and Information System</i> , FIPS Publication 200, <i>Security Controls for Federal Information and Information System</i> and related NIST Special Publications 800 series, as applicable, and any updates and amendments to these documents at contract award, in securing Network services, Network services OSS, and any contractor premises information system that stores Government related information (e.g., inventory, billing, etc.).
3	All contractor's systems that store Government related information shall comply with all security controls specified in SP 800-53, Annex 1, and in Section C.3, Management and Operations. In addition, the contractor shall implement any additional security controls ordered by individual Government Agencies under the Network contract (e.g, ordered via Customer Specific Design and Engineering Services).
4	The contractor shall ensure confidentiality of data. The contractor shall follow Federal Government-accepted security principles and practices per NIST SP 800-14, or better, to protect Government information in the contractor's infrastructure from disclosure to unauthorized persons. This protection shall include, but not be limited to, sensitive information maintained in the network such as subscriber profiles, billing data, inventory data, network performance statistics, Agency network configuration data, and network vulnerabilities.
5	For some Network services, subscribers may use Government equipment for encryption of user information. The contractor's infrastructure shall support the transmission of all encrypted information that is generated by the Government equipment in a transparent manner, when such equipment meets the Network service specific interface requirements.
6	The contractor shall ensure data integrity. The contractor shall protect the Government information from unauthorized modification while contained within the contractor's infrastructure.
7	The contractor shall ensure identification and authentication of personnel involved in the operation and management of Network services. The contractor shall identify and authenticate contractor personnel and Government personnel who are authorized to place orders or to access network management information.
8	The contractor shall protect its infrastructure from any information threats or attacks (e.g., threats from hackers, criminals, and terrorist activities) carried out by domestic or non-domestic entities including subcontractors.

**C.3.3.2.2.5 Step 5--Information Assurance**

ID Number	Description
1	The contractor shall adhere to Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect the databases, OSS, and information processing systems that are critical for the continuous, reliable operation of its Network services.
2	The contractor shall protect against unauthorized access to these databases, OSS, and information processing systems by entry from external communications devices. Information systems shall include but not be limited to the OSS, audio and video teleconferencing reservation systems, repositories of Agency network configuration, repositories of users' identification and authorization information and Call Detail Records (CDRs).
3	Access Control - The contractor shall provide access controls consistent with Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect its OSS and switching systems from attacks via publicly accessible ports (e.g., maintenance ports). The contractor shall ensure that its access controls provide access to network management or customer-related information only to authorized contractor personnel and Government personnel.
4	Denial of Service - The contractor shall adhere, as applicable, to Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect its transmission facilities, switching components, network management systems and other essential contractor facilities from denial-of-service attacks, intrusions and other perceived threats. Denial of service attacks shall be reported as network security breaches.
5	Implementation of information assurance - The contractor shall describe its protection for information assurance of its databases, OSS, and information systems in its Security Plan
6	The contractor shall include in the Security Plan how technicians' accesses and privileges to network elements and routing policies will be controlled and managed. At a minimum, the contractor shall define network elements security policies, access privileges structure, and what processes, procedures, and mechanisms will be in place to control and manage access to network elements and routing policies by contractor's operators and technicians.
7	The contractor shall provide, within 60 days of Government request, evidence (e.g., test results, evaluations, audits, etc.) that security controls for Network services and OSS as specified in its Security Plan are implemented correctly, operating as intended, and producing the desired outcomes in meeting Government security requirements. The contractor shall provide evidence that is recent, and in no case older than 24 months. If the contractor determines that it will take more than 60 days to provide the requested evidence, the contractor shall notify the PMO and request an extension in writing with appropriate justification.

**C.3.3.2.2.6 Step 6--Notification of Security Breaches**

ID Number	Description
1	The contractor shall take a proactive approach in developing methods to prevent, detect and report security breaches of its network, OSS, and databases.
2	The contractor shall take all prudent measures to detect and prevent security breaches of the Network program.
3	The contractor shall identify all security-related system and network vulnerabilities and take corrective measures to eliminate them, and upon request, advise Agencies how to best deter security breaches when using the contractor's Network services.
4	The contractor shall within 15 minutes of determination notify the PMO, and affected Agencies, of any suspected or actual security violation, including but not limited to



ID Number	Description
	unauthorized intrusions, denial of service attacks, and all other security breaches.
5	The contractor shall immediately (within 15 minutes of determination) notify the PMO and all affected Agencies when a security breach occurs in any of the OSS.
6	The contractor shall report on the results of the investigation and corrective measures applied to the security breach or problem within 4 hours of notifying the PMO and Agencies that a security breach, violation or problem has occurred.
7	The contractor shall verbally notify the PMO or its designated representative, and include as much information about the event as known at that point, and actions being taken to correct the situation. The contractor shall provide updates on the status of this event upon the request of the PMO or its designated representative.
8	The contractor shall provide the PMO and impacted Agencies a written Security Breach Notification Report within seven (7) calendar days after the initial verbal notification of a security breach. See Section C.3.3.2.4.1.3, Security Breach Notification Report for report requirements.
9	The contractor shall provide the PMO and customer Agencies a monthly Security Breach Detection Report. This report shall summarize all incidents as described in steps 1-3 that occur within a calendar month. See Section C.3.3.2.4.1.1, Security Breach Detection Report for report requirements.

#### C.3.3.2.2.7 Step 7--Alarms and Audit Trails

ID Number	Description
1	The contractor shall log all contract services security violations and other security-related events (e.g., attempts to breach security).
2	The contractor shall log all OSS (e.g., Billing, Inventory, Fault Management, etc.) security violations and other security-related events (e.g., attempts to breach security) and transactions.
3	The contractor shall log all Network private Website security violations and other security-related events (e.g., attempts to breach security).
4	The contractor shall log all alarms generated by security monitors, intrusion detection systems, and any other security management capabilities implemented by the contractor for Network services.
5	The contractor shall log all alarms generated by OSS (Billing, Inventory, network management etc.) security monitors, intrusion detection systems, and any other security management capabilities implemented by the contractor.
6	The contractor shall log all alarms generated by Network Website security monitors, intrusion detection systems, and any other security management capabilities implemented by the contractor.
7	The contractor shall maintain all information associated with security violations including the associated reports and alarm information from alarms logs associated with the violation for three years from the date of the incident, or of the report, whichever is later. However, the PMO may request that these records be maintained longer (for a maximum of three additional years) or turned over to the PMO via electronic medium, at no additional cost to the Government.
8	The contractor shall make available all information associated with security violations including the associated reports and alarm information from alarm logs associated with the violation for three years from the date of the incident, or of the report, whichever is later. However, the PMO may request that these records be made available longer (for a maximum of three additional years) at no additional cost to the Government.
9	The contractor shall provide and maintain real-time operational procedures and capability for detecting and monitoring suspected abuse or intrusions to the network and set off alarms for those events that require immediate attention by PMO, affected

ID Number	Description
	Agency or site, and/or contractor staff.
10	The contractor shall provide these procedures to the PMO within 60 calendar days after Notice to Proceed with updates as requested by the Government.

**C.3.3.2.2.8 Step 8--Personnel Security**

ID Number	Description
1	The contractor shall initiate requests for background investigations of personnel, as identified by the Government, requiring national Agency checks. Failure to secure the proper clearances for personnel within a reasonable amount of time (as determined by the Government based on recent similar requests) may result in delays in or inability to perform in accordance with the contract.
2	Performance under the contract(s) may require the contractor to have access to information classified up to and including "Top Secret." Therefore, upon award and as requested by the Government, the contractor shall obtain and maintain the appropriate background investigations as well as personnel and facility clearances to have access to and custody of such information. The GSA or respective agency CO will initiate and coordinate the appropriate background investigation process.
3	Specific guidance applicable to services provided under the Networkx contracts will be coordinated by the awarding contracting officer. This may be provided in the form of a Department of Defense Contract Security Classification Specification (DD Form 254) for clearance requirements or other agency specific directives, policies and procedures as identified under each associated service requirement.
4	The contractor shall take actions to ensure the proper paperwork is received for processing within 30 calendar days, according to the OPM instructions, or the Government may terminate the contract.

**C.3.3.2.2.9 Step 9 -- Physical Security**

ID Number	Description
1	The contractor shall follow Federal Government accepted security principles and practices per NIST SP 800-14, or better, to safeguard Networkx services related facilities and equipment against sabotage, espionage, damage, and theft corresponding to the critical nature of the facility or equipment to the Networkx Program.
2	The contractor shall physically protect and prevent unauthorized access to Networkx services operations facilities, equipment, material and documents, and any other Networkx related contractor facility and equipment that stores or handles Networkx related information or data.
3	The contractor shall control access to its Networkx services related facilities, equipment, material and documents by employees and visitors via electronic and/or physical methods corresponding to the critical nature of the work being performed, or the sensitive nature of the Government information being handled. Electronic and physical methods of security include, but are not limited to, guards, intrusion detection devices, surveillance cameras, lighting and fencing.
4	The contractor shall protect its Networkx services operations facilities from basic service interruptions such as those caused by electrical outages, flooding, etc.
5	The contractor shall protect its Networkx services operations facilities by meeting fire code regulations specific to the location of the facility.
6	The contractor shall ensure offsite backup and storage of critical Networkx services configuration and OSS data and information generated and stored at its Networkx facilities. Critical data and information is any data or information that is essential for the restoration of services and operation in the event of a disaster that impacts the

ID Number	Description
	contractor's Network facilities or operation.
7	The contractor shall protect its Network services hardware and software from theft or other human threats that may impact the availability of Network services or compromise Government information or data.

**C.3.3.2.2.10 Step 10--Procedural Security**

ID Number	Description
1	The contractor shall establish, and provide to the Government, security procedures, including but not limited to: (a) Procedures for controlling access to Government-related sensitive databases and information (b) Procedures to prevent fraudulent use of Government information or services (c) Procedures to prevent fraudulent use of Network Calling Cards

**C.3.3.2.2.11 Step 11--Ongoing Security Refreshment**

ID Number	Description
1	Following Government approval, the contractor shall incorporate new security-related standards for telecommunications transmission and switching technologies as they mature and become accepted practice in the commercial environment.
2	If these security-related standards are implemented at no additional cost to any commercial customers, the Government shall receive the same treatment.
3	The contractor shall work with the Government on an ongoing basis to certify and enhance the strength of security.
4	Post award activities shall include, but not be limited to: (a) Providing the Government with summaries of security-related events. (b) Working with the Government to reassess the severity of new or perceived threats and to take countermeasures to assure the specified network availability in accordance with the Security Plan. (c) Preparation of security practices and briefings for GSA and Agency representatives and, upon request, conducting the briefings.
5	The contractor shall be proactive in improving the security of the Network services, databases, and OSS, and shall describe in the Security Plan the contractor's approach for keeping apprised of the latest threats, modernizing with the latest trends, methods, and technologies for preventing and detecting security breaches, and improving overall Network security throughout the life of the contract.
6	The contractor shall be proactive in ensuring that security is considered as part of any new deployments or changes to services and OSS, and shall describe in the Security Plan how it will ensure that security is considered and built into new Network services deployments and enhancements, new OSS deployments and enhancements, and Network services and OSS configuration changes.
7	The contractor shall ensure throughout the life of the contract that all Network OSS and service components software have current and up-to-date security updates and patches for all known vulnerabilities.

**C.3.3.2.2.12 Step 12--Non Domestic Services**

ID Number	Description
1	The contractor shall provide the best commercial security practices in supporting service delivery to non-domestic locations.

ID Number	Description
2	The contractor shall monitor the performance of its foreign subcontractors' business partners and Post Telephone and Telegraph (PTT) operating administrations' services and immediately (within 30 minutes of determination) report verbally to the PMO and the Contracting Officer (CO) any unusual or suspicious outage, blockage, or tampering that may indicate that users of services are being denied service or are being compromised.
3	The contractor shall provide the PMO and impacted Agencies a written Non-Domestic Services Security Notification Report within seven (7) calendar days after the initial verbal notification of unusual or suspicious outage or activity. See Section C.3.3.2.4.1.4, Non-Domestic Services Security Notification Report for report requirements.
4	Any connectivity to the Internet or a commercial network service provided by the contractor to non-domestic service delivery locations shall meet the security requirements identified in Section C.3.3.2, Security Management.

#### C.3.3.2.2.13 Step 13--Fraud Prevention Management

ID Number	Description
1	The contractor shall take a proactive approach in developing methods to prevent, detect and report fraudulent use of services, and the contractor shall describe in its Security Plan the approach for modernizing with the latest fraud prevention and detection trends, methods, and technologies and for improving fraud detection and prevention capabilities throughout the life of the contract.
2	The contractor shall take all adequate and prudent measures to detect and prevent fraud abuse related to the Networx program.
3	The contractor shall identify all fraud-related system and network vulnerabilities and take corrective measures to eliminate them, perform message and calling pattern analyses prior to and after billing, investigate annoyance calls, investigate incidents of programmed system and network computers programmed in error, and advise Agencies how to best employ fraud prevention and detection techniques when using the contractor's Networx services..
4	The Government is particularly concerned with potential fraud associated with both domestic and non-domestic use of calling card authorization codes and wireless services. In particular, and since authorization cards are intended for only individual use and not group use, the contractor shall automatically block simultaneous calls made from the same card.
5	The contractor shall notify the Designated Agency Representative (DAR) or Agency designated security POC when triggers, such as the allowable cost or traffic threshold(s) (as mutually agreed between the PMO and the contractor), are reached on any calling card. In limited instances, an Agency may wish to have unrestricted calling cards. In those cases, the Agency will identify the users of those cards and establish special fraud management arrangements with the contractor on an individual case basis following award.
6	The contractor shall notify the PMO, and affected Agencies, within 30 minutes, of any incidents where it detects or suspects fraudulent use of services.
7	The contractor's notification shall be made verbally to the PMO or its designated representative, and include as much information about the event as known at that point, and actions being taken to correct the situation. The contractor shall provide updates on the status of this event upon the request of the PMO or its designated representative.
8	The contractor shall provide the PMO and impacted Agencies a written Fraud

ID Number	Description
	Incident Notification Report within seven (7) calendar days after the initial verbal notification of detection or suspicion of fraudulent activity. See Section C.3.3.2.4.1.5, Fraud Incident Notification Report for report requirements.
9	The contractor shall provide the PMO and customer Agencies a Network Fraud Performance Measurements report. This report shall summarize all incidents as described in steps 1-3 that occur within a calendar month. See Sections C.3.3.2.4.1.2, Network Fraud Performance Measurements Report for report requirements.
10	The contractor shall provide the Network Fraud Performance Measurements report to the Government 15 business days following the end of the reporting period, including months that may have no actions or security breaches have not been reported.

**C.3.3.2.3 Security Management Data Requirements**

None

**C.3.3.2.4 Security Management Report Requirements**

**C.3.3.2.4.1 Contractor Reports Provided to Government**

**C.3.3.2.4.1.1 Security Breach Detection Report**

The contractor shall summarize security violations related information, including data for all customer Agencies, and shall produce and deliver the Security Breach Detection Report according to the frequency, media, transport, file format and content as specified in this section.

**C.3.3.2.4.1.1.1 Frequency - Security Breach Detection Report**

- Initial: Within 15 business days after the calendar month in which the first SOCN is delivered
- Monthly: No later than 15 business days after the end of the calendar month

**C.3.3.2.4.1.1.2 Deliver To – Security Breach Detection Report**

- GSA COR
- Affected Agency

**C.3.3.2.4.1.1.3 Media/Transport/Format –Security Breach Detection Report**

**C.3.3.2.4.1.1.3.1 Media/Transport/Format –Security Breach Detection Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Excel 97 through 2003</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.2.4.1.1.3.2 Media/Transport/Format –Security Breach Detection Report sent to Agency**

The contractor shall provide and deliver the Agency Security Breach Detection Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.3.2.4.1.1.4 Content -- Security Breach Detection Report**

ID No.	Information Elements	Description
1	Title	Security Breach Detection Report
2	Reporting Period	Reporting period
3	Contents	Number of network security breaches detected Number of network security breaches investigated Resolution of network security breach investigations Summary of methods used by parties with intent to defraud

**C.3.3.2.4.1.2 Network Fraud Performance Measurements Report**

The contractor shall summarize fraud related information, for all customer Agencies, and shall produce and deliver the Network Fraud Performance Measurements Reports according to the frequency, media, transport, file format and content as specified in this section.

**C.3.3.2.4.1.2.1 Frequency - Network Fraud Performance Measurements Report**

- Initial: 15 business days after the calendar month in which the first SOCN is delivered
- Updated: Monthly, within 15 business days from the end of the calendar month

**C.3.3.2.4.1.2.2 Deliver To – Network Fraud Performance Measurements Report**

- GSA COR
- Agency DAR or Agency designated security POC

**C.3.3.2.4.1.2.3 Media/Transport/Format – Network Fraud Performance Measurements Report**

**C.3.3.2.4.1.2.3.1 Media/Transport/Format – Network Fraud Performance Measurements Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Excel 97 through 2003</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.2.4.1.2.3.2 Media/Transport/Format – Network Fraud Performance Measurements Report sent to Agency**

The contractor shall provide and deliver the Network Fraud Performance Measurements Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.3.2.4.1.2.4 Content -- Network Fraud Performance Measurements Report**

ID No.	Information Elements	Description
1	Title	Network Fraud Performance Measurements
2	Reporting Period	Reporting period in MM-YYYY format
3	Contents	Number of calling cards active at end of reporting period Number of calling cards investigated by the contractor for waste, fraud, and abuse in reporting period Number of calling cards reported lost or stolen in reporting period Dollar amount incurred for fraudulent calling card usage on domestic calling Number of calling cards that trigger waste, fraud, or abuse parameters in reporting period Number of calling cards deactivated for waste, fraud, or abuse in reporting period Number of calling cards deactivated because lost or stolen in reporting period Number of calling cards deactivated in the reporting period by authorized users Dollar amount on calling cards billed to authorized users that users claim is fraudulent in reporting period <ul style="list-style-type: none"> <li>Number of fraudulent domestic wireless calls attempted in period</li> <li>Number of fraudulent international wireless calls attempted in period</li> <li>Total dollar amount incurred from fraudulent calling in the reporting period</li> <li>Number of requests from Agencies for information concerning investigations of abuse of services in</li> </ul>

ID No.	Information Elements	Description
		reporting period <ul style="list-style-type: none"> <li>Status of contractor's investigations of fraudulent use of services, including number of investigations opened during period, closed during period, active at end of period, inactive at end of period</li> </ul>

**C.3.3.2.4.1.3 Security Breach Notification Report**

The contractor shall produce and deliver the Security Breach Notification Report, according to the frequency, media, transport, file format and content as specified in this section.

**C.3.3.2.4.1.3.1 Frequency –Security Breach Notification Report**

- Within seven calendar days after the occurrence of a security breach

**C.3.3.2.4.1.3.2 Deliver To –Security Breach Notification Report**

- GSA COR
- Affected Agency

**C.3.3.2.4.1.3.3 Media/Transport/Format –Security Breach Notification Report**

**C.3.3.2.4.1.3.3.1 Media/Transport/Format –Security Breach Notification Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.2.4.1.3.3.2 Media/Transport/Format –Security Breach Notification Report sent to Agency**

The contractor shall provide and deliver the Agency's Security Breach Notification Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.3.2.4.1.3.4 Content –Security Breach Notification Report**

ID No.	Information Elements	Description
1	Title	Security Breach Notification
2	Date	Date in which the written notification was issued and sent to



ID No.	Information Elements	Description
		the Government.
3	Name	Contractor name
4	Contents	Date and time security breach occurred. Description of security breach incident including the type of breach, UBI if applicable, and information or access that was compromised. In some instances, due to the proprietary nature of the information, Agencies may not want the contractor to share all incident details with the PMO; however, the PMO needs to have an appropriate level of information about the incident in order to carry out its fiduciary responsibilities in administering the Network contract. Actions and steps taken by the contractor to correct and prevent future incidents. Date when all preventive actions were completed.

**C.3.3.2.4.1.4 Non-Domestic Services Security Notification Report**

The contractor shall produce and deliver the Non-Domestic Services Security Notification Report according to the frequency, media, transport, file format and content as specified in this section

**C.3.3.2.4.1.4.1 Frequency - Non-Domestic Services Security Notification Report**

- Within seven calendar days after the occurrence of a non domestic security incident or suspicious activity

**C.3.3.2.4.1.4.2 Deliver To – Non-Domestic Services Security Notification Report**

- CO
- GSA COR
- Affected Agency

**C.3.3.2.4.1.4.3 Media/Transport/Format –Non-Domestic Services Security Notification Report**

**C.3.3.2.4.1.4.3.1 Media/Transport/Format –Non-Domestic Services Security Notification Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.2.4.1.4.3.2 Media/Transport/Format –Non-Domestic Services Security Notification Report sent to Agency**

The contractor shall provide and deliver the Agency Non-Domestic Services Security Notification Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.3.3.2.4.1.4.4 Content Non-Domestic Services Security Notification Report**

ID No.	Data Elements	Description
1	Title	Non-Domestic Services Security Notification
2	Date	Date in which the written notification was issued and sent to the Government.
3	Name	Contractor name
4	Contents	Date and time security breach or suspicious activity was identified Description of security breach incident or suspicious activity including the type of breach, UBI if applicable, service impacted, and information or access that was compromised. Actions and steps taken by the contractor to correct and prevent future incidents. Date when all preventative actions were completed

**C.3.3.2.4.1.5 Fraud Incident Notification Report**

The contractor shall produce and deliver the Fraud Incident Notification Report, according to the frequency, media, transport, file format and content as specified in this section.

**C.3.3.2.4.1.5.1 Frequency - Fraud Incident Notification Report**

- Within seven calendar days after detecting a fraud or possible fraud situation

**C.3.3.2.4.1.5.2 Deliver To –Fraud Incident Notification Report**

- GSA COR
- Agency

**C.3.3.2.4.1.5.3 Media/Transport/Format –Fraud Incident Notification Report**

**C.3.3.2.4.1.5.3.1 Media/Transport/Format –Fraud Incident Notification Report sent to GSA**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.2.4.1.5.3.2 Media/Transport/Format –Fraud Incident Notification Report sent to Agency**

The contractor shall provide and deliver the Agency Fraud Incident Notification Report to the requesting Agency in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements

**C.3.3.2.4.1.5.4 Content -- Fraud Incident Notification Report**

ID No.	Information Elements	Description
1	Title	Fraud Incident Notification
	Date	Date in which the written notification was issued and sent to the Government
2	Name	Contractor name
3	Contents	Date and time fraud incident was detected Description of security breach incident including the type of breach, UBI if applicable, and information or access that was compromised. Actions and steps taken by the contractor to correct and prevent future incidents. Date when all preventive actions were completed

**C.3.3.2.4.2 Contractor Provided Reports to GSA**

**C.3.3.2.4.2.1 Security Plan and Risks Assessment**

The contractor shall produce a Security Plan and Risks Assessment that addresses the requirements identified in Section 3.3.2.2.1, Step 1 - Security Plan, and Section 3.3.2.2.2, Step 2 – Security Risk Analysis for all Network services. The contractor shall produce and deliver the Security Plan according to the frequency, media, transport, format, and content as specified in this section.

**C.3.3.2.4.2.1.1 Frequency - Security Plan and Risks Assessment**

- Initial: Included at Contract Award
- Revised: Within 30 calendar days of Notice to Proceed; revised to include the Security Risks Assessment Report as an attachment to the plan and as necessary to reflect actions taken after risk assessment/mitigation
- Updated: Annually, 30 business days after the end of each contract year

**C.3.3.2.4.2.1.2 Deliver To – Security Plan and Risks Assessment**

- GSA COR

**C.3.3.2.4.2.1.3 Media/Transport/Format – Security Plan and Risks Assessment**

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> </ul>

#### C.3.3.2.4.2.1.4 Content -- Security Plan and Risks Assessment

The Security Plan shall be in narrative form and include at minimum the following:

ID Number	Information Elements	Description
1	Cover Page	Report cover page
1.1	Report Title	Security Plan
1.2	Contractor	Contractor's name
1.3	Version	Version number of the report
1.4	Date	Date of issue of the report
2	Contents	<p>At minimum the following areas shall be included:</p> <ul style="list-style-type: none"> <li>• Security Management Organization and Planning</li> <li>• Security Risk Management</li> <li>• Information Security Management</li> <li>• Information Assurance Management</li> <li>• Security Breach Response Management</li> <li>• Alarms and Audit Trails</li> <li>• Personnel Security</li> <li>• Physical Security</li> <li>• Procedural Security</li> <li>• Security Refreshment</li> <li>• Non-Domestic Services Security Management</li> <li>• Fraud Prevention Management</li> <li>• Improved security-related processes and technologies that have become available and are being incorporated</li> </ul>
3	Risks Assessment Attachment	<p>At a minimum, the following areas shall be included:</p> <ul style="list-style-type: none"> <li>• Security vulnerabilities identified and their associated risks</li> <li>• Likelihood that the risks will occur</li> <li>• Impact of the risks to the Government</li> <li>• Severity of the risks</li> <li>• Mitigation strategy</li> <li>• Commercially reasonable measure that the contract will take to mitigate the risks</li> </ul>

#### C.3.3.3 Disaster Recovery

A significant element of the provision of the contract services is the demonstration of the capability to respond to emergency situations. The contractor is required to have a mature and detailed Disaster Recovery Plan to deal with disasters (e.g., fires) that affect its operational facilities or infrastructure under this contract.

##### C.3.3.3.1 Disaster Recovery Process Definition

Disaster Recovery entails the development and implementation of a Disaster Recovery Plan that addresses preparedness for disasters (e.g., fires) that affect the contractor's facilities or infrastructure and that may impact Network services and support systems. National Security/Emergency Preparedness (NS/EP) Requirements are covered in Section C.5, National Security and Emergency Preparedness (NS/EP), and are separate from Disaster Recovery requirements contained in this section except as specified for the liaison officer.

**C.3.3.3.1.1 Disaster Recovery Process Narrative**

Step Number	Description	Executing Entities
1	The contractor provides a Disaster Recovery Plan.	Contractor
2	The contractor notifies the PMO when a disaster has major consequences on its Network services, and coordinates as appropriate with the PMO and impacted Agencies.	Contractor
3	The contractor provides a disaster recovery liaison officer to interface with the PMO in the event of a disaster.	Contractor
4	The contractor will work with the Government on an ongoing basis to enhance its disaster recovery preparedness and maintain readiness as it relates to Network services.	Contractor

**C.3.3.3.2 Disaster Recovery Functional Requirements****C.3.3.3.2.1 Step 1--Disaster Recovery Plan**

ID Number	Description
1	A Disaster Recovery Plan shall be included in the contract at award.
2	The contractor's Disaster Recovery Plan shall describe in detail how the contractor shall satisfy the disaster recovery requirements as identified in Section C.3.3.3, Disaster Recovery and all sub-sections.
3	The contractor shall utilize the format for the Disaster Recovery Plan as described in Section C.3.3.3.4.1.1, Disaster Recovery Plan.
4	Within 30 calendar days of Notice to Proceed, the contractor shall provide the GSA COR an update to the Disaster Recovery Plan.
5	The contractor shall provide the GSA COR an update to its Disaster Recovery Plan annually.
6	The contractor shall address in each annual update how improved disaster recovery practices, processes, and technologies are to be incorporated into the contract as they become available.
7	The contractor shall address in the Disaster Recovery Plan its disaster recovery command structure for managing disaster and how it will communicate, interface and coordinate internally and with the Government, suppliers, partners, and other Network stakeholders as appropriate. Communication requirements from the contractor's network control center(s) to National Communication System (NCS) locations or other critical Government locations during an emergency will be defined by the Government after contract award.
8	The contractor shall address in the Disaster Recovery Plan its overall strategy for service restoration including prioritization and partial or full restoration as appropriate.
9	The contractor shall address in the Disaster Recovery Plan as appropriate back up strategies for services affecting facilities, operational support systems and data, and key service components
10	The contractor shall address in the Disaster Recovery Plan how it ensures that domestic and non-domestic suppliers or partners for which Network service offering depends on have in place adequate and viable disaster recovery plans and strategies.

**C.3.3.3.2.2 Step 2--Disaster Recovery**

ID Number	Description
1	The contractor shall notify the PMO by phone and e-mail within 15 minutes of determining that an event has occurred that may have major consequences to the Network services. The disaster notification shall include at a minimum: a brief description of the disaster, date/time of the disaster, what Network services are impacted by the disaster, and impacted Agencies.
2	The contractor shall update and provide the Disaster Recovery Plan annually for emergency management actions affecting the contractor's network based on the critical users' requirements for service to continue during emergencies.
3	The contractor shall be solely responsible for network operations. However, the PMO will set priorities for Network services users.
4	The emergency management capability will be activated at the discretion of the PMO.
5	The contractor's network management system design shall provide features that will make real-time network monitoring resistant to failure and avoid the possibility of a single point of failure impacting the entire network management function.
6	The contractor's network management system shall continue to provide network management functions during emergency periods or periods of severe overload conditions.
7	The contractor shall continue to supply telecommunications services without interruption or impairment, if the network management system fails.

**C.3.3.3.2.3 Step 3—Disaster Recovery Interfaces with the Contractor**

ID Number	Description
1	The contractor shall provide a Network disaster recovery liaison officer, cleared at the Secret level or higher, to meet with the Government, whenever required by the PMO, pertaining to disaster recovery or NS/EP (see Section C.5, National Security and Emergency Preparedness) matters related to the Network contract.
2	If the contractor has a dedicated representative to the NCS's National Coordinating Center (NCC) for Telecommunications, the contractor's Network liaison officer for the Network contract shall be a different person from the contractor's NCS/NCC representative.
3	In the event of a disaster situation, the contractor's disaster recovery liaison officer shall have no conflicts of duties that could interfere with Network contract requirements.
4	The contractor's disaster recovery liaison officer shall be prepared to discuss classified requirements or problems with the Government at the planning and operational levels, for crisis or emergency situations.
5	The disaster recovery liaison officer shall be named in the C.3.3.3.2.1, Disaster Recovery Plan, and in the C.3.2.2.2, Program Management Plan.
6	The contractor's disaster recovery liaison officer shall be familiar with the general and technical management organization of the contractor.
7	The contractor's disaster recovery liaison officer shall have established channels for initiating necessary actions and obtaining necessary decisions for disaster recovery.
8	The contractor's disaster recovery liaison officer or a fully-qualified alternate shall be on site at the PMO no later than four hours after receiving notice of a disaster.
9	In an extended disaster event, the contractor's disaster recovery liaison officer shall be available, as requested by the PMO on an extended basis.

**C.3.3.3.2.4 Step 4--Ongoing Disaster Recovery Preparedness**

ID Number	Description
1	The contractor shall work with the Government on an ongoing basis to enhance its disaster recovery preparedness as it relates to Networx services.
2	The contractor's post-award activities shall include, but not be limited to: <ul style="list-style-type: none"> <li>(a) Providing the Government yearly briefings to:                             <ul style="list-style-type: none"> <li>• Inform and educate the Government on the latest issues, trends, technologies, and practices pertaining to disaster recovery</li> <li>• Discuss the implications of these trends, technologies, and practices to the Networx Program</li> <li>• Inform the Government of any actions the contractor plans to take to improve its readiness vis-à-vis these trends, technologies, and practices</li> </ul> </li> <li>(b) Working with the Government to reassess its current disaster recovery plan and practices and planned improvements, and determine what further changes if any should be incorporated as part of the Networx Program.</li> <li>(c) Preparation of disaster recovery practices and briefings for GSA and Agency representatives and, upon request, conducting the briefings.</li> </ul>
3	The contractor shall include and discuss as part of its Disaster Recovery Plan how it will ensure that its disaster recovery plan is effective and that its operation is in a state of readiness to address disasters.
4	The contractor shall conduct annual preparedness drills for disaster recovery, document the results of such drills, and report to the PMO in annual updates to the Disaster Recovery Plan the actions the contractor will take or has taken to address any shortcoming.

**C.3.3.3.3 Disaster Recovery Data Requirements**

None

**C.3.3.3.4 Disaster Recovery Report Requirements**

**C.3.3.3.4.1 Contractor Reports Provided to GSA**

**C.3.3.3.4.1.1 Disaster Recovery Plan**

The contractor shall produce and deliver the Disaster Recovery Plan to GSA, according to the frequency, media, transport, format, and content as specified in this section.

**C.3.3.3.4.1.1.1 Frequency - Disaster Recovery Plan**

- Initial: Included at Contract Award
- Revised: Within 30 calendar days of Notice to Proceed, based on Government comments
- Updated: Annually, 30 business days after the end of each contract year

**C.3.3.3.4.1.1.2 Delivery To - Disaster Recovery Plan**

- GSA COR

**C.3.3.3.4.1.1.3 Media/Transport/Format - Disaster Recovery Plan**

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.3.3.4.1.1.4 Content - Disaster Recovery Plan**

The Disaster Recovery Plan shall be in narrative form and include at minimum the following:

ID Number	Information Elements	Description
1	Cover Page	Report cover page
1.1	Report Title	Disaster Recovery Plan
1.2	Contractor	Contractor's name
1.3	Version	Version number of the report
1.4	Date	Date of issue of the report
2	Contents	At minimum the following areas need to be included: <ul style="list-style-type: none"> <li>• Disaster Recovery Organization</li> <li>• Disaster Recovery Communication</li> <li>• Disaster Recovery Strategy</li> <li>• Disaster Recovery Capabilities</li> <li>• Disaster Recovery Readiness/Preparedness</li> </ul>

The contractor may add other elements to the content and structure of the Disaster Recovery Plan as appropriate to ensure that all requirements in Section C.3.3, Disaster Recovery are addressed and that the material in the plan is presented in a cohesive and logical manner.

**C.3.4 Customer Service**

**C.3.4.1 Customer Support**

**C.3.4.1.1 Customer Support Process Definition**

**C.3.4.1.1.1 Customer Support Process Description**



Customer support entails the implementation by the contractor of an office to facilitate the Government’s use of the Networx Contract. The contractor’s Customer Support Office (CSO) will be the focal point for the contractor’s sales, service and implementation activities with the Government. The contractor’s Customer Support Office will be set up to communicate effectively with Government users of the Networx contract around the world using all common means of communications.

**C.3.4.1.1.2 Customer Support Process Narrative**

Step Number	Description	Executing Entities
1	A Customer Support Office (CSO) function will be the primary point of interface between the contractor and Government entities interested in or using the Networx Contract.	Contractor
2	The CSO responds to general inquiries.	Contractor
3	The CSO provides information regarding available products and services, responds to service inquiries, and accepts orders.	Contractor
4	The CSO accepts billing inquiries and provides billing status.	Contractor
5	The CSO provides training registration and scheduling information.	Contractor
6	The CSO provides technical support.	Contractor

**C.3.4.1.2 Functional Requirements**

**C.3.4.1.2.1 Step 1--General Customer Support Office Requirements**

ID Number	Description
1	The contractor shall establish and operate a Customer Support Office (CSO).
2	The contractor shall identify the structure of the CSO to the Government in the contract.
3	The contractor shall make the CSO functions accessible to Government users by all of the following methods: telephone, facsimile, e-mail, postal service and public website.
4	The contractor shall respond to inquiries via the same method the user accessed the CSO, unless otherwise specified by the user.
5	The contractor shall provide a main US toll free telephone number through which all CSO functional areas can be accessed.
5.1	The contractor shall provide the capability for non-domestic users to contact the CSO without incurring international charges.
5.2	The contractor shall minimize, to the extent possible, the different CSO contact numbers that will be required to support non-domestic users.
6	The contractor shall provide contact info, as defined in Section 3.2.2.1.7, Coordination and Communication for each functional area of the CSO.
7	The contractor shall make the CSO functions accessible to Government users through the contractor’s Networx public website.
8	The contractor shall provide hot-links from the contractor’s Networx public website to CSO functional area e-mail addresses.
9	The contractor shall make available all CSO functional area telephone numbers, facsimile numbers and the CSO postal address at the contractor’s Networx public website per Section 3.4.3, Customer Service.
10	The contractor shall provide TDD access to the CSO for individuals who are hearing impaired or have speech disabilities.
11	The contractor shall provide basic operations of the CSO at contract award, including the main toll free telephone number, primary e-mail address and primary facsimile

ID Number	Description
	access.
12	The contractor shall have all functional areas of the CSO fully operational within 30 calendar days of contract award.
13	The contractor's CSO shall be located at premises provided by the contractor.
14	The contractor's CSO shall be structured to deal effectively with the geographical distribution of Networx subscribing Agencies and the GSA Program Management Office taking into account GSA Program Management Office activities in the GSA regions and GSA international activities in Germany and elsewhere.
15	The contractor's CSO shall conduct business 24x7.
16	The contractor shall answer 80% of all monthly calls placed to the CSO within 60 seconds.
17	The contractor shall respond to e-mail, facsimile or postal inquiries within one business day of receipt by the CSO.
18	The contractor shall respond to 80% of all monthly TDD inquiries within 60 seconds.

#### C.3.4.1.2.2 Step 2--CSO - General Inquiries

ID Number	Description
1	The contractor's CSO shall provide responses to user inquiries of a general nature such as: Contractor's established administrative and operational procedures Contractor's points of contact User forum information.

#### C.3.4.1.2.3 Step 3--CSO – Service Information, Inquiries and Orders

ID Number	Description
1	The contractor's CSO shall respond to inquiries from Government Agencies regarding services available through the Networx contract.

#### C.3.4.1.2.4 Step 4--CSO - Billing Inquiries and Dispute Status

ID Number	Description
1	The contractor's CSO shall respond to Billing and Dispute inquiries as described in C.3.6. Billing

#### C.3.4.1.2.5 Step 5--CSO - Training Registration and Scheduling

ID Number	Description
1	The contractor's CSO shall provide information on available training classes. Training requirements are described in C.3.7, Training.
2	The contractor's CSO shall provide guidance and assistance with registration for training classes.

#### C.3.4.1.2.6 Step 6--CSO - Technical Support

ID Number	Description
1	The contractor's CSO shall provide a technical group to support Agencies and the

ID Number	Description
	PMO regarding the services the contractor delivers to the Government.
2	The contractor's CSO technical support shall include, but not be limited to: Answering questions related to how users can obtain the functions designed into the services the contractor provides via the Network Contract. Advising users on the capabilities incorporated into service features. Providing technical support to assist either the contractor technicians or the Agencies or other organizations or personnel in the timely resolution of troubles. Notifying users of new services and features that are planned or that have recently been added to the contract. Providing support for service ordering and tracking. Providing support regarding billing issues.

#### C.3.4.1.3 Customer Support Data Requirements

None

#### C.3.4.1.4 Customer Support Report Requirements

None

#### C.3.4.2 CSO – Trouble and Complaint Handling

##### C.3.4.2.1 Trouble and Complaint Handling Process Definition

##### C.3.4.2.1.1 Trouble and Complaint Handling Process Description

In addition to the requirements of the CSO detailed in the preceding section C.3.4.1, Customer Support, this section presents the Government's requirements specific to entering and handling trouble and complaint reports. In addition, this section specifies the Government's management-level performance reports required to monitor the contractor's responsiveness to trouble and complaint handling. (See Attachment J.11 for definitions of Trouble Report and Complaint Report.) NOTE: Land Mobile Radio Service (LMRS) has unique requirements for training, trouble handling, and network management. As such, those portions of the Management and Operations requirements DO NOT apply to LMRS.

##### C.3.4.2.1.2 Trouble and Complaint Handling Process Narrative

Step Number	Description	Executing Entities
1	GSA or Agency experiences problem with service and reports it to the contractor.	GSA or Agency
2	The contractor creates an electronic record of the report and begins resolution.	Contractor
3	The contractor provides status updates to the reporting office.	Contractor
4	The contractor provides the on-line real-time access to information in the record to allow the Government to perform ad hoc status inquiries.	Contractor
5	The contractor resolves the issue, recording progress and performing internal escalations as needed.	Contractor
6	The contractor reports resolution to the Government	Contractor

Step Number	Description	Executing Entities
	and closes the record.	

**C.3.4.2.2 Trouble and Complaint Handling Functional Requirements**

**C.3.4.2.2.1 Step 2--Recording Troubles and Complaints and Initiating Resolution**

ID Number	Description
1	The contractor shall establish and implement procedures and systems for 24x7 trouble and complaint collection, entry, tracking, analysis, priority classification, and escalation for all services to ensure that problems are resolved within the time frames specified in Sections C.2, Technical Requirements and Attachment J.13, Service Level Requirements.
2	The contractor's reporting system shall allow for identification of troubles and complaints for both Agency-identified mission-critical Telecommunications Service Priority (TSP) and non mission-critical (non-TSP) services.
3	The Agencies will identify services with a "restoration TSP" code at the time of ordering or at any other time after that, and the contractor shall carry that designation forward to the trouble and complaint handling and network management systems.
4	The contractor shall work to restore any TSP restoration coded service before any non-TSP coded service, as soon as possible, using best effort. The only service that may be worked on before attempting to restore TSP-restorable services is an order for new service that bears a TSP provisioning code.
5	Upon receipt of a trouble or complaint report, the contractor shall respond using the same medium as the initiator used to report the problem OR by telephone and shall provide the following: Tracking number for the record Confirmation of the contact information (name, phone, e-mail) of the initiator reporting the problem, the contact listed in the customer profile for that service, or an alternate contact the reporter designates Estimated time to resolve, if known Expected intervals for status updates Any suspected or known causes or correlation to other events, as known at the time Confirmation of TSP code or non-TSP designation Identification of "critical" service level or "routine" service level Method of contact should the Government require additional information.
6	The contractor shall use the same trouble management system regardless of whether the report is initiated by the Government or by the contractor.
7	The trouble management system and the complaint handling system need not be integrated, but the contractor shall provide a single interface to the Government that does not require the Government to distinguish between systems.
8	The contractor's trouble and complaint reporting system shall record and store the history or audit trails of resolution activities.
9	The contractor's system shall assign a unique tracking number to each record and capture the initiator's name and Agency.

**C.3.4.2.2.2 Step 3--Status Updating Requirements**

ID Number	Description
1	The contractor shall provide the status of an open trouble report for non-TSP services verbally to the initiator of the report every two hours, unless the requester

ID Number	Description
	authorizes updates by e-mail, designates an alternate contact, requests status intervals longer than two hours, or agrees to obtain ad hoc updates through the method described in C.3.4.2.2.3, Ad Hoc Trouble and Complaint Status Inquiries.
2	For an open trouble report involving a TSP service, the contractor shall provide status updates every hour to the initiator or alternate contact as authorized by the initiator.

#### C.3.4.2.2.3 Step 4--Ad Hoc Trouble and Complaint Status Inquiries

ID Number	Description
1	The contractor shall provide status of troubles or complaints any time the Government submits a request through any of the means available for reporting problems. The contractor shall respond using the same medium as the requester used OR by telephone.
2	The contractor shall provide secured Web-based real-time access to trouble and complaint reporting information for the Government to obtain ad hoc status updates.
3	The contractor shall allow the user to access the desired record(s) by entering the Agency reporting the issue AND either the trouble tracking or complaint record number or the name of the initiator.
4	The contractor shall implement measures to preclude Agencies from accessing records for Agencies other than their own. The system shall allow GSA to access all records pertaining to the contract.
5	The contractor shall provide the capability to query and sort trouble and complaint records by any field or combination of formatted (that is, not free-form text) fields in each record.
6	The contractor's system shall allow the user the choice to download the results of a query in spreadsheet and in comma separated values (CSV) formats.

#### C.3.4.2.2.4 Step 5--Resolution of Trouble or Complaint

ID Number	Description
1	The contractor shall implement an internal process for escalating an issue to increasing levels of technical expertise when the current level is unable to resolve the problem within the required interval.
2	The contractor shall implement a process for customer-driven escalations as well as internally-driven escalations to succeeding levels of management when a trouble or complaint is not resolved within the required performance target or when the customer has indicated dissatisfaction with the way the contractor has handled the issue. Requirements for the contractor's escalation contacts are in Section C.3.2.2.1, Contractor's Program Organization.
3	The contractor shall report the resolution of a trouble report or complaint to the initiator or alternate contact.
4	The contractor shall provide the initiator of a trouble report with the date, time and nature of the trouble when the trouble report is resolved.
5	The contractor shall resolve complaint reports within 7 business days of receipt.
6	If the Government's site representative is unavailable to participate in cooperative testing to confirm reestablishment of the service, the contractor shall note the time interval between the request for the Government's assistance and the time the Government's assistance for cooperative testing was actually obtained.
7	If the contractor makes best efforts to contact the initiator or alternate contact, and that person is unavailable to confirm resolution of the issue, the contractor shall record the

ID Number	Description
	resolved time of the issue as determined by the contractor.
8	A report shall be finally closed out only when the initiator or alternate contact agrees that service has been restored or the complaint has been resolved.
9	If the initiator or alternate contact is unavailable to authorize close-out, the contractor shall make best efforts to contact the initiator or alternate contact before closing the report record.
10	The contractor shall be responsible for maintaining a record of the resolution and close-out times, which includes recording entries for the beginning time and ending time of the outage.

#### C.3.4.2.2.5 Step 6--Reporting Resolution Information

ID Number	Description
1	The contractor's trouble and complaint reporting system shall be the source of record for the contractor's data regarding performance measurement of trouble and complaint reporting for all services.
2	The contractor shall maintain a history of the time the trouble or complaint was reported, the Agency that reported it, the service affected, the UBI of the service, the root cause of the problem, the resolution action, the time it was resolved, and the time the record was closed out.
3	The contractor shall process any credits applicable to the service outage based on this record of information. SLAs and credits are defined in Attachment J.13, Service Level Agreements.
4	The contractor shall maintain an archive of trouble and complaint reports and their resolutions for six years and nine months after contract expiration or termination.
5	The contractor shall, upon request from the PMO and Agencies, deliver archived trouble and complaint report data within 3 business days of the request for such information.

#### C.3.4.2.3 Trouble and Complaint Handling Data Requirements

None

#### C.3.4.2.4 Trouble and Complaint Handling Report Requirements

None

### C.3.4.3 Business Relationship Management

#### C.3.4.3.1 Business Relationship Management Process Definition

##### C.3.4.3.1.1 Business Relationship Management Process Description

The Networkx contractor is responsible for providing information on its Networkx solution to all Government personnel. This will include, at a minimum, an overview of the contract, a list of the contractor's available services, the contractor's organizational structure, key points of contact and numbers for ordering, billing, and trouble reporting, instruction manuals, and other information important to the day-to-day functioning of the contractor/Government relationship.

##### C.3.4.3.1.2 Business Relationship Management Process Narrative

Step Number	Description	Executing Entities
1	The contractor develops a Website for the dissemination of its Network contract information.	Contractor
2	The contractor maintains a list on the Website of Contractor points of contact (POCs) for critical contract functions.	Contractor
3	The contractor maintains a list on the Website of Products and Services available under the contract.	Contractor
4	The contractor provides access to Contract Operational and Administrative Data (COAD) on its Website.	Contractor

**C.3.4.3.2 Business Relationship Management Functional Requirements**

**C.3.4.3.2.1 Step 1--Network Website**

The Government anticipates at least two types of Network Website Subscriber users: a) Users who need controlled access to information, operational support systems, or operational support system functions within the constraint of their specific Agency information domain, and b) Users (e.g., DAR) who need access to all information, operational support systems, and functions within the constraint of their specific Agency information domain.

ID Number	Description
1	Within 30 calendar days from Notice to Proceed the contractor shall establish a Website for Network dedicated to providing information on its Network contract. Timeframes for adding content to the Website are as listed in specific items in Steps 1 through 4 below.
2	The contractor shall separate the Website into two main logical groupings: (1) Public; and (2) Network Subscriber.
3	The contractor shall be responsible for all aspects of hosting the Website.
4	The contractor shall make the Network public website accessible to all persons.
5	The contractor shall make the Network Subscriber Website accessible only to authorized Government and contractor personnel based on the profiles for the Government personnel that are provided in Section C.3.4.3.3.1, GSA Provided Data to contractors.
5.1	The contractor shall provide, at a minimum, Website access control capabilities to: <ul style="list-style-type: none"> <li>• Restrict user access to each specific OSS that is available to the Government through the Network Website as part of the Network contract (e.g., access to trouble management system and not to ordering system)</li> <li>• Restrict user access to certain functions within an OSS (e.g., able to view an order, but not enter an order). Specific requirements for functional control within a specific OSS are specified in the contract sections dealing with each functional area</li> <li>• Restrict users access to certain areas of the Website, or certain information published on the Network Website</li> <li>• Restrict user access to information specific to their Agency</li> </ul>
5.2	The contractor shall also provide any additional Website access controls as specified in other subsections within Section C.3, Management and Operations.
6	The contractor shall provide a monthly Network Subscriber Website List of Authorized Users report that details all individuals and their access rights.
7	The contractor shall make the Website available 24x7, recognizing that it is integral to the exchange of information between the contractor and the Government.

ID Number	Description
8	The contractor shall provide links, one on the Public site start page and one on the Networx Subscriber site start page, that provide the taxonomy of the sites based on industry best practices to ease user location of pertinent information.
9	The contractor shall maintain a list of authorized users with electronic access to the Networx Subscriber Website, including their specific access privileges or access rights profiles to perform actions that are limited by this contract (e.g., ordering).
10	The contractor shall maintain a list of authorized users of the Networx Subscriber Website for the purposes of limiting access to viewing restricted information.
11	The contractor shall enforce electronic access restrictions to the Networx Subscriber Website using industry best practices.
12	The contractor shall provide updates to the authorized access list to the Networx Contracting Officer Representative monthly.
13	Within 30 calendar days after contract award, the contractor shall provide access on the Networx public website to the original contract in redacted format consistent with certain protections afforded proprietary information under the Freedom of Information Act (FOIA). See Section H.11, Electronic Access to Contract.

#### C.3.4.3.2.2 Step 2--Points of Contract

ID Number	Description
1	Within 30 calendar days after Notice to Proceed, the contractor shall provide a list on its Networx public website of all contractor POCs per requirements in Sections C.3.2.2.1.7, Coordination and Communications, and C.3.2.3.3, contractor Data Provided to GSA, and C.3.2.3.4, Contractor Data Provided to Agency.

#### C.3.4.3.2.3 Step 3 -- Products and Services Available Under the Contract

ID Number	Description
1	Within 30 calendar days of Notice to Proceed, the contractor shall provide on the Networx public website information per Section C.3.4.3.4.1.1, Networx Products and Services on the technical details of the Networx products and services offering.
2	Within 30 calendar days of Notice to Proceed, the contractor shall provide information on the Networx public website on the use of each product and service.
3	Within 30 calendar days of Notice to Proceed, the contractor shall provide on the Networx public website alternatives, where they exist, to the product or service to aid in the Government's decision making process for placing an order.
4	Within 15 business days of the first Agency's selection of the contractor, the contractor shall provide links on the Networx public website to on-line training programs.
5	Within 15 business days of the first Agency's selection of the contractor, the contractor shall provide access on the Networx Public Website for Training registration.

#### C.3.4.3.2.4 Step 4--Contract Operational and Administrative Data (COAD)

ID Number	Description
1	The contractor shall provide access controls to ensure that only authorized Agency officials are allowed to place Networx orders through the Networx Subscriber Website for their respective Agencies.
2	Within 5 business days of the first Agency's selection of the contractor, the contractor shall provide the links described in ID Numbers 3 through 10 below.
3	The contractor shall provide links on the Networx Subscriber Website to order status information.



ID Number	Description
4	The contractor shall provide restricted access on the Networx Subscriber Website to Service Order tracking data.
5	The contractor shall provide restricted access on the Networx Subscriber Website to Trouble reporting data.
6	The contractor shall provide restricted access on the Networx Subscriber Website to Billing data.
7	The contractor shall provide restricted access on the Networx Subscriber Website to Transition data.
8	The contractor shall provide restricted access on the Networx Subscriber Website to Billing Dispute data.
9	The contractor shall provide restricted access on the Networx Subscriber Website to service-affecting faults.
10	The contractor shall provide restricted access on the Networx Subscriber Website to Performance data.
11	The contractor shall maintain the confidentiality of Agency data and information that is accessible through the Networx Subscriber Website, and ensure that only those who are authorized to view Agency data and information will have access to it.

**C.3.4.3.3 Business Relationship Management Data Requirements**

**C.3.4.3.3.1 GSA Data Provided to Contractors**

**C.3.4.3.3.1.1 Networx Subscriber Website Authorized GSA Personnel**

GSA will provide the contractor with the names of personnel, Website access privileges, and contact information as described below.

**C.3.4.3.3.1.1.1 Frequency – Networx Subscriber Website Authorized GSA Personnel**

- As needed

**C.3.4.3.3.1.1.2 Deliver To – Networx Subscriber Website Authorized GSA Personnel**

- Contractor

**C.3.4.3.3.1.1.3 Media/Transport/Format – Networx Subscriber Website Authorized GSA Personnel**

Data		
Media	Transport	Data Format
E-mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.4.3.3.1.1.4 Record Elements – Networx Subscriber Website Authorized GSA Personnel**

ID Number	Data Elements	Description
1	Name	Full name of the person with authorized access
2	Role	Government functional role for the person with authorized access
3	Access Privileges	Access privileges of the person with authorized access
4	Email	Government email address for the person with authorized access
5	Street Address 1	Street address for the primary physical location of the person with authorized access
6	Street Address 2	Street address for the primary physical location of the person with authorized access
7	City	City for the primary physical location of the person with authorized access
8	State	State for the primary physical location of the person with authorized access
9	Zip Code	Zip code for the primary physical location of the person with authorized access
10	Phone	Telephone number for the person with authorized access

**C.3.4.3.3.2 Agency Data Provided to Contractors**

**C.3.4.3.3.2.1 Networkx Subscriber Website Authorized Agency Personnel**

The Agencies will provide the contractor with the names of authorized personnel, Website access privileges, and contact information as described below.

**C.3.4.3.3.2.1.1 Frequency – Networkx Subscriber Website Authorized Agency Personnel**

- As needed

**C.3.4.3.3.2.1.2 Deliver To – Networkx Subscriber Website Authorized Agency Personnel**

- Contractor

**C.3.4.3.3.2.1.3 Media/Transport/Format – Networkx Subscriber Website Authorized Agency Personnel**

The Agency will provide and deliver the Networkx Subscriber Website Authorized Agency Personnel list to the contractor in accordance with the procedures and in any of the media, transport, and format types described in the Data table in Section C.3.1.2, Data and Report Requirements.

**C.3.4.3.3.2.1.4 Record Elements – Networkx Subscriber Website Authorized Agency Personnel**

ID Number	Data Elements	Description
1	Name	Full name of the person with authorized access
2	Role	Government functional role for the person with authorized access
3	Access Privileges	Access privileges of the person with authorized access
4	Email	Government email address for the person with authorized access
5	Street Address 1	Street address for the primary physical location of the person with

ID Number	Data Elements	Description
		authorized access
6	Street Address 2	Street address for the primary physical location of the person with authorized access
7	City	City for the primary physical location of the person with authorized access
8	State	State for the primary physical location of the person with authorized access
9	Zip Code	Zip code for the primary physical location of the person with authorized access
10	Phone	Telephone number for the person with authorized access
11	Agency Name	Name of Agency

#### C.3.4.3.4 Business Relationship Management Report Requirements

##### C.3.4.3.4.1 Contractor Reports Provided to GSA

###### C.3.4.3.4.1.1 Networkx Products and Services

The contractor shall provide a report titled Networkx Products and Services that identifies all products and services offered under the Networkx contract.

###### C.3.4.3.4.1.1.1 Frequency - Networkx Products and Services

- Initial: As part of initial Networkx Public Website
- Final: Form/format within 15 business days of receiving GSA comment
- Updated: Semi-annually , 30 business days after the end of each period, and within 30 calendar days of any Networkx contract modification that adds new services to the contract

###### C.3.4.3.4.1.1.2 Delivery To - Networkx Products and Services

- Contractor's Networkx public Website

###### C.3.4.3.4.1.1.3 Media/Transport/Format - Networkx Products and Services

Report		
Media	Transport	File Format
File Server	<ul style="list-style-type: none"> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

###### C.3.4.3.4.1.1.4 Contents - Networkx Products and Services

ID Number	Information Elements	Description
1	Title	Networkx Products and Services
2	Contractor	Name of Contractor
3	Date	Date the list of services was last updated

ID Number	Information Elements	Description
4	Contents	A list and description of all Products and Services that are available on the contractor's Networkx contract. An explanation of any usage restrictions or any other type of restrictions for each Product and Service. For those Products and Services that have restrictions, a description of any alternatives that are available.

**C.3.4.3.4.1.2 Networkx Subscriber Website List of Authorized Users**

The contractor shall provide to the PMO a report titled Networkx Subscriber List of Authorized Users that includes a list of all Government users who have authorized access to the Networkx Web site. The contractor shall produce and deliver the Networkx Subscriber Website List of Authorized Users according to the frequency, media, transport, format, and content as specified in this section.

**C.3.4.3.4.1.2.1 Frequency - Networkx Subscriber Website List of Authorized Users**

- Initial: 30 calendar days after Notice to Proceed
- Updated: Monthly, Within 15 business days after end of calendar month

**C.3.4.3.4.1.2.2 Delivery To - Networkx Subscriber Website List of Authorized Users**

- GSA COR

**C.3.4.3.4.1.2.3 Media/Transport/Format - Networkx Subscriber Website List of Authorized Users**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.4.3.4.1.2.4 Content - Networkx Subscriber Website List of Authorized Users**

ID Number	Information Elements	Description
1	Title	Networkx Subscriber Website List of Authorized Users
2	Contractor	Name of contractor
3	Date	Date of Report
4	Contents	The report shall contain the following information on each individual with access to the Networkx Subscriber Website: (a) Name (b) Agency (c) Government Role (d) Networkx Website Role (e) E-mail (f) Address (g) Phone number

ID Number	Information Elements	Description
		(h) Access Rights

**C.3.4.4 Revenue Forecast**

The Networkx Program is a non-appropriated Government program; it is self-funded based on fees collected from Agencies that use the Networkx services. In order to manage the Networkx Program effectively, ensure its expenses are met, and ensure that minimum revenue guarantees to contractors are met, GSA needs to be able to accurately forecast the Networkx Program revenue stream. GSA acknowledges the proprietary nature of the contractor’s opportunity pipeline, and will take appropriate measures to ensure the confidentiality of this information.

This section defines GSA’s requirements for information that GSA needs from contractors in order to analyze and forecast the Networkx Program revenue stream. To make accurate revenue forecasts, GSA needs information from contractors pertaining to newly awarded Networkx services business, new Networkx services orders that have not yet been fulfilled, changes in existing services that will affect the revenue stream, and the contractor’s Networkx opportunity pipeline. Information pertaining to newly awarded Networkx business and new Networkx orders that have been placed by Agencies but have not been fulfilled will allow GSA to forecast when this new revenue will materialize. Information pertaining to changes in existing services and to the contractor’s Networkx opportunity pipeline will allow GSA to estimate Networkx Program revenue growth.

**C.3.4.4.1 Revenue Forecast Process Definition**

**C.3.4.4.1.1 Revenue Forecast Process Description**

The Revenue Forecast Process is the steps and activities to support GSA’s analysis of the following: Agencies Networkx services usage, Agencies uptake of new services, existing revenue stream, new orders, prospective opportunities, and revenue growth in order to forecast Networkx revenues.

**C.3.4.4.1.2 Revenue Forecast Process Narrative**

Step Number	Description	Executing Entities
1	The contractor compiles and delivers to GSA information on newly awarded Networkx services business, new Networkx orders, contractor’s Networkx services opportunity pipeline, and other expected changes that will impact the revenue stream.	Contractor
2	The contractor compiles and delivers to GSA information on new Networkx orders	Contractor
3	GSA analyzes contractor provided information on business opportunities and revenue stream.	GSA
4	GSA generates and distributes to FTS management revenue forecast.	GSA

**C.3.4.4.2 Revenue Forecast Functional Requirements**

**C.3.4.4.2.1 Step 1--New/Prospective Business Information List**

ID Number	Description
1	The contractor shall compile a quarterly New/Prospective Business Information List as described in Section C.3.4.4.3.1.1, New/Prospective Business Information List.
2	The contractor shall include in the quarterly New/Prospective Business Information List all new Network services business opportunities that the contractor has been awarded during the quarter.
3	The contractor shall include in the quarterly New/Prospective Business Information List a snapshot of its opportunity pipeline that includes all prospective Network opportunities that the contractor has identified and anticipates competing for.
4	The contractor shall include in the quarterly New/Prospective Business Information List a description of any changes to existing Network business that the contractor has identified and anticipates implementing.

**C.3.4.4.2.2 Step 2--New Orders Information**

ID Number	Description
1	The contractor shall generate a quarterly New Orders Information List of unfulfilled new orders that have been placed by Agencies during the month as described in Section C.3.4.3.2, New Orders Information List.
2	The contractor shall include in the New Orders quarterly information list all new Agency orders and Agency order modifications that have been received during the quarter but have not yet been fulfilled.

**C.3.4.4.3 Revenue Forecast Data Requirements**

**C.3.4.4.3.1 Contractor Provided Data to GSA**

**C.3.4.4.3.1.1 New/Prospective Business Information List**

The contractor shall produce and deliver the New/Prospective Business Information List according to the frequency, media, transport, format, and content as specified in this section.

**C.3.4.4.3.1.1.1 Frequency – New/Prospective Business Information List**

- Quarterly, 30 business days after the end of each calendar quarter

**C.3.4.4.3.1.1.2 Deliver To - New/Prospective Business Information List**

- GSA COR

**C.3.4.4.3.1.1.3 Media/Transport/Format – New/Prospective Business Information List**

Data		
Media	Transport	Data Format
E-mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.4.4.3.1.1.4 Record Elements -- New/Prospective Business Information List**

ID Number	Data Elements	Description
1	Contractor-ID	Contractor defined 3-8 letter acronyms that uniquely identify the contractor. This code shall remain constant for the duration of the contract.
2	Business-Opportunity-ID	Contractor defined 12 or less characters alpha-numeric identification of a newly awarded or prospective business opportunity or anticipated change to existing business. This code shall remain constant for the duration of the contract.
3	Business-Opportunity-Name	Maximum 100 characters name of the business opportunity.
4	Business-Opportunity-Description	Maximum of 256 characters description of the newly awarded or prospective business opportunity or change to existing business.
5	Agency-Hierarchy-Code	Agency Hierarchy Code
6	Government-Agency	Government Agency that is the newly awarded, prospective, or impacted customer.
7	Probability of Award	Probability of being awarded the opportunity or implementing the change. For newly awarded opportunities, this number should always be 100%. For prospective opportunities or changes, this number should be a percentage less than 100% that reflects the contractor's assessment of the likelihood of being awarded this opportunity or implementing this change.
8	Anticipated-Close-Date	For newly awarded opportunities, this date should be the date on which the opportunity was awarded. For prospective opportunities and changes, this date should be the date the contractor anticipates being awarded this business or implementing the change.
9	Estimated- Value-Initiation-Charges	Estimated dollar value of any initiation charges expected for the entire opportunity or change. That is, the expected initiation charges when all expected services under this opportunity have been ordered.
10	Estimated- Value-Monthly- Charges	Estimated dollar value of monthly recurring charges expected for the entire opportunity or change. That is, the expected monthly revenue stream when all expected services under this opportunity have been ordered and put in service.
11	Estimated- Change-Initiation-Charges (applies to changes only)	Estimated increase (decrease) in dollar value of any initiation charges expected for the change.
12	Estimated- Value-Monthly- Charges (applies to changes only)	Estimated increase (decrease) in dollar value of monthly recurring charges expected for the entire change.

**C.3.4.4.3.1.2 New Orders Information List**

The contractor shall produce and deliver the New Orders Information List according to the frequency, media, transport, format, and content as specified in this section.

**C.3.4.4.3.1.2.1 Frequency – New Orders Information List**

- Quarterly, 30 business days after the end of each calendar quarter

**C.3.4.4.3.1.2.2 Deliver To - New Orders Information List**

GSA COR

**C.3.4.4.3.1.2.3 Media/Transport/Format – New Orders Information List**

Data		
Media	Transport	Data Format
E-mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.4.4.3.1.2.4 Record Elements – New Orders Information List**

ID Number	Data Elements	Description
1	Contractor-ID	Contractor defined 3-8 letter acronyms that uniquely identify the contractor. This code shall remain constant for the duration of the contract.
2	Business-Opportunity-ID	Contractor defined 12 or less characters alpha-numeric identification of a newly awarded or prospective business opportunity. This code shall remain constant for the duration of the contract.
3	Business-Opportunity-Name	Maximum 100 characters name of the business opportunity.
4	Business-Opportunity-Description	Maximum of 25 characters describing the newly awarded or prospective business opportunity.
5	Agency-Hierarchy-Code	Agency Hierarchy Code
6	Government-Agency	Government entity, Sub-Agency, or bureau that is the newly awarded or prospective customer Agency (e.g., IRS, Bureau of Engraving).
7	Order-Number	Contractor order number
8	CLIN	Contract Line Item Number for service ordered
9	Quantity-Ordered	Quantity of the particular CLIN ordered
10	Order-Date	Date in which the order was placed
11	Order-Modification-Description	If the order that has not yet been fulfilled is a modification to an order, describe the modification.

**C.3.4.4.4 Revenue Forecast Report Requirements**

None

**C.3.4.5 Service Optimization**



It is the Government's intent to encourage Agencies that co-locate on the same facility to share Network services as a way of saving money. It is also the Government's intent to present Agencies with consolidation options of existing services from the same or multiple vendors as a way of saving money, or replacing existing services with newer services that are more cost effective.

This section states the Government's requirements for the contractor to conduct annual optimization analysis and reporting of savings that can be achieved by Agencies by consolidating existing services or replacing existing services with more cost effective services.

The Government anticipates three types of optimization scenarios that apply to Telecommunications and Access Service Types; however, the contractor is free to include other optimization scenarios where the Government could save money as part of its analysis and reporting. These three scenarios are:

- Consolidation of existing Telecommunications and Access services by an Agency within a particular facility,
- Consolidation of existing Telecommunications and Access services by multiple Agencies within a particular facility.
- Replacement of existing Telecommunications and Access services with more cost effective services.

Consolidation of existing services by an Agency within a particular facility refers to a scenario in which an Agency may have multiple data or voice circuits that could be consolidated and replaced with fewer (same or higher capacity) circuits without any loss of capacity or quality of service, and the resulting configuration would be cheaper to operate.

Consolidation of existing services by multiple Agencies within a particular facility refers to a scenario in which two or more Agencies reside in the same building and each of them may have several data or voice circuits that could be consolidated and shared without any loss of capacity or quality of service, and the resulting configuration would be less costly to each Agency.

Replacement of existing services with more cost-effective services refers to a scenario in which an Agency or Agencies in the same facility may be using a type of service that could be replaced by a different or new type of service without any loss of capability or loss of services. For example, an Agency may be using voice services, and replacing it with Voice Over IP (VoIP) may be more cost-effective.

#### **C.3.4.5.1 Service Optimization Process**

##### **C.3.4.5.1.1 Service Optimization Process Description**

The Service Optimization Process is the steps and activities that GSA and the contractor will follow to determine candidate locations that may save Agencies on their monthly recurring costs for access to the vendor Points of Presence. This process

includes identification and determination of potential candidate locations for optimization, comparing candidate locations against the vendor's annual candidate list reports, and presenting the results to the Agencies for their buy-in and decision to order the optimized access solution.

**C.3.4.5.1.2 Service Optimization Process Narrative**

Step Number	Description	Executing Entities
1	Generate and provide the Government with annual Candidate Locations report	Contractor
2	Review and evaluate contractor report for compliance and accuracy within 30 calendar of receipt.	GSA
3	Correct Candidate Locations report problems and issues	Contractor
4	Generate and present to Agencies optimization reports	GSA
5	Measure and report on Optimization Program performance	GSA
6	Agencies consider optimization and order optimized solution	Agencies

**C.3.4.5.2 Service Optimization Functional Requirements**

**C.3.4.5.2.1 Step 1--Generate Annual Candidate Reports**

ID Number	Description
1	The contractor shall conduct, at no cost to the Government, an annual service optimization analysis that includes at minimum analysis of voice and data services, and shall deliver to the PMO a Candidate Locations Optimization Report that identifies Government locations that may save monthly recurring costs as a result of consolidating or replacing existing services with more efficient ones.
2	The contractor shall include in its analysis, at a minimum but not limited to, all unclassified Government buildings/facilities for which it provides Telecommunications and Access services.
3	The contractor shall include in the Candidate Locations Optimization Report, at minimum, the data elements and information described in Section C.3.4.5.4, Service Optimization Report Requirements.
4	The contractor shall include in the report savings that can be achieved by consolidating services by a single Agency within a facility.
5	The contractor shall include in the report savings that can be achieved by consolidating services from multiple Agencies within a facility.
6	The contractor shall include in the report savings that can be achieved by replacing existing services by a single Agency within a facility with more cost effective services.
7	The contractor shall include in the report savings that can be achieved by replacing existing services from multiple Agencies within a facility with more cost effective services.
8	The contractor shall provide the annual Candidate Locations report within 45 business days of the end of each Government fiscal year, starting in year two, for the duration of the contract.

**C.3.4.5.2.2 Step 3--Candidate Locations Report Issues**

ID Number	Description
1	The contractor shall correct and resolve, within 30 calendar days from receipt, any issues raised by the Government pertaining to the accuracy or completeness of the Candidate Locations report and re-submit the report.
2	The contractor shall respond within 10 business days with clarification or additional information requested by the Government related to the Candidate Locations report.

**C.3.4.5.3 Service Optimization Data Requirements**

None

**C.3.4.5.4 Service Optimization Report Requirements**

**C.3.4.5.4.1 Contractor Reports Provided to GSA**

**C.3.4.5.4.1.1 Candidate Locations Optimization Report**

The contractor shall produce and deliver the Candidate Locations Optimization Report according to the frequency, media, transport, format, and content as specified in this section. The report shall include one entry for each optimization candidate location identified and analyzed by the contractor.

**C.3.4.5.4.1.1.1 Frequency - Candidate Locations Optimization Report**

- Initial: 45 business days after the end of the first full Government fiscal year
- Updated: 45 business days after the end of each Government fiscal year

**C.3.4.5.4.1.1.2 Delivery To - Candidate Locations Optimization Report**

- GSA COR

**C.3.4.5.4.1.1.3 Media/Transport/Format - Candidate Locations Optimization Report**

Report		
Media	Transport	File Format
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Excel 97 through 2003</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.4.5.4.1.1.4 Content - Candidate Locations Optimization Report**

ID Number	Information Elements	Description
1	Report_Title	Network Candidate Locations Optimization Report
2	Date	Date in which the report is generated
3	Building_Address	The full address or appropriate identifier of the building, facility, or other service delivery point that has been identified as an optimization candidate.

ID Number	Information Elements	Description
4	Agencies	The name of the Agency or Agencies located in the building that will be party to the optimization savings.
5	Start_Up_Costs	The total start up costs to implement the optimized service solution. This should include costs such as engineering, installation, and any other costs required to implement the optimized service solution.
6	Current_Monthly_Service_Charge	Monthly service charged paid by Agency on existing configuration
7	Estimated_Monthly_Service_Charge	Estimated monthly service charge that they Agency would pay if it were to implement the optimized solution.
8	Estimated_Annual_Savings_Amount	The estimated annual savings that each Agency in the building/facility would save if optimization is implemented.
9	Existing_Access_Arrangements	Description and configuration of the existing access arrangement.
10	New_Access_Arrangement	Description and configuration of the new and optimized access arrangement.
11	New_Equipment_Required	Description of any additional equipment the Government will be required to purchase to implement the optimized solution.

### C.3.5 Service Ordering

This section applies to all services ordered under the Networkx contract.

The Service Ordering Process includes the submission of orders by Agencies and the receipt by Agencies of contractor acknowledgements at appropriate points along the ordering and provisioning processes. Other Ordering related processes such as selecting the initial Networkx contractor, selecting the subsequent Networkx contractors, task orders/delivery orders, are covered in Section G.4 Ordering.

The contractor supports the following functions through the development, implementation, and operation of processes, electronic systems, and data which meet the requirements detailed in Section C.3.5.1 Direct Ordering.

Use of the contractor's commercial systems is encouraged, as it is not the Government's intention to finance or otherwise pay for the contractor's ordering system modifications.

The contractor will accept only authorized orders from the Agencies, to ensure that correct Agency hierarchy information is provided and to provide order tracking and inquiry information to assist both the Agencies and GSA in monitoring order related activities. Of key concern to the GSA and the Agencies is the completeness, accuracy and timely receipt of the Service Order Completion Notice, as it feeds the inventory, billing verification, and ordering verification processes.

**Authorization of Orders.** Only authorized personnel are allowed to submit orders to the contractor. The contractor will not be paid for any order that is submitted by an unauthorized person and that the contractor fulfills.

Agencies will designate individuals who are authorized to place orders under this contract. These individuals may be Agency Contracting Officers or Designated Agency Representatives (DARs). Each Agency will appoint a DAR Administrator who will maintain a current list of people who are authorized to place Networx orders, and the Agency will identify the DAR Administrator to the contractor. Should the Agency change its DAR Administrator, the Agency will inform the contractor of his or her replacement.

Explanation of the roles that exist within the Government are discussed in Section G.1 Roles and Responsibilities.

**Agency Hierarchies.** Every order submitted by the Government will contain one or more Agency Hierarchy Codes (AHC), which enable the Government to account internally for charges. The contractor will not be paid for any order the Government accepts without a valid Agency Hierarchy Code. The contractor validates the Agency Hierarchy Code based on authorized user information provided by the Agency specifying the services and Agency Hierarchy Codes that are valid for each authorized user. The Government is not requiring the contractor to have a link to its own internal accounting code structure. The Government expects the contractor to use the Agency Hierarchy Codes.

The Government consists of many large hierarchical organizations that purchase services from the contractor and are billed for those services. Agencies vary in size, vary in spans of control over Agencies that are below them in the hierarchy, and vary in spans of visibility to Agencies that are above them in the hierarchy. For example, an Agency may have other Agencies under its control referred to in this contract as sub-Agencies, but the span of control can be deeper than these two levels. Each Agency or Sub-Agency defines the number of levels and use of those levels (i.e., invoicing or reporting) depending on its own needs. The Agency's location in the Government hierarchy is defined by the AHC, which is described in detail in Attachment J.11, Glossary of Terms.

An Agency at the highest level can impose a hierarchical Agency structure across its entire hierarchy or can allow each level to redefine its own hierarchical structure to meet its own needs. Agencies require either invoices or reports at various levels of their hierarchy and these levels are not always consistent across the hierarchy.

Agencies and Sub-Agencies at lower levels within the Government hierarchy may not be aware of restrictions imposed at higher levels. The contractor, however, will have interaction at all levels, so it needs to be aware of the structure and meaning of the Agency hierarchy code in each situation.

This information is used by the contractor to ensure that billing hierarchies are consistently applied at the time an order is accepted and billed.

**Ordering Data.** All Agencies, plus the GSA, require ordering data to support all processes on a continuous basis. Ordering Data requirements include data for the

Order and data for each of the acknowledgements required by this contract. In general, each acknowledgement builds on the data provided in the previous one and the final acknowledgement, the Service Order Completion notice (SOCN) contains all the information related to the order and delivery of the service.

Recognizing the variability of both contractor ordering systems and Agency ordering systems and manual processes, this contract does not impose the number of physical files (i.e. a single common format for every service), but focuses instead on the data elements required by the Government, the need for current data dictionaries, mapping and processing rules to enable the Government to interpret and process the ordering data. The contractor will provide its Data Dictionary Package as part of its initial proposal. In addition, this contract is expected to support Government efforts to automate both ordering and billing processes, so all files must be able to be loaded into Government database applications, in order to accomplish these processes.

The contractor's Data Dictionary Package for Ordering consists of a data dictionary for each of the contractor's required files, sample data for each required file, a mapping specification for each of the Government's logical files (e.g., Order, Service Order Completion Notice) and their data elements, instructions for changes, and additional descriptive information. The data dictionary describes the required file and its data elements sufficiently to indicate how the Government's logical file and data elements map to the contractor's required file and its elements. The data dictionary also contains the formats for each element and a translation of all code values for all data elements. The Data Dictionary Package presents sample data for each service on the contract in electronic files using the same structure as the files the contractor will provide to the Government during operations. The Government uses these files of sample data to validate that the Data Dictionary Package meets the requirements and to develop and test the Government's internal systems that will process the data. The mapping specification explains how the contractor will accommodate mapping the Government's data elements to the contractor's required files and elements. The instructions describe and highlight changes--, including additions and deletions,-- to the Data Dictionary Package. In addition, the contractor must provide additional descriptive information that facilitates the Government's understanding and review of the Data Dictionary Package

In all situations, ordering data (order plus acknowledgements) must be sufficient to allow the Government to:

- Ensure that the requested service has been ordered.
- Verify billing information back to a service order
- Conduct accurate Inventory Management
- Support shared tenant billing arrangements

For data file downloading or data file delivery, the contractor is required, at a minimum, to support file formats for Microsoft Excel 2002, Comma Separated Values (CSV) with field names included or tab delimited ASCII text file with field names included.

**Contract Line Item Number (CLIN).** The CLIN is highly critical to the Government's effort to automate ordering, billing, and inventory verification. The SOCN is the Government's record of the order. The contractor will provide in the SOCN every CLIN it intends to bill for and all the data elements required to verify the correct CLIN has been used. Additionally, all CLINs must be provided in the SOCN even when the price is zero or the item is not separately priced.

### **Unique Billing Identifiers (UBI)**

The purpose of a UBI is to uniquely identify a single service and all components of that service separately from all other services being provided from within that same category of Network services. The contractor must provide a Unique Billing Identifier (UBI) to identify each billed record. The Government requires the contractor to assign a unique identifier for each component of the billed service that map to the UBI. The contractor may use existing fields in its systems to provide the UBI. The contractor is allowed to determine the form of the UBI for each service (especially those with multiple components) and must provide it on the Service Order Completion Notice as well as in the Detail Billing file. The contractor will provide GSA and the customer Agency any change to the UBI and any of its' associated components via the SOCN.

As an example, two similar orders for Frame Relay Services that are to be provided at the exact same address will each be uniquely identified so they can be easily separated on the bill. The contractor may elect to create a Unique Billing Identifier field, rather than using existing data elements, but at no charge to the Government. Examples of a UBI Include: A UBI could be a Circuit ID, a Phone number, an AHC, or a combination of elements. A UBI could represent a service consisting of a combination of an access circuit, a Private Virtual Circuit (PVC) and the Service Enabling Device (SED) that supports it. A UBI could represent a managed network service or project arrangement that includes any number of components, features and services and could be an ICB CLIN combined with its Case Number.

**Other Contract Areas that Affect Ordering.** Section C.3.6.4, Shared Tenant Billing defines the requirements for billing of shared tenant services. In addition, Service Ordering is affected by the requirement that the billing start date may not precede the completion date on the Service Order Completion Notice (SOCN), and billing end date must be the actual disconnect date indicated on the SOCN. In Sections G.4, Ordering and G.5, Billing additional ordering requirements are included, including storage and archival requirements. Attachment J.12.1, Ordering Data Elements contain the definition of all data elements for the order; Attachment J.12.2, Acknowledgement Data Elements contains all the data elements for all of the order acknowledgements, and Attachment J.12.3, Service Provisioning Intervals defines completion timeframes associated with orders. C.2, Technical Requirements defines Performance Metrics for services that can be ordered. Availability for the Ordering System is in Section C.3.9, Operational Support Systems. Security requirements for Ordering System are in Section C.3.9, Operational Support Systems, and C.3.3.2, Security Management. Service Level Agreements that apply to the Ordering functions are defined in Attachment J.13, Service Level Agreements. Section H.12, Key Personnel and Corporate Structure defines contractor Service Order Manager Requirements.

### C.3.5.1 Direct Ordering

#### C.3.5.1.1 Direct Ordering Process Definition

##### C.3.5.1.1.1 Direct Ordering Process Description

The Agency may order directly from the contractor, using a process known as “direct ordering.” The direct ordering process is described in this section. Included are a functional requirements specification and a description of the required:

1. Data elements;
2. Acknowledgements;
3. Reports, and
4. Government/contractor ordering interface.

The minimum data elements required for ordering and acknowledgements are specified in Attachments J.12.1 Ordering Data Elements and J.12.2 Acknowledgement Data Elements. The contractor’s Data Dictionary Package is included in the contract at award based on what was submitted in the proposal, and the contractor provides updates as required.

##### C.3.5.1.1.2 Direct Order Process Narrative

Step Number	Description	Executing Entities
1	Contractor establishes environment to support ordering.	Contractor / GSA / Agency
1.1	Contractor provides Data Dictionary Package for Ordering.	Contractor
1.2	Agency registers with contractor for ordering.	Agency / Contractor
1.3	Contractor establishes an ordering system.	Contractor
2	Agency places order and contractor provides Agency with acknowledgements.	Agency / Contractor
2.1	Contractor provides an Order Receipt Acknowledgement to the Agency.	Contractor
2.2	Contractor reviews order validity.	Contractor
2.3	Contractor provides a Service Order Confirmation to the Agency or an Order Rejection Notice.	Contractor
2.4	Agency, at its option and if necessary, may correct an order.	Agency / Contractor
2.5	Contractor provides Agency with a Firm Order Commitment Notice.	Agency / Contractor
2.6	Contractor provides a SOCN to Agency and GSA.	Agency / Contractor
3	Agency may place change orders.	Agency
4	Agency may cancel orders.	Agency / Contractor
5	Agency may delay customer want date.	Agency / Contractor
6	Agency may place Expedited and Telecommunication Service Priority Orders (TSP).	Agency / Contractor
7	Agency may place multiple orders simultaneously.	Agency / Contractor
8	Agency may place disconnect orders.	Agency /



Step Number	Description	Executing Entities
		Contractor
9	Agency may track an order	Agency / Contractor
10	Contractor provides Order Processing Performance Reports to GSA.	Contractor
11	Contractor provides Agency-Specific Order Processing Performance Reports to Agency.	Contractor
12	Contractor provides subscriber registration, reservation, configuration changes, and network expansion for Network Services.	Contractor Agency
13	Agency may order services with Individual Case Basis (ICB) Pricing.	Contractor Agency

### C.3.5.1.2 Direct Ordering Functional Requirements

The functional requirements of each step of the direct ordering process are specified in this section.

#### C.3.5.1.2.1 Step 1--Contractor Establishes Ordering Environment

ID Number	Description
1	The contractor shall provide a point of contact, the Service Ordering Manager, in accordance with Section H.12, Key Personnel and Corporate Structure.
2	The contractor shall establish an automated ordering capability.
3	In the event an Agency needs additional data regarding a site in order to prepare a complete order, the Agency may elect to order a site survey from the contractor. The contractor shall complete the site survey and provide a report of the resulting data requested by the Agency at the time of ordering the site survey.

#### C.3.5.1.2.1.1 Step 1.1--Contractor Provides Data Dictionary Package for Ordering

ID Number	Description
1	The contractor shall provide a Data Dictionary Package for Ordering, including any changes required by the Government, and update thereafter as changes occur. See Section C.3.5.1.3.2, Contractor Data Provided to Government.
2	The contractor shall define a specific data element or data elements to create a UBI that uniquely identifies the combination of the following: [1] service type; [2] service location; and [3] Agency to which the service belongs. (Examples may include circuit ID, phone number, Contractor Service Account number, etc.). See additional guidance in the introduction to Section C.3.5, Service Ordering.
3	The contractor shall include the same UBI in both the Service Order Completion Notice (SOCN) and the Detail Billing File(s).
4	When an Agency is conducting Fair Opportunity or has selected the contractor, the Agency may request the contractor's Data Dictionary Package for Ordering. The contractor shall provide the Data Dictionary Package for Ordering to the Agency as specified in Section C.3.5.1.3.2.1 Data Dictionary Package for Ordering (identical to that provided to GSA).
5	In the Data Dictionary Package for Ordering, the contractor shall provide a mapping specification that maps the Government's logical file names and the data elements contained in the logical files to the contractor's required file names and the data elements contained in the required files, including a service-by-service mapping of the UBI.

ID Number	Description
6	The contractor shall provide a Data Dictionary Package for Ordering containing at a minimum for each logical file, a description of each of the contractor's required files and for each data element contained within the file, the data element field name, field length, field type, field characteristics, and a description of the data that could be populated in the field that is sufficient to map the Government's data elements to the data elements in the contractor's required files.
7	The contractor shall include within the data dictionary a translation of all ordering codes used by the contractor's ordering system as they apply to the coding of the ordering data elements of this contract.
8	The contractor shall provide updates to the Data Dictionary Package for Ordering, including but not limited to data elements, sample data and file layouts to both GSA and Agencies; the contractor shall indicate all changes in detail at the beginning of the documents indicating changes in the body of the document.
9	The contractor shall provide instructions with the Data Dictionary Package for Ordering that presents the details of each change and indicates the importance of each of the changes so that they may easily be identified.
10	The contractor shall provide sample data for all of the contractor's required files by including in the Data Dictionary Package electronic files in the same structure as the contractor's required files and populated with representative data values that include all services on the contract. These files of sample data will enable the Government to develop and test internal systems that process the data.
12	The contractor shall provide additional descriptive information in the Data Dictionary Package for Ordering that will enable the Government to easily interpret the contents.

#### C.3.5.1.2.1.2 Step 1.2--Agency Registers with Contractor for Ordering

ID Number	Description
1	After Notice to Proceed and ongoing as required, the contractor shall accept from the Agency/Sub-Agency the name of the DAR Administrator, who is the person authorized to provide and maintain the DAR list and provides authorization for people to have "read only" access to the contractor's system. In some cases, a DAR Administrator is also a DAR.
2	The contractor shall accept from the Agency DAR Administrator its requirement for its Agency and Sub-Agencies to be direct-billed or centrally billed. See Sections C.3.6.1, Direct Billing and C.3.6.2, Centralized Billing.
3	After Notice to Proceed, the contractor shall accept from the Agency DAR Administrator the Agency Hierarchy Code List, the list of valid AHCs for the Agency/Sub-Agency. (See Section C.3.5.1.3.1, Agency Data to Provided to contractor)
4	The contractor shall accept from the Agency its hierarchical billing requirements, including, at a minimum, at what levels invoices are to be produced and at what levels informational summaries are to be produced.
5	The contractor shall accept updates from the Agency/Sub-Agency DAR to the list of valid AHCs.
6	The contractor shall validate AHCs used in subsequent ordering files against the list of valid Agency Hierarchy Codes provided
7	The contractor shall make the AHC changes within the billing period requested by the Agency. An AHC change must not require a service interruption for any given service or service type on the contract.
8	Following a request by an Agency to modify an AHC, the contractor shall notify the GSA and Agency by way of a Service Order Completion Notice (SOCN) within one (1) business day after making changes to any of the Agency's existing AHCs, or its intention to use additional AHCs. (See Section C.3.5.1.2.2, Agency Places Order and Contractor Provides Acknowledgements.)
9	After Notice to Proceed, the contractor shall accept from the Agency DAR

ID Number	Description
	Administrator a list of DARs. See Section C.3.5.1.3.1, Agency Data Provided to Contractor.
10	The contractor shall accept updates to the list of valid DARs as necessary, by way of DAR Forms. (See Section C.3.5.1.3.1, Agency Data Provided to Contractor)

### C.3.5.1.2.1.3 Step 1.3-- Contractor Establishes an Ordering System

ID Number	Description
1	The contractor shall provide users access to a secure, online, internet-accessible electronic ordering system that meets the performance requirements of Section C.3.9, Operational Support Systems. This system will provide Order entering, viewing, printing, tracking and downloading capabilities.
1.1	The contractor shall have a process to serve users who choose not to order online.
1.2	The contractor shall provide online ordering template for manual orders and instructions for completing the template.
1.3	The contractor's system shall accept orders from Agencies as specified in Section C.3.5.1.3.1, Agency Data Provided to Contractor.
2	The contractor shall provide an ordering system that provides users with a web based means of obtaining price quotes for simple price quotes.
2.1	The contractor shall provide a means of viewing the current pricing information included in the Contractor's Pricing Volume.
2.2	The contractor shall provide a means of viewing historical pricing available for all previous contract years for all services available for ordering from the contractor.
2.3	The price quotes provided by the contractor shall allow users to rely on them when executing the Fair Opportunity process or when verifying an invoice. The price quotes shall have accurate current prices provided at the CLIN level.
2.4	During the same session, the contractor shall provide a capability that allows users to enter order requirements solely for the purpose of obtaining price quotes, for the purpose of obtaining price quotes and ordering the items quoted, or ordering without a price quote.
2.5	The contractor shall provide complex price quotes within a time period acceptable by the Government and simple price quotes immediately via the web-based tool.
2.6	The contractor shall provide a price quote capability for all CLINs in the contract.
2.7	For price quotes that contain dedicated access, the contractor's price quote shall be based on the SWC as determined by the procedures in Section C.3.2.2.10, Step 11: Network Inventory Codes.
3	The contractor shall provide an ordering system that allows Agencies to place change orders, correct orders, cancel orders, order expedited processing, place multiple orders simultaneously, place disconnect orders, and track orders. Detailed requirements for each of these situations follow throughout Section C.3.5.1.2, Direct Ordering Functional Requirements.
4	The contractor shall provide a system that accepts a user registration from the Agency that establishes a profile of each user and complies with Section C.3.5.1.3.1.1 User Registration for Ordering.
5	The contractor shall create a system account for each DAR Administrator that the Agency identifies within five business days of receiving the DAR Administrator's name from the Agency.
6	The contractor shall provide each DAR Administrator with individual "system" access information (for example, the DAR Administrator's user name and password) via internet electronic mail sent directly to the DAR Administrator's electronic mail address.

ID Number	Description
7	The contractor shall provide an ordering system that provides security requirements consistent with Sections C.3.9, Operational Support Systems, and C.3.3.2, Security Management and the following additional user access controls:
7.1	Access controls that prohibit access to the system by any unauthorized user.
7.2	Access controls that will allow individual users only to access portions of system functionality to which they are authorized and that relate to their specific ordering activities.
7.2.1	Access Controls that provide Agency "X" users with access only to portions of system functionality that relate to Agency "X's" activities.
7.2.2	The contractor shall provide specific users with access only to portions of system functionality that relate to their specific activities (e.g., ordering Voice Service), as determined by information in the user's profile.
8	The contractor shall not accept orders or directions that change the requirements of an order unless formally issued by an authorized user, and the Government will not be liable for an adjustment to the price of an order resulting from a change unless an authorized user has authorized the change.
9	The contractor shall provide a system that provides users with direct and immediate access to ordering information provided by the system that they are authorized to access.
10	The contractor shall allow authorized users to query the system for data elements pertaining to orders and acknowledgements and download the query results.
10.1	The contractor shall provide an ordering system that stores all acknowledgement information online and allows individual users to download acknowledgement information related to their ordering activities.
10.2	The contractor shall provide a system that stores all ordering data elements for the length of the contract.
10.3	The contractor shall make ordering data available to the Government within 5 business days after the contractor receives a formal request.
10.4	The contractor shall maintain and retain for ten years from contract termination or expiration copies of all data, letters, electronic mail, memorandums, adjustment data and other data pertaining to the ordering of contract services as specified in Section G.4, Ordering.
10.5	The contractor shall provide reports and data fulfilling requests for archived information and data to the Government in a format acceptable to the Government within 5 business days after receiving the Government's request for ten years from contract termination or expiration.

#### C.3.5.1.2.2 Step 2--Agency Places Order and Contractor Provides Agency with Acknowledgements

ID Number	Description
1	When Agencies send ordering data to the contractor using a non-electronic medium, the contractor shall enter the order into its online ordering system within 3 business days.
2	The contractor shall accept orders from Agencies containing the data elements specified in Attachment J.12.1, Ordering Data Elements.
3	The contractor shall provide the ordering Agency with all acknowledgements and provides GSA with the SOCN.
4	The contractor shall provide acknowledgements that shall contain the applicable data elements specified in Attachment J.12.2, Acknowledgement Data Elements to the proper Agency personnel, as mutually agreed upon between the contractor and the ordering Agency.

ID Number	Description
1	When Agencies send ordering data to the contractor using a non-electronic medium, the contractor shall enter the order into its online ordering system within 3 business days.
5	The contractor shall provide acknowledgements to the Agency in accordance with Section C.3.5.1.3.4.2 Acknowledgements
6	If the ordering Agency does not specify a media type for its acknowledgements, the contractor shall provide this information online.
7	The contractor shall provide each acknowledgement to up to five designated Agency personnel, as mutually agreed upon between the contractor and the ordering Agency.
8	The contractor shall provide an external title or subject line for all acknowledgements that includes the type of acknowledgement, an identifier (e.g. ASRN, contractor order number) and date and time stamp.
9	The contractor shall accept bulk orders and process each bulk order as a single order.
9.1	The contractor shall accept a single order for multiple instances of the same service from a single ordering Agency (bulk order) in accordance with Section C.3.5.1.3.1.2 Order.
9.2	The contractor shall accept a single ASRN for a bulk order.
9.3	The contractor shall accept a bulk order placed by an Agency via the contractor's electronic ordering system specified in Section C.3.5.1.2.1, Step 1 - Contractor Establishes Ordering Environment.
9.4	The contractor shall perform all the requirements of Section C.3.5.1.2.2, Step 2 - Agency Places Order and Contractor Provides Agency with Acknowledgements for the bulk order as a single order.

### C.3.5.1.2.2.1 Step 2.1--Contractor Provides Order Receipt Acknowledgement to the Agency

ID Number	Description
1	The contractor shall provide the ordering Agency with an Order Receipt Acknowledgement within one business day of receiving an order from the Agency.
2	The contractor shall provide an Order Receipt Acknowledgement for each order it receives from an Agency.
3	The contractor shall provide Order Receipt Acknowledgements containing the data elements specified in Attachment J.12.2, Acknowledgement Data Elements and in accordance with Section C.3.5.1.3.4.2 Acknowledgements.

### C.3.5.1.2.2.2 Step 2.2--Contractor Reviews Order Validity

ID Number	Description
1	No later than five business days after receiving the order, the contractor shall review the order and determine whether it is valid according to the requirements of Section C.3.5, Service Ordering. The Government will not be held liable for any charges resulting from the processing of an invalid order.
2	The contractor shall validate the contents of each data element in the order.
3	The contractor shall determine that an order is invalid if, in the judgment of the contractor, the contents of one or more data elements in the order appear to be incorrect, incomplete, inaccurate, or otherwise insufficient.
4	When reviewing order validity, the contractor shall pay particular attention to the accuracy and completeness of the Agency Hierarchy Code(s) (AHC(s)) and user authorizations as defined in Section C.3.5.1.2.1.3, Step 1.3 -- Contractor Establishes Ordering System. See also Attachment J.11, Glossary of Terms.
4.1	The contractor shall determine to be invalid any order with an AHC that is incorrect or incomplete, as provided to the contractor by the DAR Administrator or DAR in the Agency Hierarchy Code List.
4.2	The contractor shall determine to be invalid any order containing an AHC that the user is not authorized to provide, based on the profile of the user submitted in the User Registration form.
5	When reviewing order validity, the contractor shall pay particular attention to the service scope and funding authorization of the user.
5.1	The contractor shall determine to be invalid any order placed by a user that is not authorized, based on the profile of the user submitted in the User Registration form, to order the services requested.
5.2	The contractor shall determine to be invalid any order placed by a user that does not identify the correct funding source, based on the profile of the user submitted in the User Registration form.

### C.3.5.1.2.2.3 Step 2.3--Contractor Provides a Service Order Confirmation or an Order Rejection Notice to the Agency

ID Number	Description
1	If the contractor determines that the order is valid, the contractor shall issue within five business days after receiving the order a Service Order Confirmation to the Agency that contains the data elements specified in Attachment J.12.2, Acknowledgement Data Elements and in accordance with Section C.3.5.1.3.4.2 Acknowledgements.
2	The contractor shall contact the Agency within one business day after determining that the order is invalid.

ID Number	Description
3	If the Agency doesn't respond within five business days of the contractor's determination that the order is invalid, the contractor shall provide the Agency with an Order Rejection Notice that contains the data elements specified in Attachment J.12.2, Acknowledgement Data Elements and in accordance with Section C.3.5.1.3.4.2 Acknowledgements.

#### C.3.5.1.2.2.4 Step 2.4--Agency, at Its Option and If Necessary, may **Correct an Order**

ID Number	Description
1	The contractor shall accept from an Agency a correction to an order prior to delivery of the SOCN if a) the contractor rejected the initial order or b) the Agency determines it is necessary to correct the order or change the customer want date (see Section C.3.5.1.2.5, Step 5 – Agency May Delay the Customer Want Date).
2	The contractor shall provide the ordering Agency with an Order Receipt Acknowledgement.
3	The contractor shall review the validity of the corrected order.
4	The contractor shall provide the ordering Agency with an Order Rejection Notice, if necessary.
5	The contractor shall use the same Agency Service Request Number (ASRN) in the corrected order that was contained in the original order, if an ASRN was provided.
6	The contractor shall use the same contractor-provided Contractor Service Order Number, for tracking purposes, in the corrected order that was provided with the original order, if assigned.

#### C.3.5.1.2.2.5 Step 2.5--Contractor Provides Agency with a Firm Order Commitment Notice

ID Number	Description
1	The contractor shall provide a Firm Order Commitment Notice to the ordering Agency that makes best attempt to meet the customer want date.
2	The Firm Order Commitment Notice shall contain the data elements specified in Attachment J.12.2, Acknowledgement Data Elements and in accordance with Section C.3.5.1.3.4.2 Acknowledgements.
3	The contractor shall provide a firm order commitment date in the Firm Order Commitment Notice that either complies with the implementation interval specified in Attachment J.12.3, Service Provisioning Intervals or is negotiated with the DAR prior to issuance of the Firm Order Commitment Notice.
4	The contractor shall review each order and determine whether the contractor or the Agency is responsible for procuring local access service to deliver ordered services to the Agency.
4.1	If the contractor must procure local access services from another provider to meet the order requirements, the contractor shall obtain a Firm Order Confirmation date from the Local Exchange Carrier(s) (LECs) or other service provider(s) that will provide local access services.
5	When the contractor procures local access services from another provider, the contractor shall provide the Firm Order Commitment Notice to the Agency within one business day of receiving a Firm Order Confirmation date from the LEC or other provider of local access service.

ID Number	Description
6	When the contractor does not procure local access service from another provider, the contractor shall provide its Firm Order Commitment Notice to the ordering Agency within five days after the Service Order Confirmation is provided to the Agency or at least ten business days before the firm order commitment date, whichever comes first.
7	The contractor shall provide an updated Firm Order Commitment Notice to the ordering Agency one business day after becoming aware of any change in its ability to meet the firm order commitment date.
8	The contractor shall not issue the Service Order Completion Notice and begin billing in advance of the firm order commitment date on the Firm Order Commitment Notice unless authorized by the ordering Agency.

**C.3.5.1.2.2.6 Step 2.6--Contractor Provides a Service Order Completion Notice (SOCN) to Agency and GSA**

ID Number	Description
1	The contractor shall implement the order within the implementation interval established in Attachment J.12.3, Service Provisioning Intervals and defined as the number of calendar days from the Service Order Confirmation date to the completion date of the SOCN.
2	The contractor shall provide the ordering Agency and GSA with a SOCN within one business day after all the components of order are fully implemented, the contractor has completed testing, and the service is ready for the customer's use.
3	If the Agency reports a problem within the Acceptance period in accordance with Section E.4, Verification and Acceptance Testing of Telecommunications Services, the contractor shall fix, test, and send another SOCN with updated information within one business day after the Agency accepts the repaired service.
4	If the Agency acceptance period has elapsed in accordance with Section E.4, Verification and Acceptance Testing of Telecommunications Services, the contractor shall begin billing on the completion date.
5	The contractor shall provide a SOCN for each order it fulfills under this contract.
6	The SOCNs that the contractor provides shall contain the data elements specified in Attachment J.12.2, Acknowledgement Data Elements and in accordance with Section C.3.5.1.3.4.2, Acknowledgements.
7	The contractor shall provide the UBI in the SOCN.
8	The contractor shall provide in the SOCN every ordered CLIN it intends to bill for.
9	The contractor shall provide in the SOCN all ordered CLINS for services even when the price is zero or the item is Not Separately Priced (NSP).
10	The contractor shall provide in the SOCN, for each ordered CLIN, all the data elements that are required by Section B, Pricing to accurately verify the price of each service except for usage-based services.
11	If the contractor makes any change to the information provided on the SOCN at any time, then the contractor shall provide a revised SOCN within one business day.

**C.3.5.1.2.3 Step 3-- Agency May Place Change Orders**

ID Number	Description
1	The contractor shall accept orders from Agencies to change orders. For example: ADMINISTRATIVE CHANGES:
1.1	The contractor shall accept orders to change the AHC of a previously completed order.



ID Number	Description
1.2	The contractor shall accept orders to change the DAR or Agency Contracting Officer responsible.
	SERVICE CHANGES:
1.3	The contractor shall accept orders to change any other Agency-defined fields, such as the location of a Service Delivery Address.
1.4	The contractor shall accept orders to add services, features, or equipment to an existing order.
2	The contractor shall process change orders in accordance with the requirements of Section C.3.5.1.2, Direct Ordering Functional Requirements.
3	The contractor shall accept the ASRN in the change order even if it is the same as was contained in the original order.
4	The contractor shall provide the ordering Agency with all acknowledgements in accordance with Attachment J.12.2, Acknowledgement Data Elements and Section C.3.5.1.2.2, Step 2 – Agency Places Order and contractor Provides Acknowledgements.

#### C.3.5.1.2.4 Step 4: Agency May Cancel Orders

ID Number	Description
1	The contractor shall accept an order from an Agency to cancel a pending order at any step of the order process prior to service acceptance.
2	If the contractor determines that a cancellation order is valid, the contractor shall not complete the implementation of the service required by the initial order.
3	The contractor shall not charge the ordering Agency for service required by the initial order under either of the following conditions:
3.1	The network access and/or transport bandwidth of the service required by the initial order was less than T1 and the ordering Agency placed the cancellation order ten or more business days before the later of: (a) the customer want date in the initial order; or (b) the firm order commitment date. See Section B.6, General Pricing and Other Elements.
3.2	The network access and/or transport bandwidth of the service required by the initial order was T1 or above and the ordering Agency placed the cancellation order thirty or more business days before the later of: (a) the customer want date in the initial order; or (b) the firm order commitment date. See Section B.6, General Pricing and Other Elements.

#### C.3.5.1.2.5 Step 5: Agency May Delay the Customer Want Date

ID Number	Description
1	An Agency may delay the original customer want date by correcting an order in accordance with Section C.3.5.1.2.2, Step 2 -- Agency Places Order and Contractor Provides Agency with Acknowledgements. If the Agency delays the customer want date prior to receiving the Firm Order Commitment Notice, the contractor shall not issue the Service Order Completion Notice and begin billing prior to the new customer want date, except as noted in ID Number two below.
2	If the Agency delays the customer want date fewer than ten business days before the later of: (a) the customer want date in the initial order; or (b) the firm order commitment date, the contractor may invoice the ordering Agency pass through of actual costs without overhead for local access service required by the initial order. See Section B.6, General Pricing and Other Elements.

**C.3.5.1.2.6 Step 6: Agency May Place Expedited and TSP Order Processing**

ID Number	Description
1	The contractor shall provide two classes of expedited service implementation, hereinafter referred to as Class A and Class B, for all services ordered by Agencies under this contract.
2	The contractor shall meet reduced contractual service implementation intervals when fulfilling an expedited order.
3	The contractor shall provide Class A expedited service implementation when the ordering Agency requires priority provisioning for National Security / Emergency Preparedness (NS/EP) circumstances or other circumstances in which the Telecommunications Service Priority (TSP) system is invoked.
3.1	The contractor shall make best effort to implement the ordered service(s) by the customer want date, based on essential priorities as certified by the DAR, and not later than the expedited provisioning interval in Attachment J.12.3, Service Provisioning Intervals.
3.2	The contractor shall charge the price in the contract for expedited order.
4	The contractor shall provide Class B expedited service implementation when the ordering Agency requires priority provisioning due to potential hardship to the Agency, however not due to circumstances covered by TSP.
4.1	The contractor shall develop a proposed Class B expedite schedule based on a customer want date and provide the proposed schedule to the DAR.
4.2	The contractor may charge the ordering Agency the NRC for Class B expedited service implementation, as specified in the Price Volume of the contract, after the contractor provides the Service Order Confirmation, even if the ordering Agency subsequently cancels the order.
4.3	The contractor shall not charge the ordering Agency the NRC for Class B expedited service implementation if the contractor fails to meet the service provisioning interval for class B expedited orders in Table J.12.3-1.

**C.3.5.1.2.7 Step 7: Agency May Place Multiple Orders Simultaneously**

ID Number	Description
1	The contractor shall accept from a single ordering Agency multiple orders contained in a single file in accordance with Section C.3.5.1.3.1.2 Order.
2	The contractor shall process each individual order within the file separately, according to the requirements of Section C.3.5.1.2, Direct Ordering Functional Requirements, which includes but is not limited to the following: Order Receipt Acknowledgement, Service Order Confirmation, Firm Order Commitment Notice, and SOCN for each of the orders.

**C.3.5.1.2.8 Step 8: Agency May Place Disconnect Orders**

ID Number	Description
1	The contractor shall accept orders from Agencies to disconnect orders at any time.
2	Billing for the services that are to be disconnected must stop on the completion date in the Service Order Completion Notice and within the Provisioning Intervals for Disconnects as specified in Attachment J.12.3, Service Provisioning Intervals.

**C.3.5.1.2.9 Step 9: Agency May Track an Order**

ID Number	Description
1	The contractor shall provide a means for the user to track the status of each order the user is authorized to monitor from the time the Service Order Confirmation is issued to the expiration of the contract.
2	Access to this information shall be via the contractor's online system or via a Customer Service Representative during normal business hours.
3	If the user requests status information regarding an order, the contractor shall provide the status information within one hour during normal business hours.
4	The order status information provided by the contractor shall be in accordance with Section C.3.5.1.3.4.3 Order Tracking Status.

**C.3.5.1.2.10 Step 10: Contractor Provides Order Processing Performance Report to GSA**

ID Number	Description
1	The contractor shall provide to GSA, on a monthly basis, an Order Processing Performance Report documenting the contractor's performance against contractual requirements for ordering, during any month in which the contractor received, processed, or completed orders under this contract.
2	The contractor shall provide the Order Processing Performance Report in accordance with Section C.3.5.1.4.1.1, Order Processing Performance Report.,
3	Each Order Processing Performance Report shall document the contractor's order processing performance for the prior calendar month.
4	The order status information provided by the contractor shall be in accordance with Section C.3.5.1.3.4.3 Order Tracking Status.

**C.3.5.1.2.11 Step 11: Contractor Provides Agency-Specific Order Processing Performance Reports to Agency**

ID Number	Description
1	At the request of a user, the contractor shall provide an Agency-Specific Order Processing Performance Report to the Agency in accordance with Section C.3.5.1.4.1.1, Order Processing Performance Report.
1.1	The contractor shall provide an Agency-Specific Order Processing Performance Report to the Agency that includes data that pertains only to the specific ordering activities of the ordering Agency, as indicated by the AHC.

**C.3.5.1.2.12 Step 12 -- Contractor Provides Subscriber Registration, Reservation, Service Configuration, Reporting, and Network Expansion Capabilities**

ID Number	Description
1	The contractor shall provide subscriber registration capabilities for all of the Network services that require subscriber registration (e.g. Calling Cards).
2	The contractor shall provide reservation capability for all services that have a reservation capability (e.g. teleconferencing).

ID Number	Description
3	The contractor shall provide Agency controlled configuration changes for all services that support it (e.g. change routing for Toll free service).
4	The Contractor shall provide Agency initiated network expansion capabilities for all services that allow a customer to initiate them (e.g. add a "hot spot" for MWLANS).
5	The contractor shall accept subscriber registrations only from an Agency DAR.
6	The contractor shall accept reservations, Agency controlled configuration changes, and Agency initiated network expansion capabilities from Agency DARs or registered users.
7	The contractor shall provide reports for all services which have reporting capability (e.g. Toll-free)

### C.3.5.1.2.13 Step 13 -- Agency may order services with ICB Pricing

ID Number	Description
1	With custom design work or in situations where a service or feature is priced on an individual case basis (ICB), the contractor shall provide to the Government an ICB Case number as outlined in Section B.1.2
2	The ICB Case Number shall be an integer between 1 and 2,147,483,647, inclusive.
3	The ICB Case Number must be unique by CLIN within each contract. The ICB CLIN/ICB Case Number pair must have the same meaning and unit price each time it appears.
4	The contractor shall update its ordering system to include this ICB case number and price and validate orders for the ICB service against the ICB case number and associated price.
5	The contractor shall provide, in addition to the required data elements for ordering, the CLIN, the ICB Case Number, and the price on each of the acknowledgements sent to the Agency.

### C.3.5.1.3 Direct Ordering Data Requirements

#### C.3.5.1.3.1 Agency Data Provided to Contractor

##### C.3.5.1.3.1.1 User Registration for Ordering

##### C.3.5.1.3.1.1.1 Frequency - User Registration for Ordering

- As required

##### C.3.5.1.3.1.1.2 Media/Transport/Format – User Registration for Ordering

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> </ul>	

Data		
Media	Transport	Format
	<ul style="list-style-type: none"> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>Other formats as mutually agreed between Agency and Contractor</li> <li>XML</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>Other formats as mutually agreed between Agency and contractor</li> <li>XML</li> </ul>
Voice	<ul style="list-style-type: none"> <li>Telephone</li> <li>In person</li> </ul>	Not Applicable

\*Media type changes per section C.3.1.2

### C.3.5.1.3.1.1.3 Record Elements – User Registration for Ordering

ID Number	Data Elements	Description
1	Agency	Agency
2	Name	Name
	Title	DAR Administrator, DAR, Agency Contracting Officer, Service Coordinator (SC), Local Government Contact (LGC), Alternate Government Contact(ALGC), Local Technical Contact (LTC)
	Type of Access	System, "order entry", "read only"
3	Address of Named User	
4	Mailing Address	
5	City	

ID Number	Data Elements	Description
6	State	
7	Telephone number	
8	Zip Code	
9	Facsimile number	
10	Internet electronic mail address	
11	Status	Status as an employee or contractor of the Agency
12	Media preference	Media preference for delivery of required order processing data items (for example, acknowledgements) in accordance with Section C.3.5.1.3.4
13	Funding authority	Source of the funding that will pay for the order (e.g. Government purchase order number).
14	Service scope	Authorization to order specified Network services
15	Organizational scope	Agency Hierarchy Codes (AHCs – see Attachment J.11, Glossary of Terms) or levels within AHCs that define the organizational scope of the user's ordering authority.
16	Contractor	Contractor Name / Contract Number

**C.3.5.1.3.1.2 Order**

**C.3.5.1.3.1.2.1 Frequency – Order**

- As required

**C.3.5.1.3.1.2.2 Media/Transport/Format – Order**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97</li> </ul>

Data		
Media	Transport	Format
Email Server	(SMTP) <ul style="list-style-type: none"> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>
Voice	<ul style="list-style-type: none"> <li>Telephone</li> <li>In person</li> </ul>	Not Applicable

\*Media type changes per section C.3.1.2

#### C.3.5.1.3.1.2.3 Record Elements – Order

The Agency will enter data that applies to the service type being ordered. See Attachment J.12.1, Ordering Data Elements for a listing of the ordering data elements that may be entered.

#### C.3.5.1.3.1.3 Agency Hierarchy Code List

##### C.3.5.1.3.1.3.1 Frequency - Agency Hierarchy Code List

- As required

##### C.3.5.1.3.1.3.2 Media/Transport/Format – Agency Hierarchy Code List

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> </ul>

Data		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

### C.3.5.1.3.1.3.3 Record Elements – Agency Hierarchy Code List

ID Number	Data Elements	Description
1	File Name	(Agency Bureau Code) AHCList (example: 4700AHCList)
2	Date	Date current list was created or updated
3	AHC(s)	Agency Hierarchy Code(s) (all levels must be reported)
4	AHC(s) Name	Name of Agency/Sub-Agency/reporting unit(s)
5	Billable Level	Whether this is a Billable level of the Agency Hierarchy Code Codes: Y or N
6	Cent/Dir	Whether this is a Centralized or Direct billed Agency Hierarchy Code Codes: C or D
7	DAR Administrator	DAR Administrator's name
8	POC	Name of Agency Point of Contact of list creator/updater
9	POC Phone	Agency POC Phone number
10	POC Email	Agency POC Electronic mail address
11	Contractor	Contractor Name and Contract Number

### C.3.5.1.3.1.4 Designated Agency Representative List

#### C.3.5.1.3.1.4.1 Frequency - Designated Agency Representative List

- As required

#### C.3.5.1.3.1.4.2 Media/Transport/Format – Designated Agency Representative List

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> </ul>



Data		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

#### C.3.5.1.3.1.4.3 Record Elements – Designated Agency Representative List

ID Number	Data Elements	Description
1	File Name	(Designated Agency Representative) DARList
2	DAR Name	Designated Agency Representative's Name
3	DAR Agency	DAR's Agency's Name
4	DAR AHC	Highest AHC level at which the DAR is authorized to order services
5	DAR Address	DAR Mail Stop and Street Address
6	DAR City	DAR City
7	DAR State	DAR State
8	DAR Zip	DAR Zip Code
9	DAR Phone	DAR Phone Number
10	DAR Email	DAR Electronic mail Address
11	POC	Name of Agency Point of Contact of list creator/updater
12	POC Phone	Agency POC Phone number
13	POC Email	Agency POC Electronic mail address
14	DAR Administrator	DAR Administrator's Name
15	Contractor	Contractor Name / Contract Number

#### C.3.5.1.3.1.5 DAR Form

##### C.3.5.1.3.1.5.1 Frequency - DAR Form

- As required

##### C.3.5.1.3.1.5.2 Media/Transport/Format – DAR Form

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> </ul>

Data		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

### C.3.5.1.3.1.5.3 Record Elements – DAR Form

ID Number	Data Elements	Description
1	Agency	DAR's Agency's Name
2	DAR Name	Designated Agency Representative's Name
3	DAR Address	DAR Mail Stop and Street Address
4	DAR City	DAR City
5	DAR State	DAR State
6	DAR Zip	DAR Zip Code
DAR Phone Number 8	DAR Phone	DAR Phone Number
9	DAR Email	DAR Electronic mail Address
10	DAR Fax	DAR Facsimile Number
11	Status	Status as an employee or contractor of the Agency
12	Media Preference	Media preference for delivery of required order processing data items (for example, acknowledgements) in accordance with Section C.3.5.1.3.4
13	Funding Authority	Source of the funding that will pay for the order (e.g. Government purchase order number)
14	Service Scope	Authorization to order specified Network services
15	Organizational Scope	Agency Hierarchy Codes (AHCs – see Attachment J.11, Glossary of Terms) or levels within AHCs that define the organizational scope of the user's ordering authority.
16	Contractor	Contractor Name/ Contract Number

### C.3.5.1.3.2 Contractor Data Provided to Government

#### C.3.5.1.3.2.1 Data Dictionary Package for Ordering

The Data Dictionary Package for Ordering consists of a contractor data dictionary for each file provided by the contractor, sample data for each file, a mapping table for each ordering file required by the GSA and Agencies (e.g., Order, Order Receipt Acknowledgement, Service Order Confirmation, Order Rejection Notice, Firm Order Commitment Notice, Service Order Completion Notice) and instructions. It is the format for delivering all Direct-ordered data files, and includes all new data elements and all code values (both old and new) for all data elements. Changes, additions and deletions are to be detailed in the instructions and highlighted in the Data Dictionary Package. In

In addition, the contractor may provide additional descriptive documentation that will facilitate the Government's review of the Data Dictionary Package for Ordering.

**C.3.5.1.3.2.1.1 Frequency – Data Dictionary Package for Ordering**

- Initial:
- Sent to GSA: Included at Contract Award
- Sent to Agency: After Notice to Proceed and within 5 business days of Agency request
- Revised: GSA only, 5 business days after receiving GSA comment
- Updated: As changes occur, no less than 60 calendar days prior to implementation; updates due to changes in standards or introduction of new services no more than once every 60 days

**C.3.5.1.3.2.1.2 Deliver To – Data Dictionary Package for Ordering**

- GSA PMO
- Agency, as requested

**C.3.5.1.3.2.1.3 Media/Transport/Format – Data Dictionary Package for Ordering**

**C.3.5.1.3.2.1.3.1 Media/Transport/Format – Data Dictionary Package for Ordering sent to GSA**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Attachment to Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
	<ul style="list-style-type: none"> <li>• mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.5.1.3.2.1.3.2 Media/Transport/Format – Data Dictionary Package for Ordering sent to Agency**

Data		
Media	Transport	Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.5.1.3.2.1.4 Record Elements – Data Dictionary Package for Ordering**

ID Number	Data Elements	Description
		(Applies to ID Number 1-10) One is required for each of the contractor-provided files submitted to meet ordering requirements
1	Title	Data Dictionary for Direct Ordering
2	Contractor	Contractor Name / Contract Number
3	File Name	Contractor File Name (if applicable)
4	Date	Date of the Version or Update

ID Number	Data Elements	Description
		Applies to ID Numbers 5-10, One per Data Element
5	Data Element	Data Element Field Name (e.g., network call redirect MRC, etc.)
6	Field Length	Length of the Data Element Field in the Output File
7	Field Type	Field Format Type (e.g., text)
8	Field Characteristics	Field Characteristics (e.g., numerical, number of decimal places, alphabetical, etc.)
		Applies to ID number 9 – one per Code Value
9	Code Value	Code Value (i.e., internal contractor defined alpha/numeric code value such as "151" or "A2169")
10	Data Description	Description of the data that could be populated in the field that is sufficient to map the element to the Government data elements
		(Applies to ID number 11-15 – one for each of the Government Required Ordering Files is required (i.e. Order, Order Receipt Acknowledgement, Service Order Confirmation, Order Rejection Notice, Firm Order Commitment Notice, and Service Order Completion Notice.)
11	Report Title	Mapping Table for (insert Government required file name)
12	Contractor	Contractor Name/Contract Number
13	File Name	Contractor File Name (if applicable)
14	Date	Date of version or Update
15	Government File	e.g. Service Order Completion Notice
		(Applies to ID number 16-20) One for each data element within the Government file (in order according to Attachment J.12) is required.
16	Data Element	Government data element
17	File Name	Contractor file name where element exists for each is located.
18	Contractor Data Element Name	Contractor data element name
19	Mapping Rules	Data transformation or other actions required by Government to locate data element
20	Comments	Note other information that the contractor believes will assist the Government in interpreting the data.
		(Applies to ID number 21-23) One for the entire package as a whole
21	Report Title	Instructions for Data Dictionary Package for Ordering
22	Files and Dates	Name of the contractor files and dates contained in the package
23	Instructions	Changes from the previous version of the package, contact information, names and dates of all files contained in the Data Dictionary Package, any additional information that will assist the Government in interpreting the data dictionary.

### C.3.5.1.3.3 Contractor Data Provided to GSA

**C.3.5.1.3.3.1 Service Order Completion Notice (SOCN)**

**C.3.5.1.3.3.1.1 Frequency – Service Order Completion Notice (SOCN)**

- Initial: One business day after each order is fully implemented, the contractor has completed testing, and the service is ready for the customer’s use.
- Updated: After Agency reports problem, within one business day after the contractor fixes, tests, and Agency accepts the repaired service.

**C.3.5.1.3.3.1.2 Deliver To - Service Order Completion Notice (SOCN)**

- GSA PMO

**C.3.5.1.3.3.1.3 Media/Transport/Format – Service Order Completion Notice (SOCN)**

Data		
Media	Transport	Data Format
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.5.1.3.3.1.4 Record Elements – Service Order Completion Notice (SOCN)**

See Attachment J.12.2.5, Unit 5: Service Order Completion Notice (SOCN).

**C.3.5.1.3.4 Contractor Data Provided to Agency**

**C.3.5.1.3.4.1 Reserved**

**C.3.5.1.3.4.2 Acknowledgements**

The following acknowledgements are required:

- Order Receipt Acknowledgement

- Service Order Confirmation
- Order Rejection Notice
- Firm Order Commitment Notice
- Service Order Completion Notice

**C.3.5.1.3.4.2.1 Frequency – Acknowledgements**

- Order Receipt Acknowledgement: within one business day of receipt of order
- Service Order Confirmation: within five business days of receipt of order
- Order Rejection Notice: within five business days of notifying the ordering Agency that the order is invalid
- Firm Order Commitment Notice:
  - Initial: within five business days after delivery of the Service Order Confirmation or at least ten business days before the firm order commitment date, whichever comes first
  - Updated: within one business day of becoming aware the firm order commitment date needs to be changed
- Service Order Completion Notice:
  - Initial: within one business day after each order is fully implemented, the contractor has completed testing, and the service is ready for the customer's use
  - Updated: After Agency reports a problem, within one business day after the contractor resolves the problem, tests, and Agency accepts the repaired service

**C.3.5.1.3.4.2.2 Deliver To – Acknowledgements**

- Agency,
- Direct-Billed Agency
- PMO, depending on the specific acknowledgement

**C.3.5.1.3.4.2.3 Media/Transport/Format – Acknowledgements**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> </ul>

Data		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.5.1.3.4.2.4 Record Elements – Acknowledgements**

See Attachment J.12.2 Acknowledgement Data Elements for a listing of the data elements that are required.

**C.3.5.1.3.4.3 Order Tracking Status**

**C.3.5.1.3.4.3.1 Frequency – Order Tracking Status**

- One hour after receiving request

**C.3.5.1.3.4.3.2 Deliver To - Order Tracking Status**

- Agency
- Direct-Billed Agency

**C.3.5.1.3.4.3.3 Media/Transport/Format – Order Tracking Status**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97</li> </ul>



Data		
Media	Transport	Format
	<ul style="list-style-type: none"> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>HTML</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> </ul>

Data		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	Not Applicable

\*Media type changes per section C.3.1.2

#### C.3.5.1.3.4.3.4 Record Elements – Order Tracking Status

ID Number	Data Elements	Description
1	Contract Number	Contractor's Contract Number
2	Contractor	Contractor name
3	ASRN	Agency Service Request Number
4	User	Agency DAR or Contracting Officer who is responsible for the order
5	Project Identifier	Agency-assigned project identifier associated with this order, if assigned
6	Contractor Order Tracking Number	Contractor's tracking number for this order
7	Order Type	Identifies whether order is for New services, a Change, a Cancellation or a Disconnect
8	Transition Order	Y/N
9	Shared Tenant Order	Y/N
10	Service	Contract service being provided. See Section C.2 Technical Requirements
11	Firm Order Commitment Date	If this information is available (see Attachment J.12.2.4, Unit 4, Firm Order Commitment Notice.)
12	Status	R = Received; V = Being Validated; C = Confirmed; J = Rejected; P = Being Provisioned; I = Implemented; A = Accepted; D = Disconnected; X = Cancelled.
13	Comments	As appropriate
14	UBI	Unique Billing Identifier (If available).
15	Network Inventory Code(s)	11 character Originating and Terminating location Code(s) for services defined in Section C.3.2
16	Contractor	Contractor Name / Contract Number
17	Title	(As appropriate)
18	As of Date	Date the status is valid

**C.3.5.1.3.4.4 Price Quotes**

**C.3.5.1.3.4.4.1 Frequency – Price Quotes**

- As required

**C.3.5.1.3.4.4.2 Deliver To - Price Quotes**

- Agency
- Direct-Billed Agency

**C.3.5.1.3.4.4.3 Media/Transport/Format – Price Quotes**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually</li> </ul>

Data		
Media	Transport	Format
		agreed between Agency and contractor
Voice	<ul style="list-style-type: none"><li>• Telephone</li><li>• In person</li></ul>	Not Applicable

\*Media type changes per section C.3.1.2

**C.3.5.1.3.4.4.4 Record Elements – Price Quotes**

ID Number	Data Elements	Description
1	Contract Number	Number of contractor's contract number
2	Contractor	Contractor's name
3	Data Elements	data elements, including prices and quantities, of the applicable tables in the Price tables of the contract
4	Quote Valid Dates	contract period over which the price quote applies are to be provided
5	Title	(As appropriate)

**C.3.5.1.4 Direct Ordering Report Requirements**

**C.3.5.1.4.1 Contractor Reports Provided to Government**

**C.3.5.1.4.1.1 Order Processing Performance Report**

**C.3.5.1.4.1.1.1 Frequency - Order Processing Performance Report**

- Initial:
  - Sent to GSA: Within 10 business days after end of calendar month in which orders were received, processed, or completed
  - Sent to Agency: Within 10 business days after end of calendar month in which Agency requests report
- Updated:
  - Sent to GSA: Monthly within 15 business days after end of calendar month, unless no orders were received, processed, or completed
  - Sent to Agency: As needed

**C.3.5.1.4.1.1.2 Deliver To – Order Processing Performance Report**

- GSA PMO
- Agency

**C.3.5.1.4.1.1.3 Media/Transport/Format – Order Processing Performance Report**

**C.3.5.1.4.1.1.3.1 Media/Transport/Format – Order Processing Performance Report sent to GSA**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and</li> </ul>

Report		
Media	Transport	File Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>contractor</li> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.5.1.4.1.1.3.2 Media/Transport/Format – Order Processing Performance Report**

Reports		
Media	Transport	Format
CD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>HTML</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	

Reports		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• Other formats as mutually agreed</li> <li>• between Agency and contractor</li> </ul>

#### C.3.5.1.4.1.1.4 Content – Order Processing Performance Report to GSA

ID Number	Information Elements	Description
1	Title	Order Processing Performance Report
2	Report Period	Month that the data are from
3	System Availability	The availability of the contractor's online ordering system over the reporting interval; i.e., the total hours the system was available for Government use divided by the total hours of the reporting interval.
4	Orders Received	Total number of orders received during the report period (including new, transition, change, shared tenant, cancellation, and disconnect orders)
5	Orders Rejected	Total number of Order Rejection Notices issued for orders received during the report period
6	Expedited Orders Received	Total expedited orders received during reporting interval for: Class A Class B
7	Disconnect Orders Received	Total number of disconnect orders received during the report period
8	Orders Completed	Total number of SOCNs issued during the report period
9	Expedited Orders Completed	Total number of SOCNs issued during the report period for expedited orders Class A Class B
10	On Time Expedited Performance	Number of SOCNs for expedited orders delivered within the intervals in Attachment J.12.3, Service Provisioning Intervals divided by the total expedited orders completed: Class A Class B
11	Late Expedited Order	A listing of all expedited orders not delivered within the intervals in Attachment J.12.3, Service Provisioning Intervals: Class A Class B
12	Disconnect Orders Completed	Total number of SOCNs issued during the report period for disconnect orders
13	On Time Disconnect Performance	Number of SOCNs for disconnect orders delivered within the intervals in Attachment J.12.3, Service Provisioning Intervals divided by the total disconnect orders completed
14	Other Orders Completed	Total orders other than expedited and disconnects received during reporting interval
15	On Time Other-Orders Performance	Number of SOCNs for orders other than expedited and disconnects delivered within the intervals in Attachment J.12.3, Service Provisioning Intervals divided by the total

ID Number	Information Elements	Description
		other orders completed
16	Service Delivery Effectiveness	The number of SOCNs delivered within the intervals specified in Attachment J.12.3, Service Provisioning Intervals, divided by the total number of orders completed during the reporting interval.
17	Excused Late Deliveries	The number and list of SOCNs that were late due to factors beyond the contractor's control (provide an explanation with each affected SOCN)
18	Adjusted Service Delivery Effectiveness	The number of SOCNs delivered within the intervals specified in Attachment J.12.3, Service Provisioning Intervals, divided by (the total number of orders completed during the reporting interval minus the number of late SOCNs due to factors beyond the contractor's control)
19	Customer Satisfaction Measure	Total number of SOCNs delivered by the customer want date divided by orders completed
20	Order Receipt Acknowledgement Timeliness	Number of acknowledgements delivered on time (that is, within one business day of receipt of order) divided by the total number of acknowledgements delivered during the reporting interval.
21	New Registrations	Total number of valid new user registrations to ordering systems
22	Contractor	Contractor Name / Contract Number

#### **C.3.5.1.4.2 Contractor Reports Provided to the Agency**

##### **C.3.5.1.4.2.1 Site Survey Report**

###### **C.3.5.1.4.2.1.1 Frequency – Site Survey Report**

- As requested

###### **C.3.5.1.4.2.1.2 Deliver To – Site Survey Report**

- Direct-Billed Agency
- Agency

###### **C.3.5.1.4.2.1.3 Media/Transport/Format – Site Survey Report**

The contractor shall provide and deliver the Site Survey report to the Agencies in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

###### **C.3.5.1.4.2.1.4 Content – Site Survey Report**

Format will be defined by the requesting Agency.

#### **C.3.6 Billing**

This section applies to all services billed under the Network contract.



The Billing process includes the receipt of invoices and billing data from the contractor, validation and dispute handling and adjustments, support to internal Government re-billing and payment to the contractor by the Government. In addition, it includes the process of allocating charges among Agencies for shared use of Government switches, called Shared Tenant Arrangements. Other billing information is provided in Section G.5 Billing.

The contractor supports the following functions through the development, implementation, and operation of processes and electronic systems that meet the requirements detailed in the sections that follow.

- (1) Section C.3.6.1 Direct Billing
- (2) Section C.3.6.2 Centralized Billing
- (3) Section C.3.6.3 Billing Disputes and Adjustments
- (4) Section C.3.6.4 Shared Tenant Billing

**Agency Hierarchies.** Every order submitted by the Government will contain one or more Agency Hierarchy Codes (AHC), which enable the Government to account internally for charges. The contractor will not be paid for any order the Government accepts without a valid Agency Hierarchy Code. The contractor validates the Agency Hierarchy Code based on authorized user information provided by the Agency specifying the services and Agency Hierarchy Codes that are valid for each authorized user. The Government is not requiring the contractor to have a link to its own internal accounting code structure. The Government expects the contractor to use the Agency Hierarchy Codes.

The Government consists of many large hierarchical organizations that purchase services from the contractor and are billed for those services. Agencies vary in size, vary in spans of control over Agencies that are below them in the hierarchy, and vary in spans of visibility to Agencies that are above them in the hierarchy. For example, an Agency may have other Agencies under its control referred to in this contract as sub-Agencies, but the span of control can be deeper than these two levels. Each Agency or Sub-Agency defines the number of levels and use of those levels (i.e., invoicing or reporting) depending on its own needs. The Agency's location in the Government hierarchy is defined by the AHC, which is described in detail in Attachment J.11 Glossary of Terms.

An Agency at the highest level can impose a hierarchical Agency structure across its entire hierarchy or can allow each level to redefine its own hierarchical structure to meet its own needs. Agencies require either invoices or reports at various levels of their hierarchy and these levels are not always consistent across the hierarchy.

Agencies and Sub-Agencies at lower levels within the Government hierarchy may not be aware of restrictions imposed at higher levels. The contractor, however, will have interaction at all levels, so it needs to be aware of the structure and meaning of the Agency hierarchy code in each situation.

This information is used by the contractor to ensure that billing hierarchies are consistently applied at the time an order is accepted and billed.

## **Agency Billing Choices**

Agencies select either Direct Billing, where the contractor bills the Agency directly for all charges and is paid by the Agency; or Centralized Billing, where the contractor bills the GSA and is paid by the GSA. GSA re-bills the Agencies who have chosen centralized billing. The Agency can change from Centralized to Direct Billing at any time at no cost to the Government. The Agency can change from Direct Billing to Centralized Billing at any time at no cost to the Government.

The Agency at the highest level of the hierarchy can have varying degrees of control over the Sub-Agencies within its hierarchy with respect to their billing choices. It may impose direct or centralized billing on all of the hierarchy or may allow Sub-Agencies below it to choose Direct Billing or Centralized Billing.

In the case of centralized billing, hierarchical billing and reporting is also required. The contractor provides only one invoice to the GSA, effectively adding another level on top of the Agency hierarchy that covers all Agencies that have chosen centralized billing. Hierarchical reporting is required in order to provide data files to the Agencies and sub-Agencies that need it. The GSA re-bills the Agencies.

After award and before Notice to Proceed, the Agency will identify to the GSA which Agencies and/or Sub-Agencies will receive centralized or direct billing, the Agencies' definition of the AHC and requirements for hierarchical billing and reporting of billing data. After the Notice to Proceed, the Agency will identify to the contractor which Agencies and/or Sub-Agencies will receive centralized or direct billing, the Agencies' definition of the AHC and requirements for hierarchical billing and reporting of billing data. The Agency will notify the contractor and GSA as this information changes on an ongoing basis.

An Agency chooses direct or centralized billing for all its services at the time it registers to purchase services from the Networx contract and it can change from Direct to Centralized billing or Centralized to Direct at any time.

## **Billing Data**

The Government seeks to increase efficiency by using automated systems as much as possible and by receiving data in a form that can be easily processed to be loaded into Government systems.

All Agencies, plus the GSA, require billing data to support all invoices on a monthly basis. Billing Data requirements include the Invoice File and the Detail Billing File(s). The Invoice file supports the invoice and the Detail Billing(s) File is produced at a lower level that varies depending on the service, but must include a single charge inclusive of all fees or discounts on each record and provide enough data to enable the Government to ensure the accuracy of that single charge by consulting the order and its completion notice, Networx price tables, known fee schedules and agreed upon discounts.

Recognizing the variability of both contractor billing systems and Agency billing systems and manual processes, this contract does not impose the number of physical files (i.e. a single common format for every service), but focuses instead on the data elements required by the Government, the need for current data dictionaries, and mapping and processing rules to enable the Government to interpret and process the billing data. In addition, this contract is expected to support Government efforts to automate both ordering and billing processes, so all files must be able to be loaded into Government database applications, in order to accomplish these processes. The contractor will provide its Data Dictionary Package for Billing as part of its initial proposal. Although the requirements for the Data Dictionary Package for Billing are stated in Section C.3.6.1, Direct Billing, the package must accommodate both Direct and Centralized Billing methods.

The contractor's Data Dictionary Package for Billing consists of a data dictionary for each of the contractor's required files, sample data for each required file, a mapping specification for each of the Government's logical files (e.g., Invoice, Detail Billing, Disputes) and their data elements, instructions for changes, and additional descriptive information. The data dictionary describes the required file and its data elements sufficiently to indicate how the Government's logical file and data elements map to the contractor's required file and its elements. The data dictionary also contains the formats for each element and a translation of all code values for all data elements. The Data Dictionary Package presents sample data for each service on the contract in electronic files using the same structure as the files the contractor will provide to the Government during operations. The Government uses these files of sample data to validate that the Data Dictionary Package meets the requirements and to develop and test the Government's internal systems that will process the data. The mapping specification explains how the contractor will accommodate mapping the Government's data elements to the contractor's required files and elements. The instructions describe and highlight changes, including additions and deletions, to the Data Dictionary Package. In addition, the contractor must provide additional descriptive information that facilitates the Government's understanding and review of the Data Dictionary Package.

In all situations, billing data must be sufficient to allow the Government to:

- a. Create a single Detail Billing File
- b. Balance the Detail Billing File to the Billing Invoice File
- c. Verify billing information back to an order
- d. Validate the accuracy of each charge on each record in the Detail Billing File.
- e. Verify adjustments at the lowest level (e.g., service period of original charge type/description)
- f. Re-bill its own internal customers
- g. Support the management of inventory.

For data file downloading or data file delivery, the contractor is required, at a minimum, to support file formats for Microsoft Excel 2002, Comma Separated Values (CSV) with field names included, or tab delimited ASCII text file with field names included.

**Contract Line Item Number (CLIN).** The CLIN is highly critical to the Government's effort to automate ordering, billing, and inventory verification. The SOCN is the Government's record of the order. The contractor will provide in the SOCN every CLIN it intends to bill for and all the data elements required to verify the correct CLIN has been used. Additionally, all CLINs must be provided in the SOCN even when the price is zero or the item is not separately priced. The Government will verify that every CLIN which appears on the Detail Billing File is present on the SOCN.

**Unique Billing Identifier (UBI)** The purpose of a UBI is to uniquely identify a single service and all components of that service separately from all other services being provided from within that same category of Network services. The contractor must provide a Unique Billing Identifier (UBI) to identify each billed record. The Government requires the contractor to assign a unique identifier for each component of the billed service that map to the UBI. The contractor may use existing fields in its systems to provide the UBI. The contractor is allowed to determine the form of the UBI for each service (especially those with multiple components) and must provide it on the Service Order Completion Notice as well as in the Detail Billing file. The contractor will provide GSA and the customer Agency any change to the UBI and any of its' associated components via the SOCN.

As an example, two similar orders for Frame Relay Services that are to be provided at the exact same address will each be uniquely identified so they can be easily separated on the bill. The contractor may elect to create a Unique Billing Identifier field, rather than using existing data elements, but at no charge to the Government. Examples of a UBI Include: A UBI could be a Circuit ID, a Phone number, an AHC, or a combination of elements. A UBI could represent a service consisting of a combination of an access circuit, a Private Virtual Circuit (PVC) and the Service Enabling Device (SED) that supports it. A UBI could represent a managed network service or project arrangement that includes any number of components, features, and services and could be an ICB CLIN combined with its Case Number.

#### **Other Contract Areas That Affect Billing**

Section C.3.5, Service Ordering defines the Agency Hierarchy Code, which is included on every order, and must appear on every Detail Billing file record provided by the contractor. As well, Service Ordering is affected by the requirement that the billing start date may not precede the completion date in the Service Order Completion Notice (SOCN), and billing end date must be the actual disconnect date indicated on the SOCN. Section G.5, Billing contains address requirements for mailing and receiving invoices and data. Section G.6, Payment of Invoices by Government covers payment of bills, payment information including the statement that upon 60 calendar days notice by the Agency or GSA, the contractor will change the billing from centralized to direct billing or vice versa, at no additional cost to the Government. Also in Section G.6, Payment of Invoices by Government is the requirement that GSA is responsible to pay the contractor only for the

Networkx centralized invoices that charge the centralized billing user Agencies or sub-Agencies. GSA, while offering two billing methods for Networkx, will not be responsible for paying for any charges directly invoiced to any Agency or Sub-Agency. According to Section G.6, Payment of Invoices by Government the contractor shall be responsible for the collection of charges from the directly billed Agencies from the Agencies. Security requirements for Billing are in Section C.3.9, Operational Support Systems, and C.3.3.2, Security Management. Attachment J.12.4, Billing Invoice and Detail contains the definition of all data elements not defined in Section C.3.6, Billing. Section H.12, Key Personnel and Corporate Structure defines contractor Billing Manager requirements.

**C.3.6.1 Direct Billing**

The Networkx contractor will provide both Centralized and Direct Billing for its services. Government Agencies that use Direct Billing will be invoiced by the contractor, and will pay the invoice directly to the contractor. The contractor will be responsible for collection of all accounts receivable associated with direct-billed revenue. This is opposed to Centralized Billing where all invoices are delivered to and paid through GSA. The processes, systems and procedures developed, implemented, and maintained in support of this billing option will be detailed in sections C.3.6.1.1, Direct Billing Process Definition, C.3.6.1.2, Direct Billing Functional Requirements, C.3.6.1.3, Direct Billing Data Requirements and C.3.6.1.4, Direct Billing Report Requirements.

**C.3.6.1.1 Direct Billing Process Definition**

**C.3.6.1.1.1 Direct Billing Process Description**

The contractor will provide the direct-billed Agency/sub Agency and GSA with the direct-billed billing files every month by the 15<sup>th</sup> business day after the conclusion of the Government's billing period (See Section C.3.6.1.2.3, Step 3 – The contractor Delivers Direct-billed Invoice, Detail Billing, and Adjustment to Agency and GSA Files). The Government will provide an acknowledgement to the contractor of receipt of the billing files. The contractor's Data Dictionary Package for Billing is included in the contract at award based on what the contractor submitted in the proposal, and the contractor updates the Data Dictionary Package as required. The Service Order Completion Notice (SOCN) must be received by the GSA and the Agency prior to being invoiced for the service. The billing start date may not precede the completion date on the Service Order Completion Notice (SOCN) and billing end date must be the actual disconnect date indicated on the SOCN. The GSA Management Service (GMS) Fee will be computed based on the billed eligible revenue of the invoice and paid via direct payment to GSA (not as a credit on the invoice) within 60 calendar days after the end of the applicable reporting period (refer to Section G.5.3, GSA Management Service (GMS) Fee).

**C.3.6.1.1.2 Direct Billing Process Narrative**

Step Number	Description	Executing Entities
1	Agency indicates Direct billing requirement and delivers list(s) of valid Agency hierarchy codes (AHCs), Designated Agency Representatives (DARs), and Agency hierarchical billing requirements to the contractor and to GSA.	Agency and Contractor

Step Number	Description	Executing Entities
2	The contractor delivers the Data Dictionary Package for Billing for all billing output files and subsequent Data Dictionary Package updates and changes to GSA and Agencies.	Contractor
3	The contractor delivers direct-billed invoice and Detail Billing Files to the Agency's designated office(s) and to GSA	Contractor
4	The contractor delivers a list of direct-billed Agencies to GSA	Contractor
5	The contractor manages a GSA Management Service (GMS) fee.	Contractor
6	Agency/contractor follows Dispute Process.	Agency and Contractor
7	Following invoice certification process, Agency remits payment to contractor.	Agency
8	The contractor maintains and retains copies of all contract-related billing data.	Contractor

**C.3.6.1.2 Direct Billing Functional Requirements**

**C.3.6.1.2.1 Step 1--Agency Indicates Direct Billing Requirement**

ID Number	Description
1	The contractor shall accept from any Agency/Sub-Agency its requirement to be direct-billed or to be centrally billed as well as its hierarchical billing requirements in accordance with Section C.3.5.1.2.1, Step 1 – Contractor Establishes Ordering Environment.

**C.3.6.1.2.2 Step 2--The Contractor Delivers Data Dictionary Package for Billing**

ID Number	Description
1	The contractor shall provide a Data Dictionary Package for Billing, including any changes required by the Government, and update thereafter as changes occur. See Section C.3.6.1.3.2.1 Data Dictionary Package for Billing.
2	The contractor shall define a specific data element or data elements to create a UBI that uniquely identifies the combination of the following: [1] service type; [2] service location; and [3] Agency to which the service belongs. (Examples may include: circuit ID, phone number, Contractor Service Account number, etc.). See additional guidance in the introduction to Section C.3.6, Billing.
3	The contractor shall include the same UBI in both the Service Order Completion Notice (SOCN) and the Detail Billing File(s).
4	When an Agency is conducting Fair Opportunity or has selected the contractor, the Agency may request the contractor's Data Dictionary Package for Billing. The contractor shall provide the Data Dictionary Package for Billing to the Agency as specified in Section C.3.6.1.3.2.1 Data Dictionary Package for Billing.(identical to that provided to GSA).
5	The contractor shall consider each file required by the Government as a logical file and shall submit descriptions of one or more required files it will send to the Government, so that the Government can create the logical file.
6	In the Data Dictionary Package for Billing, the contractor shall provide a mapping specification that maps the Government's logical file names and the data elements contained in the logical files to the contractor's required file names and the data elements contained in the required files, including a service-by-service mapping of the UBI.

ID Number	Description
7	The contractor shall provide a Data Dictionary Package for Billing containing at a minimum for each logical file, a description of each of the contractor's required files and for each data element contained within the file, the data element field name, field length, field type, field characteristics, and a description of the data that could be populated in the field that is sufficient to map the Government's data elements to the data elements in the contractor's required files.
8	The contractor shall include within the Data Dictionary a translation of all billing codes used by the contractor's billing system as they apply to the coding of the billing data elements of this contract.
9	The contractor shall provide updates to the Data Dictionary Package for Billing, including but not limited to data elements, sample data and file layouts prior to implementation to both GSA and Agencies; the contractor shall indicate all changes in detail at the beginning of the documents indicating changes in the body of the document.
10	The contractor shall provide instructions with the Data Dictionary Package for Billing that presents the details of each change and indicates the importance of each of the changes so that they may easily be identified.
11	The contractor shall provide sample data for all of the contractor's required files by including in the Data Dictionary Package electronic files in the same structure as the contractor's required files and populated with representative data values that include all services on the contract. These files of sample data will enable the Government to develop and test internal systems that process the data.
12	The contractor shall provide additional descriptive information in the Data Dictionary Package for Billing that will enable the Government to easily interpret the contents.

#### C.3.6.1.2.3 Step 3--The Contractor Delivers Direct-billed Invoice, Detail Billing, and Adjustments Files to the Agency and GSA

ID Number	Description
1	In accordance with requirements specified in Section G.5, Billing and within 15 business days after the close of the billing period, the contractor shall provide the Invoice, Detail Billing, and Adjustments Files to each Agency that has direct-billed services from the contractor.
2	In accordance with requirements specified in Section G.5, Billing and within 15 business days after the close of the billing period, the contractor shall provide the Invoice, Detail Billing, and Adjustments Files to GSA for all services provided to all Agencies.
3	The contractor shall comply with Government's billing period that runs from the 1 <sup>st</sup> through the last day of the calendar month for the contractor's services.
4	The contractor shall deliver direct-billed invoice, Detail Billing, and Adjustments Files in accordance with Section 3.6.1.3.2.2 Direct-Billed Invoice, Detail Billing and Adjustment Files., Attachment J.12.4, Billing Invoice and Detail, and J.12.6, Adjustments.
5	The following requirements apply to the Invoice Files:
5.1	The contractor shall invoice all services on a consolidated invoice.
5.2	The contractor shall carry all GSA-provided contract numbers on its invoices.
5.3	The contractor shall provide 60 calendar days notice to the GSA and Agency in writing before making changes to the format.
5.4	The contractor shall implement any changes to the invoice content, including changes resulting from the inclusion of future services or enhancements, that are in accordance with commercial invoicing capabilities at no additional cost to the Government, and within timeframe agreed upon between GSA and the contractor.

ID Number	Description
5.5	The contractor may provide additional data elements on the invoice consistent with the contractor's existing practice as agreed upon by the Government.
6	The following requirements apply to the Detail Billing File(s)
6.1	The contractor shall provide Detail Billing File(s) with billed amounts for direct-billed Agencies that sum to the total amount billed on the invoice for direct-billed Agencies.
6.2	The contractor shall provide all charges on the Detail Billing File(s) such that the Government can verify all price elements and CLINs as specified in Section B, Pricing. The Detail Billing File(s) may also include additional data elements consistent with the contractor's existing practice.
6.3	The contractor shall provide a Detail Billing File(s) that contains the data elements as specified in Attachment J.12.4.2, Detail Billing File.
6.4	The contractor shall deliver monthly all of the direct billing data elements to the Agencies and sub-Agencies that are authorized for direct billing.
6.5	The contractor shall ensure that the Detail Billing File(s) contains a separate record for each instance of each individual item ordered and those detailed records are associated with the order number. For example, if 10 calling cards were ordered as part of a bulk order, it must be possible to separate the detailed billing records associated with one of those cards without affecting the detailed billing records of the other nine.
6.6	The contractor shall ensure that detailed billing records for usage charges are at the lowest level captured on the contractor's network and appropriate to define the billed transaction.
6.7	The contractor shall provide CDR records in the Detail Billing File(s) for switched voice services.
6.8	The contractor shall provide CDR level (i.e., the lowest level available, such as circuit level, PVC, SED) records for all other services in the Detail Billing File(s).
6.9	The contractor shall ensure that the CLIN for a feature charge can be associated with the CDR or CDR level record to which it applies.
6.10	The contractor shall ensure that tax, surcharge, duty, fee, and adjustment records can be associated with the CDR, CDR level, monthly recurring, or non-recurring record(s) to which they apply.
6.11	The contractor shall provide data elements as specified in the data dictionary so that the charges can be billed to appropriate Agency hierarchical levels and so that detail reporting of each charge can be produced at appropriate hierarchical levels.
6.12	The contractor shall have all data fields populated as appropriate (i.e., in the case where a charge or code does not apply to a service, those fields would not be populated; conversely, all pertinent data elements shall be populated for a service).
6.13	The contractor shall not bill for any taxes, surcharges, duties or fees not in accordance or applicable under the terms and conditions of this contract.
6.14	The contractor shall provide all CLINs associated with the UBI even if the prices are zero or not separately priced.
6.15	The contractor shall pro-rate charges for a CLIN when the rate for a CLIN changes during a billing period such that correct daily rate is charged on a per day basis.
6.16	In cases where there are multiple charging units, the contractor shall provide separate records in the detail billing file, and for each record, the CLINS, quantities, charging units, and charges shall be separate.
7	The contractor shall include with the direct-billed Invoice, Detail Billing, and Adjustments Files a Monthly Billing Informational Memorandum to detail any pertinent information to the current billing data files that affects all contract customers. See Sections C.3.6.1.4.1, Contractor Reports Provided to Government.
8	The contractor shall obtain written approval from the GSA Contracting Officer (CO) to initiate an emergency change in the invoice or Detail Billing File(s).



ID Number	Description
9	The contractor shall bill the entire Billing of Non-recurring charges (NRC) and, if appropriate, indicate waived or discounted charges, on the invoice following acceptance by the Government for the installation of the service contained in the completed order.
10	The contractor shall provide the Agency/Sub-Agency any application software packages required to read and analyze electronic billing data.
11	The contractor shall provide access to its price-quote system information to enable authorized Agency representatives to verify pricing of billed charges with history available through all contract years.
12	The contractor shall provide a secure, web-based capability for the Agency/Sub-Agency and the GSA to inquire on detail billing and adjustment records and download them as necessary.
13	The contractor shall accept from GSA, within 1 business day of receipt of files, a Notification of Receipt of Invoice, Detail Billing, and Adjustments Files that data files have been received. See Section C.3.6.1.3.1, GSA Data to contractors.
14.1	In the event data files are incomplete, the contractor shall notify GSA with the method contractor will use to correct the problem, and provide the complete set of files within one (1) business day.
14.2	In the event the data files are not loadable, the contractor shall make best effort with GSA to identify the cause of the problem and determine the corrective action(s).
14.3	For data loading problems isolated to contractor causes, the contractor shall correct the error within one (1) business day.

**C.3.6.1.2.4 Step 4--The Contractor Delivers a List of Direct-Billing Agencies to GSA**

ID Number	Description
1	The contractor shall deliver to the GSA by the last business day of each calendar month a current list of Agencies with direct-billed charges in accordance with Section C.3.6.1.3.3.1 Direct-Billed Agency List.

**C.3.6.1.2.5 Step 5--The Contractor Manages a GSA Management Service (GMS) Fee.**

ID Number	Description
1	The contractor shall collect the GMS fee from direct-billed customers on a monthly basis throughout the life of the contract. See Section G.5.3, GSA Management Service Fee (GMS).
2	The contractor shall calculate the direct-billed management fee based on amounts billed by Agency hierarchy code for each service.
2.1	The contractor shall not apply taxes to the GMS.
2.2	The contractor shall not include any taxes in the calculation of the GMS, with the following exception. The Government may require that all taxes, fees and surcharges be included in Agency Unique CLIN (AUC) prices associated with a task order if this has been authorized by a Delegation of Procurement Authority (DPA) issued by the GSA Network Contracting Officer (CO) to a warranted agency Ordering Contracting Officer (OCO). While the agency may include this requirement in its task order solicitation, the contractor may elect to respond to this requirement in a solicitation at its discretion. If the GSA-issued DPA authorizes the requirement stated above, contractors may include taxes, fees and surcharges in the calculation of the GMS. AUC price-based invoice amounts that include taxes, fees and surcharges will be considered billed eligible revenue.

ID Number	Description
3	The contractor shall include this GMS fee in all of its published prices.
4	The GSA will advise the contractor after Notice to Proceed the amount of this fee in terms of a percentage to be applied to all of the contractor's base prices.
5	The contractor shall accommodate a single GMS fee structure that applies to all services.
6	The GSA will evaluate the GMS fee on an annual basis.
7	The contractor shall implement changes in the GMS fee at no additional cost to the Government.
8	The contractor shall calculate the GMS fee on billed eligible revenue for each service.
9	The contractor shall accept exceptions/exclusions from GSA to the billed eligible revenue within 30 calendar days after Notice to Proceed and include them in the GMS calculation.
10	The contractor shall collect a GMS fee from all direct-billed Agencies.
11	The contractor shall provide to the GSA a report of Agencies that are designated as direct-billed whose billing is considered delinquent. The Direct-Billed A/R Delinquency Aging Report shall reflect delinquent balances greater than 60 calendar days, 90 calendar days, and 120 calendar days and comply with Section C.3.6.1.4.2.1 Direct-Billed A/R Delinquency Aging Report.
12	The contractor shall make the payment to GSA via direct payment (not as a credit on the invoice) within 60 calendar days after the end of the applicable reporting period, to be sent in accordance with Section G.5.3, GSA Management Service Fee.
13	For direct-billed Agencies, the contractor shall not show the GMS fee as a separate item on the invoice or include it in the Detail Billing File(s).
14	If the full amount of the GMS fee is not paid within 60 calendar days after the end of the applicable reporting period, the nonpayment shall constitute a contract debt to the United States Government.
15	The contractor shall include GMS fees for direct-billed in the Contractor GMS Fee Reconciliation Report. See Section C.3.6.2.4.1.2, GMS Fee Reconciliation Report.

**C.3.6.1.2.6 Step 6-- Agency/Contractor Billing Inquiries ad Disputes Process.**

ID Number	Description
1	The contractor shall follow the Agency/contractor Billing Disputes and Adjustments process covered in Section C.3.6.3. Billing Disputes and Adjustments.

**C.3.6.1.2.7 Step 8--The Contractor Maintains and Retains Copies of All Contract-related Billing Data.**

ID Number	Description
1	The contractor shall maintain and retain for ten years from expiration or termination of the contract copies of all data, hardcopy, letters, electronic mail, memorandums, adjustment data and other data pertaining to the billing of contract services as specified in Section G.5. Billing.
2	The contractor shall provide reports and data fulfilling requests for archived information and data to the Government in a format acceptable to the Government within 5 business days after receiving the Government's request for ten years from expiration or termination of the contract.

**C.3.6.1.3 Direct Billing Data Requirements**

**C.3.6.1.3.1 GSA Data Provided to Contractors**

**C.3.6.1.3.1.1 Notification of Receipt of Invoice, Detail Billing, and Adjustment Files**

**C.3.6.1.3.1.1.1 Frequency – Notification of Receipt of Invoice, Detail Billing, and Adjustment Files**

- As required

**C.3.6.1.3.1.1.2 Media/Transport/Format – Notification of Receipt of Invoice, Detail Billing, and Adjustment Files**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.1.3.1.1.3 Record Elements – Notification of Receipt of Invoice, Detail Billing, and Adjustment Files**

ID Number	Data Elements	Description
1	Title	Notification of Receipt of Contractor Billing Files
2	Date	Date of receipt of files at GSA
3	File Identification 1	Name of Data set
4	File Identification 2	Record and block formatting (if applicable)
5	File Identification 3	Media numbers ( tape or volume serial numbers, for example)
6	Missing file(s)	List of any files that were not included in the delivery but were listed in the Contractor Notification of Pending Delivery.
7	Contractor	Contractor Name / Contract Number
8	Government POC	Name and phone number of Government point of contact for this Notification

\*Media type changes per section C.3.1.2

**C.3.6.1.3.1.2 Notification of Data File Loading Problems**

**C.3.6.1.3.1.2.1 Frequency – Notification of Data File Loading Problems**

- As required

**C.3.6.1.3.1.2.2 Media/Transport/Format – Notification of Data File Loading Problems**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.1.3.1.2.3 Record Elements – Notification of Data File Loading Problems**

ID Number	Data Elements	Description
1	Title	Notification of Contractor Billing Data Files in Error
2	Date	Date of Notification
3	Reason	Confirmed or suspected reason for the problem with the file(s). Reason for each problem if more than one. Examples: Incomplete files, incorrect record length or blocking size, physical media corrupted.
4	Contractor	Contractor Name / Contract Number
5	Government POC	Name and phone number of Government point of contact for this Notification

**C.3.6.1.3.2 Contractor Data Provided to Government**

**C.3.6.1.3.2.1 Data Dictionary Package for Billing**

**C.3.6.1.3.2.1.1 Frequency – Data Dictionary Package for Billing**

- Initial
  - Sent to GSA: Included at Award

- Sent to Agency: After Notice to Proceed and within 5 business days of Agency request
- Revised: GSA only: Within 5 business days after receiving GSA comment
- Updated: As changes occur; no less than 60 calendar days prior to implementation; updates due to changes in standards or introduction of new services no more than once every 60 days

**C.3.6.1.3.2.1.2 Deliver To - Data Dictionary Package for Billing GSA PMO**

**C.3.6.1.3.2.1.3 Media/Transport/Format – Data Dictionary Package for Billing**

**C.3.6.1.3.2.1.3.1 Media/Transport/Format – Data Dictionary Package for Billing sent to GSA**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	

**C.3.6.1.3.2.1.3.2 Media/Transport/Format – Data Dictionary Package for Billing Sent to Agency**

Data		
Media	Transport	Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> </ul>	

Data		
Media	Transport	Format
	<ul style="list-style-type: none"> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text</li> </ul>
		<ul style="list-style-type: none"> <li>Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.1.3.2.1.4 Record Elements – Data Dictionary Package for Billing**

ID Number	Data Elements	Description
		(Applies to ID Number 1-10) One is required for each of the Billing files submitted by the contractor
1	Report Title	Data Dictionary
2	Contractor	Contractor Name/Contract Number
3	File Name	Contractor File Name (if applicable)
4	Date	Date of the Version or Update
		Applies to ID Number 5-10, One is required for each data element
5	Data Element	Data Element Field Name (e.g., network call redirect MRC, etc.)
6	Field Length	Length of the Data Element Field in the contractor provided File
7	Field Type	Field Format Type (e.g., text)
8	Field	Field Characteristics (e.g., numerical, number of decimal

ID Number	Data Elements	Description
	Characteristics	places, alphabetical, etc.)
		Applies to ID Number 9 , One is required for each code value
9	Code Value	Code Value (i.e., internal contractor defined alpha/numeric code value such as "151" or "A2169")
10	Data Description	Description of the data that could be populated in the field that is sufficient to map the element to the Government data elements
		(Applies to ID number 11-15) One for each of the Billing files submitted by the contractor is required.
11	Report Title	Contractor Sample Data for (include file name)
12	Contractor	Contractor Name/Contract Number
13	File Name	Contractor File Name
14	Date	Date of Version or Update
15	Data	Sample data in the same format as defined in the data dictionary.
		(Applies to ID number 16-25 – one for each of the Government Billing Files required (i.e. Invoice File and Detail billing file).
16	Report Title	Mapping Table for (Insert Government Billing File Name)
17	Contractor	Contractor Name/Contract Number
18	File Name	Contractor File Name (if applicable)
19	Date	Date of version or Update
20	Government File	e.g. Detail Billing file for Direct Bill, Adjustments
		(Applies to ID number 21-25) One for each data element in the Government file (in order according to Attachment J.12) is required.
21	Data Element	Government data element
22	File Name	Contractor file name where element exists
23	Contractor Data Element Name	Contractor data element name
24	Mapping Rules	Data transformation or other actions required by Government to locate data element
25	Comments	
		(Applies to ID number 26-28) One for entire Data Dictionary Package as a whole
26	Report Title	Instructions for Data Dictionary Package for Billing
27	Files and Dates	Name of the contractor files and dates contained in the package
28	Instructions	Change from the previous version of the package, contact information, names and dates of all files contained in the Data Dictionary Package, other information which will enable the Government to interpret the contents of the Data Dictionary Package.

**C.3.6.1.3.2.2 Direct-Billed Invoice, Detail Billing, and Adjustment Files**

**C.3.6.1.3.2.2.1 Frequency – Direct-Billed Invoice, Detail Billing, and Adjustment Files**

- Initial: 15 business days after close of first month in which contractor has billable charges for Direct-Billed customers
- Updated: Monthly within 15 business days after preceding calendar month

**C.3.6.1.3.2.2.2 Deliver To - Direct-Billed Invoice, Detail Billing, and Adjustment Files**

- GSA PMO
- Direct Billed Agency

**C.3.6.1.3.2.2.3 Media/Transport/Format – Direct-Billed Invoice, Detail Billing, and Adjustment Files**

**C.3.6.1.3.2.2.3.1 Media/Transport/Format – Direct-Billed Invoice, Detail Billing, and Adjustment Files sent to GSA**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

\*Media type changes per section C.3.1.2



**C.3.6.1.3.2.2.3.2 Media/Transport/Format – Direct-Billed Invoice, Detail Billing, and Adjustment Files sent to Agency**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97</li> </ul>
	<ul style="list-style-type: none"> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

\*Media type changes per section C.3.1.2

**C.3.6.1.3.2.2.4 Record Elements – Direct-Billed Invoice, Detail Billing, and Adjustment Files**

ID Number	Data Elements	Description
1	Title	Direct-Billed Invoice, Detail Billing, and Adjustments Files
2	Invoice File Elements	See Attachment J.12.4.1, Unit 1: Invoice File
3	Detail Billing File Elements	See Attachment J.12.4.2, Unit 2: Detail Billing File
4	Adjustment Data File Elements	See Attachment J.12.6, Adjustments
5	Agency	Agency's name

**C.3.6.1.3.3 Contractor Data Provided to GSA**

**C.3.6.1.3.3.1 Direct-Billed Agency List**

**C.3.6.1.3.3.1.1 Frequency–Direct-Billing Agency List**

- Initial: 5 business days after close of first month in which contractor receives orders for Direct-Billed customers
- Updated: Monthly within 5 business days after preceding calendar month

**C.3.6.1.3.3.1.2 Deliver To - Direct-Billed Agency List**

- GSA PMO

**C.3.6.1.3.3.1.3 Media/Transport/Format – Direct-Billed Agency List**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	

Data		
Media	Transport	Data Format
		between GSA and contractor

\*Media type changes per section C.3.1.2

#### C.3.6.1.3.3.1.4 Record Elements – Direct-Billed Agency List

ID Number	Data Elements	Description
1	Agency Name	Name of direct-billed Agency/Sub-Agency
2	AHC	Agency Hierarchy Code associated with Agency/Sub-Agency
3	DAR Administrator	Name of DAR Administrator
4	POC	Name of Agency Billing Point of Contact
5	POC Phone	Agency POC Phone number
6	POC Email	Agency POC Electronic mail address
7	Contractor	Contractor Name and Contract Number
8	Title	(As appropriate)
9	As of Date	Date on which list is current

#### C.3.6.1.4 Direct Billing Report Requirements

##### C.3.6.1.4.1 Contractor Reports Provided to Government

##### C.3.6.1.4.1.1 Monthly Billing Informational Memorandum

##### C.3.6.1.4.1.1.1 Frequency - Monthly Billing Informational Memorandum

- Monthly, to be delivered with the Invoice

##### C.3.6.1.4.1.1.2 Deliver To – Monthly Billing Informational Memorandum

- GSA PMO
- Direct-Billed Agency

##### C.3.6.1.4.1.1.3 Media/Transport/Format – Monthly Billing Informational Memorandum

**C.3.6.1.4.1.1.3.1 Media/Transport/Format – Monthly Billing Informational Memorandum sent to GSA**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> </ul> <p>Other formats as mutually agreed between GSA and contractor</p>

**C.3.6.1.4.1.1.3.2 Media/Transport/Format – Monthly Billing Informational Memorandum sent to Agency**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	

Report		
Media	Transport	File Format
Email Serve	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to internet E-Mail</li> <li>Encrypted Internet E-Mail</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97</li> </ul>
	<ul style="list-style-type: none"> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	through 2003 <ul style="list-style-type: none"> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.1.4.1.1.4 Content – Monthly Billing Informational Memorandum**

ID Number	Data Elements	Data Elements
1	Title of Report	Monthly Billing Informational Memorandum
2	Contractor	Contractor Name / Contract Number
3	Period	Month and year of reporting period
4	Date	Date of report
5	Information	List of information that applies to all Direct-Billed Agencies and the current invoice. This includes, but is not limited to, items that will explain changes in billing, changes to data formats (addressed in Section C.3.6.1.3.4.1), and new services added to the billing, and issues pertaining to balancing charges.

**C.3.6.1.4.2 Contractor Reports Provided to GSA**

**C.3.6.1.4.2.1 Direct-Billed A/R Delinquency Aging Report**

**C.3.6.1.4.2.1.1 Frequency–Direct-Billed A/R Delinquency Aging Report**

- Initial: Within 15 business days after close of billing period in which accounts become delinquent
- Updated: Monthly (indicate if no accounts are delinquent)

**C.3.6.1.4.2.1.2 Deliver To–Direct-Billed A/R Delinquency Aging Report**

- GSA PMO

**C.3.6.1.4.2.1.3 Media/Transport/Format – Direct-Billed A/R Delinquency Aging Report**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

\*Media type changes per section C.3.1.2

**C.3.6.1.4.2.1.4 Content – Direct-Billed A/R Delinquency Aging Report**

ID Number	Data Elements	Description
1	AHC	Agency Hierarchy Code
2	Invoice Number	Contractor Invoice Number
3	Invoice Date	Invoice Date
4	Service Type	Service Type
5	# Days Delinquent	Number of Actual Calendar days the Payment of Invoice is Delinquent
6	Invoice Balance Due	Invoice Balance Due
7	GMS Fee Balance Due	GMS Fee Balance Due
8	Contractor	Contractor Name and Contract Number
9	Title	(As appropriate)
10	As of Date	Date on which data are current

**C.3.6.2 Centralized Billing**

**C.3.6.2.1 Centralized Billing Process Definition**

**C.3.6.2.1.1 Centralized Billing Process Description**

The contractor will provide GSA with the billing files for Agencies billed centrally every month by the 15<sup>th</sup> business day after the close of the contractor billing period. GSA will provide an acknowledgement to the contractor of receipt of the billing files. The contractor will also provide GSA with all Centralized and Direct billing file data layouts and data dictionaries, and provide updates as required. The Service Order Completion Notice (SOCN) must be received by the GSA and the Agency prior to being invoiced for the service. The billing start date on each billing record may not precede the completion date on the Service (SOCN), and billing end date must be the actual disconnect date indicated on the SOCN. The GSA Management Service (GMS) Fee will be computed based on the eligible billed revenue of the invoice, and broken out on the invoice as a credit on the Centralized Invoice copies (refer to Section G.5, Billing).

In the case that GSA cannot verify and validate the invoice and billing files, or in the case of an 'out-of-balance' situation, GSA will notify the contractor, reject the invoice, and return the billing files.

GSA will process the billing files to verify and validate the bills and to produce the billing for the Agencies using centralized billing and issue the payment to the contractor. Finally, the contractor will provide contractor billing information to Agencies as well.

**C.3.6.2.1.2 Centralized Billing Process Narrative**

Step Number	Description	Executing Entities
1	Agency indicates Centralized billing requirement and Agency hierarchy billing requirements	Agency/Contractor
2	The contractor delivers Centralized billed Invoice, Detail Billing, and Adjustment Files to GSA and the Agency.	Contractor
3	The contractor manages the GSA Management Service (GMS) fee.	Contractor
4	GSA verifies and validates Centralized billing data.	GSA/Contractor
5	Government/contractor Dispute Process covered in Section C.3.6.3 Billing Disputes and Adjustments.	GSA/Agency/ Contractor
6	GSA issues Centralized payment to contractor	GSA/Contractor
7	The contractor maintains and retains copies of all contract-related billing data.	Contractor

**C.3.6.2.2 Centralized Billing Functional Requirements**

**C.3.6.2.2.1 Step 1--Agency Indicates Centralized Billing Requirement and Agency hierarchical billing requirements**

ID Number	Description
1	The contractor shall accept from any Agency/Sub-Agency its requirement to be

ID Number	Description
	direct-billed or to be centrally billed as well as its hierarchical billing requirements in accordance with Section C.3.5.1.2.1, Step 1 – Contractor Establishes Ordering Environment.

#### C.3.6.2.2.2 Step 2--The Contractor delivers Data Dictionary Package for Billing

ID Number	Description
1	The contractor shall provide a Data Dictionary Package for billing according to Section C.3.6.1.2.2, Step 2 – the Contractor Delivers Data Dictionary for Billing.

#### C.3.6.2.2.3 Step 3--The Contractor Delivers Centralized Billed Invoice and Detail Billing, and Adjustment Files to the Agency and GSA

ID Number	Description
1	In accordance with requirements specified in Section G.5, Billing and within 15 business days after the close of the billing period, the contractor shall provide the Invoice, Detail Billing, and Adjustments Files to each Agency that has centralized-billed services from the contractor.
2	In accordance with requirements specified in Section G.5, Billing and within 15 business days after the close of the billing period, the contractor shall provide the Invoice, Detail Billing, and Adjustments Files to GSA for all services provided to all Agencies.
3	The contractor shall comply with Government's billing period that runs from the 1 <sup>st</sup> through the last day of the calendar month for the contractor's services.
4	The contractor shall deliver Centralized Invoice, Detail Billing, and Adjustments Files in accordance with Section C.3.6.2.3.2.1, Centralized Billed Invoicing, Detailed Billing, and Adjustment Files as well as Attachments J.12.4, Billing Invoice and Detail and J.12.6, Adjustments.
5	The following requirements apply to the Invoice Files:
5.1	The contractor shall invoice all services on a consolidated invoice.
5.2	The contractor shall carry all GSA-provided contract numbers on its invoices.
5.3	The contractor shall provide 60 calendar days notice to the GSA and Agency in writing before making changes to the format.
5.4	The contractor shall implement any changes to the invoice content, including changes resulting from the inclusion of future services or enhancements that are in accordance with commercial invoicing capabilities at no additional cost to the Government, and within timeframe agreed upon between GSA and the contractor.
5.5	The contractor may provide additional data elements on the invoice consistent with the contractor's existing practice as agreed upon by the Government.
6	The following requirements apply to the Detail Billing File(s)
6.1	The contractor shall provide Detail Billing File(s) with billed amounts for Centralized billed Agencies that sum to the total amount billed on the invoice for Centralized billed Agencies.
6.2	The contractor shall provide all charges on the Detail Billing File(s) such that the Government can verify all price elements and CLINs as specified in Section B, Pricing. The Detail Billing File(s) may also include additional data elements consistent with the contractor's existing practice.
6.3	The contractor shall provide a Detail Billing File(s) that contains the data elements as specified in Attachment J.12.4.2, Detail Billing File.



ID Number	Description
6.4	The contractor shall deliver monthly all of the centralized billing data elements to the Agencies and sub-Agencies that are authorized for centralized billing.
6.5	The contractor shall ensure that the Detail Billing File(s) contains a separate record for each instance of each individual item ordered and those detailed records are associated with the order number. For example, if 10 calling cards were ordered as part of a bulk order, it must be possible to separate the detailed billing records associated with one of those cards without affecting the detailed billing records of the other nine.
6.6.	The contractor shall ensure that detailed billing records for usage charges are at the lowest level captured on the contractor's network and appropriate to define the billed transaction.
6.7	The contractor shall provide CDR records in the Detail Billing File(s) for switched voice services
6.8	The contractor shall provide CDR level (i.e., the lowest level available, such as circuit level, PVC, SED) records for all other services in the Detail Billing File(s).
6.9	The contractor shall ensure that the CLIN for a feature charge can be associated with the CDR or CDR level record to which it applies.
6.10	The contractor shall ensure that tax, surcharge, duty, fee, and adjustment records can be associated with the CDR, CDR level, monthly recurring, or non-recurring record(s) to which they apply.
6.11	The contractor shall provide data elements as specified in the data dictionary so that the charges can be billed to appropriate hierarchical Agency levels and so that detail reporting of each charge can be produced at appropriate hierarchical levels.
6.12	The contractor shall have all data fields populated as appropriate (i.e., in the case where a charge or code does not apply to a service, those fields would not be populated; conversely, all pertinent data elements shall be populated for a service).
6.13	The contractor shall not bill for any taxes, surcharges, duties or fees not in accordance or applicable under the terms and conditions of this contract.
6.14	The contractor shall provide all CLINs associated with the UB I even if the charges are zero.
6.15	The contractor shall pro-rate charges for a CLIN when the rate for a CLIN changes during a billing period such that correct daily rate is charged on a per day basis.
6.16	In cases where there are multiple charging units, the contractor shall provide separate records in the detail billing file, and for each record, the CLINS, quantities, charging units, and charges shall be separate.
7	The contractor shall include with the centralized-billed Invoice, Detail Billing, and Adjustments Files a Monthly Billing Informational Memorandum to detail any pertinent information to the current billing data files that affects all contract customers. See Section C.3.6.2.3.2, Contractor Data Provided to Government.
8	The contractor shall obtain written approval from the GSA Contracting Officer (CO) to initiate an emergency change in the invoice or Detail Billing File(s).
9	The contractor shall bill the entire Billing of Non-recurring charges (NRC) and, if appropriate, indicate waived or discounted charges, on the invoice following acceptance by the Government for the installation of the service contained in the completed order.
10	The contractor shall provide the Agency/Sub-Agency any application software packages required to read and analyze electronic billing data.
11	The contractor shall provide access to its price-quote system information to enable authorized Agency representatives to verify pricing of billed charges with history available through all contract years.
12	The contractor shall accept from GSA, within 1 business day of receipt of files, a Notification of Receipt of Invoice, Detail Billing, and Adjustments Files that data files have been received. See Section C.3.6.2.3.1, GSA Data Provided to contractors.

ID Number	Description
	The contractor shall accept from GSA, within 7 business days of receipt of files, a Notification of Data File Loading Problems if data files cannot be loaded or are not complete. See Section C.3.6.2.3.1, GSA Data Provided to contractors.
13.1	In the event data files are incomplete, the contractor shall notify GSA with the method contractor will use to correct the problem, and provide the complete set of files within one (1) business day.
13.2	In the event the data files are not loadable, the contractor shall make best effort with GSA to identify the cause of the problem and determine the corrective action(s).
13.3	For data loading problems isolated to contractor causes, the contractor shall correct the error within one (1) business day.

#### C.3.6.2.2.4 Step 4--The Contractor Manages a GSA Services (GMS) Fee

ID Number	Description
1	The contractor shall calculate the GMS fee for Centralized billed customers on a monthly basis throughout the life of the contract.
2	The contractor shall calculate the Centralized billed management fee based on amounts billed by Agency hierarchy code for each service.
3	The contractor shall include this GMS fee in all of its published prices.
4	GSA will advise the contractor after Notice to Proceed the amount of this fee in terms of a percentage to be applied to all of the contractor's base prices.
5	The contractor shall accommodate a single GMS fee structure that applies to all services.
6	GSA will evaluate the GMS fee on an annual basis. The contractor shall implement changes in the GMS fee at no additional cost to the Government.
7	The contractor shall calculate the GMS fee on eligible billed revenue for each service.
8	The contractor shall accept exceptions/exclusions from the GSA to the billed revenue within 30 calendar days of contract award and include them the GMS calculation.
9	The contractor shall provide to GSA a contractor GMS Fee Reconciliation Report on a monthly basis that includes GMS fees for both direct and centralized billing. Report shall contain a table listing the breakdown of all the GMS fees, Centralized and Direct fees in separate tables, with GMS detailed by Services and Products when they are different from the standard GMS fee. See Section C.3.6.2.4.1.3 GMS Fee Reconciliation Report.
10	The contractor shall indicate the GMS fee collected as a credit on the monthly invoice.

#### C.3.6.2.2.5 Step 5--GSA Verifies and Validates Centralized Billing Data

ID Number	Description
1	The contractor shall accept from GSA, within 1 business day of receipt of files, a Notification of Receipt of Invoice, Detail Billing, and Adjustments Files that data files have been received. See Section C.3.6.2.3.1, GSA Data Provided to Contractors.
2	The contractor shall accept from GSA, within 7 business days of receipt of files, a Notification of Data File Loading Problems if data files cannot be loaded or are not complete. See Section C.3.6.2.3.1, GSA Data Provided to Contractors.
3	In the event data files are incomplete, the contractor shall notify GSA with the method contractor will use to correct the problem, and provide the complete set of files within one (1) business day.
4	In the event the data files are not loadable, the contractor shall make best effort with GSA to identify the cause of the problem and determine the corrective action(s).
5	For data loading problems isolated to contractor causes, the contractor shall correct the error within one (1) business day.

ID Number	Description
6	In the event the summary data does not match the detail data, the invoice shall be deemed "out-of-balance." The contractor shall accept from GSA an Invoice Billing Data Files Out-of-Balance Report. GSA will reject the invoice within seven (7) calendar days of receipt of all Invoice copies and data files. See Section C.3.6.2.3.1, GSA Data Provided to Contractors.
7	In the case of the Government's request for resubmitted billing files, the Contractor shall accept the data media, and the Contractor shall deliver new corrected Invoice and Detail Billing data files within one (1) business day.
8	The Contractor shall accept from GSA a Receipt of Acceptably Balanced Centralized Billing Data Files Acknowledgement after it has verified that the files are readable and loadable and the invoice file balances to the Detail Billing File(s). See Section C.3.6.2.3.1, GSA Data Provided to Contractors.
9	GSA will start the Prompt Payment Clock in accordance with FAR (See Section I.1.62 Prompt Payment) when one copy of the Invoice File has been delivered to the GSA Office of Finance and one copy of the Invoice File and the Detail Billing File(s) to the GSA Program Office and the data files have been verified as complete and loadable, and the Invoice File balances to the Detail Billing File(s).
10	GSA reserves the right to reject the invoice in accordance with the Prompt Payment Act. Notification of invoice rejection will be within seven (7) calendar days of start of Prompt Payment.

**C.3.6.2.2.6 Step 6--Government/Contractor Dispute Process**

ID Number	Description
1	The contractor shall follow the Government/Contractor Dispute process covered in Section C.3.6.3 Billing Disputes and Adjustments

**C.3.6.2.2.7 Step 7--GSA Issues Centralized Payment to Contractor**

ID Number	Description
1	GSA Office of Finance will adjust payment as necessary for any interest accrued due to the Prompt Payment clause.
2	GSA will prepare the receiving report for amount of payment.
3	GSA Office of Finance will adjust payment as necessary for Over 30 Day payment clause.
4	Payment will be the invoice amount less the GSA Management Service fee, non-compliance amounts and any amounts withheld by GSA. See Section C.3.6.3, Disputes and Adjustments.
5	GSA Office of Finance will pay the contractor via US Treasury electronic funds transfer. (See Section C.3.6.2.3.1.1 Contractor Payment)

**C.3.6.2.2.8 Step 8--The Contractor Maintains and Retain Copies of all Contract-Related Billing Data**

ID Number	Description
1	The contractor shall maintain and retain for ten years after termination or expiration of the contract copies of all data, letters, electronic mail, memorandums, adjustment data and other data pertaining to the billing of contract services as specified in Section G.5, Billing.
2	The contractor shall provide reports and data fulfilling requests for archived information and data to the Government in a format acceptable to the Government within 5 business days after receiving the Government's request.

**C.3.6.2.3 Centralized Billing Data Requirements**

**C.3.6.2.3.1 GSA Data Provided to Contractors**

**C.3.6.2.3.1.1 Contractor Payment**

Payment file is forwarded from GSA Office of Finance to the Department of Treasury for disbursement to contractors after invoice has been authorized and payment certified.

**C.3.6.2.3.1.1.1 Frequency – Contractor Payment**

**C.3.6.2.3.1.1.2 Media/Transport/Format – Contractor Payment**

Data		
Media	Transport	Data Format
File Server	<ul style="list-style-type: none"> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>Electronic Funds transfer</li> </ul>

**C.3.6.2.3.1.1.3 Record Elements – Contractor Payment**

ID Number	Data Elements	Description
1		All data elements per Dept. of Treasury transaction for EFT

**C.3.6.2.3.1.2 Notification of Receipt of Billing Invoice Detailing Billing and Adjustments Files**

**C.3.6.2.3.1.2.1 Frequency – Notification of Receipt of Invoice, Detail Billing, and Adjustment Files**

- As required

**C.3.6.2.3.1.2.2 Media/Transport/Format – Notification of Receipt of Invoice Detail Billing, and Adjustment Files**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> </ul>

Data		
Media	Transport	Format
	<ul style="list-style-type: none"> <li>Attachment to E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.3.1.2.3 Record Elements – Notification of Receipt of Invoice, Detail Billing, and Adjustment Files**

ID Number	Data Elements	Description
1	Title	Notification of Receipt of Contractor Billing Files – these are to include all files necessary for GSA to balance and verify the invoice, for both Centralized and Direct invoices.
2	Date	Date of receipt of files at GSA
3	File Identification 1	Name of Data set
4	File Identification 2	Record and block formatting (if applicable)
5	File Identification 3	Media numbers (tape or Volume Serial Number (volser) numbers, for example)
6	Missing file(s)	List of any files that were not included in the delivery, but were listed in the Contractor Notification of Pending Delivery.
7	Contractor	Contractor Name and Number

**C.3.6.2.3.1.3 Notification of Data File Loading Problems**

**C.3.6.2.3.1.3.1 Frequency – Notification of Data File Loading Problems**

- As required

**C.3.6.2.3.1.3.2 Media/Transport/Format – Notification of Data File Loading Problems**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.3.1.3.3 Record Elements – Notification of Data File Loading Problems**

ID Number	Data Elements	Description
1	Title	Notification of Contractor Billing Data Files in Error
2	Date	Date of Notification
3	Reason	Confirmed or suspected reason for the problem with the file(s). Reason for each problem if more than one. Examples: Incomplete files, incorrect record length or blocking size, physical media corrupted.
4	Contractor	Contractor Name and Contract Number

**C.3.6.2.3.1.4 Invoice Billing Data Files Out-of Balance Report**

**C.3.6.2.3.1.4.1 Frequency – Invoice Billing Data Files Out-of Balance Report**

- Monthly, by 7 calendar days after receipt of the data files

**C.3.6.2.3.1.4.2 Media/Transport/Format – Invoice Billing Data Files Out-of Balance Report**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to E-Mail</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97</li> </ul>

Data		
Media	Transport	Format
	<ul style="list-style-type: none"> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	through 2003 <ul style="list-style-type: none"> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.3.1.4.3 Record Elements – Invoice Billing Data Files Out-of Balance Report**

ID Number	Data Elements	Description	Frequency
1	Report Title	Contractor Billing Data Out-of-Balance Report	Monthly (by (7) calendar days after receipt of the data files)
2	Report Period	Dates of Invoice Charges (example: 6/01/2003 to 6/30/2003)	
3	Report Date	Date the Out-of-Balance Report was created	
4	Contractor	Contractor Name/Contract Number	
5	Item Description Column	To include all services represented on the invoice billing data, plus the GMS Fee, Contractor Adjustments and any other charges/adjustments as included on the invoice.	
6	Invoice Column	Summary billing charges for each item from the summary billing data	
7	Detail Column	Summarized charges from the detailed billing files for each item.	
8	Balance Column	Difference between summary charges and detail charges for each item (expressed in positive or negative amounts: Invoice Amount minus Detail Amount = Balanced Amount)	
9	Total	Total Out-of-Balance Amount	
10	Notes	Footnotes or addendum with any explanatory information as needed	

**C.3.6.2.3.1.5 Receipt of Acceptably Balanced Centralized Billing Data Files Acknowledgement**

**C.3.6.2.3.1.5.1 Frequency – Receipt of Acceptably Balanced Centralized Billing Data Files Acknowledgement**

- As required

**C.3.6.2.3.1.5.2 Media/Transport/Format – Receipt of Acceptably Balanced Centralized Billing Data Files Acknowledgement**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.3.1.5.3 Record Elements – Receipt of Acceptably Balanced Centralized Billing Data Files Acknowledgement**

ID Number	Data Elements	Description
1	Date	Date of Message
2	Invoice Date	Date of Invoice
3	Receipt Date	Date the all the Invoices were received by GSA and judged complete
4	Prompt Pay Date	Notice of the date when the thirty (30) days Prompt Payment Clock will begin.
5	Payment Information	May be provided by GSA in this electronic mail.
6	Dispute Information	May be provided by GSA in this electronic mail.
7	Contractor	Contractor Name/Contract Number

**C.3.6.2.3.2 Contractor Data Provided to Government**



**C.3.6.2.3.2.1 Centralized Billed Invoice, Detail Billing, and Adjustment Files**

**C.3.6.2.3.2.1.1 Frequency – Centralized Billed Invoice, Detail Billing, and Adjustment Files**

- Initial: 15 business days after close of first month in which contractor has billable charges for Centralized Billed customers
- Updated: Monthly, within 15 business days after the end of the preceding calendar month

**C.3.6.2.3.2.1.2 Deliver To - Centralized Billed Invoice, Detail Billing, and Adjustment Files**

- GSA PMO
- Agency

**C.3.6.2.3.2.1.3 Media/Transport/Format – Centralized Billed Invoice, Detail Billing, and Adjustment Files**

**C.3.6.2.3.2.1.3.1 Media/Transport/Format – Centralized Billed Invoice, Detail Billing, and Adjustment Files sent to GSA**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	

\*Media type changes per section C.3.1.2

**C.3.6.2.3.2.1.3.2 Media/Transport/Format – Centralized Billed Invoice, Detail Billing, and Adjustment File sent to Agency**

Data		
Media	Transport	Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
		<ul style="list-style-type: none"> <li>• Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.2.3.2.1.4 Record Elements – Centralized Billed Invoice, Detail Billing, and Adjustment Files**

ID Number	Data Elements	Description
1	Title	Direct-Billed Invoice, Detail Billing, and Adjustments Files
2	Invoice File Elements	See Attachment J.12.4.1, Unit 1: Invoice File

ID Number	Data Elements	Description
3	Detail Billing File Elements	See Attachment J.12.4.2, Unit 2: Detail Billing File
4	Adjustment Data File Elements	See Attachment J.12.6, Adjustments

**C.3.6.2.3.2.2 Monthly Billing Informational Memorandum**

Report to include, but is not limited to, items that will explain changes in billing, changes to data formats, new services added to the billing, and issues pertaining to balancing charges.

**C.3.6.2.3.2.2.1 Frequency - Monthly Billing Informational Memorandum**

- Monthly, to be delivered with the Invoice

**C.3.6.2.3.2.2.2 Deliver To – Monthly Billing Informational Memorandum**

- GSA PMO
- Agency

**C.3.6.2.3.2.2.3 Media/Transport/Format – Monthly Billing Informational Memorandum**

**C.3.6.2.3.2.2.3.1 Media/Transport/Format – Monthly Billing Informational Memorandum sent to GSA**

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed</li> </ul>

Report		
Media	Transport	File Format
		between GSA and contractor

**C.3.6.2.3.2.2.3.2 Media/Transport/Format – Monthly Billing Informational Memorandum sent to Agency**

Report		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> </ul>

Report		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.2.3.2.2.4 Content – Monthly Billing Informational Memorandum**

ID Number	Data Elements	Data Elements
1	Title of Report	Contractor Monthly Billing Informational Memorandum
2	Contractor	Contractor Name and Contract Number
3	Date	Date of Report
4	New Agency Hierarchy Codes	Agency hierarchy codes added since the previous billing period and associated data elements provided by the Agency
5	Other Information	List of other information that applies to all Centralized Billed Agencies and the current invoice. This includes, but is not limited to, items that will explain changes in billing, changes to data formats, new services added to the billing, and issues pertaining to balancing charges.)

**C.3.6.2.3.3 Contractor Data Provided to GSA**

**C.3.6.2.3.3.1 Contractor Notification of Pending Delivery of Invoice, Detail Billing, and Adjustment Files**

**C.3.6.2.3.3.1.1 Frequency – Contractor Notification of Pending Delivery of Invoice, Detail Billing, and Adjustment Files**

- Within 1 business day of sending the Invoice, Detail Billing, and Adjustment Files

**C.3.6.2.3.3.1.2 Deliver To - Contractor Notification of Pending Delivery of Invoice, Detail Billing, and Adjustment Files**

- GSA PMO

**C.3.6.2.3.3.1.3 Media/Transport/Format – Contractor Notification of Pending Delivery of Invoice, Detail Billing, and Adjustment Files**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> </ul>

Data		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.3.3.1.4 Record Elements – Contractor Notification of Pending Delivery of Invoice, Detail Billing, and Adjustment Files**

ID Number	Data Elements	Description
1	Report Title	Notification of Pending Delivery of Invoice
2	Contractor	Contractor Name / Contract Number
3	Destination	Delivery destination of each document or file
4	Delivery Type	Method of delivery (i.e., Airborne, electronic mail, secure FTP, etc.)
5	Date	Date each item is to be sent
6	Item Sent	Name of each item included with the Invoice (i.e., Centralized Remit, Detailed Adjustments, etc.)
7	File detail	Electronic file name plus extension (i.e., Data dictionary.doc, detailadj.txt, etc.), record count, and data file size.
8	Media Type	Type of media used for the transmission of the data (i.e., document, CD-ROM, DVD, Mag Tape)

**C.3.6.2.4 Centralized Billing Report Requirements**

**C.3.6.2.4.1 Contractor Reports Provided to GSA**

**C.3.6.2.4.1.1 Monthly Invoice**

**C.3.6.2.4.1.1.1 Frequency - Monthly Invoice**

- Monthly, by the 15th business day of the month

**C.3.6.2.4.1.1.2 Deliver To – Monthly Invoice**

- GSA Office of Finance
- GSA PMO

**C.3.6.2.4.1.1.3 Media/Transport/Format – Monthly Invoice**

Report		
Media	Transport	File Format

Report		
Media	Transport	File Format
Paper (Original to GSA Finance Office)	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
File Server GSA PMO or GSA Office of Finance	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.4.1.1.4 Content – Monthly Invoice**

ID Number	Data Elements	Description
1	Invoice –File Elements	See Attachment J.12.4.1, Unit 1: Invoice File

**C.3.6.2.4.1.2 GMS Fee Reconciliation Report**

**C.3.6.2.4.1.2.1 Frequency - GMS Fee Reconciliation Report**

- Initial, 60 days after the end of the first month in which contractor had billable charges
- Updated: Monthly, by the 15<sup>th</sup> calendar day of the month

**C.3.6.2.4.1.2.2 Deliver To – GMS Fee Reconciliation Report**

- GSA PMO

**C.3.6.2.4.1.2.3 Media/Transport/Format – GMS Fee Reconciliation Report**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> </ul>	

Report		
Media	Transport	File Format
	<ul style="list-style-type: none"> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>HTML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.4.1.2.4 Content – GMS Fee Reconciliation Report**

ID Number	Data Elements	Description
1	Date	Date of Message
2	Invoice Date	Date of Invoice
3	GMS Table	Balancing table of all GMS fees by Centralized and Direct, Services and Products
4	Agency Detail	For each Agency, billed revenue, fee collected
5	Contractor	Contractor Name and Contract Number

**C.3.6.2.4.1.3 Invoice Change Notice**

**C.3.6.2.4.1.3.1 Frequency - Invoice Change Notice**

- As required, 60 days prior to change of invoice

**C.3.6.2.4.1.3.2 Deliver To – Invoice Change Notice**

- GSA PMO

**C.3.6.2.4.1.3.3 Media/Transport/Format – Invoice Change Notice**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>Facsimile</li> <li>Courier</li> <li>Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>Courier</li> </ul>	<ul style="list-style-type: none"> <li>MS Excel 97</li> </ul>



Report		
Media	Transport	File Format
File Server	<ul style="list-style-type: none"> <li>Postal</li> </ul>	through 2003
	<ul style="list-style-type: none"> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>PDF</li> <li>ASCII Text</li> <li>HTML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.2.4.1.3.4 Content – Invoice Change Notice**

ID Number	Data Elements	Description
1	Date	Date of Message
2	Invoice Date	Date of Invoice
3	Invoice Changes	All changes to be made on the invoice
4	Contractor	Contractor Name and Contract Number

**C.3.6.3 Billing Disputes and Adjustments**

**C.3.6.3.1 Process Definition**

**C.3.6.3.1.1 Billing Disputes and Adjustments Description**

A billing inquiry is a question or issue that may lead to a billing dispute. The Government is required to certify contractor invoices each month. During that process, billing inquiries will arise and the contractor supports those billing inquiries. Additionally, Government systems analyze invoice data and generate billing disputes in files that are sent to the contractor. The contractor maintains a web-based billing disputes system and database and allows Government access to that database to enter disputes and update them. The contractor is required to resolve disputes within a specified time frame that starts with the submission of the dispute by the Government and ends with the resolution of the dispute.

**C.3.6.3.1.2 Billing Disputes and Adjustments Process Narrative**

Step Number	Description	Executing Entities
1	Agency determines there is a billing inquiry.	Agency
2	Agency consults with the contractor to determine if billing inquiry becomes a billing dispute.	Agency/Contractor
3	For centralized bills, a GSA system checks for contractual compliance of the invoice.	GSA
4	Agency or GSA files a billing dispute with contractor.	Agency/GSA/Contractor
5	GSA receives and stores billing disputes from contractor.	GSA
6	Contractor manages the billing disputes.	Contractor
7	Agency works with contractor to resolve the billing dispute.	Agency/Contractor
8	Agency may escalate billing dispute to GSA.	Agency
9	GSA works with contractor to resolve GSA-filed billing disputes and Agency escalated disputes.	GSA/Contractor
10	GSA Contracting Officer and contractor resolve the billing dispute when escalated.	GSA/Contractor
11	Contractor sends Dispute Resolution Confirmation to Agency.	Contractor
12	GSA and Agency monitor disputes.	GSA/Agency
13	Contractor issues adjustment and retains information.	Contractor
14	GSA notifies contractor of non-compliance payment reduction – Centralized Billing.	GSA/Contractor
15	For Centralized bills, GSA adjusts payment.	GSA

**C.3.6.3.2 Billing Disputes and Adjustments Functional Requirements**

This Section C.3.6.3.2 contains requirements that pertain only to the contractor, as identified in Executing Entities portion of Section C.3.6.3.1.2, Billing Disputes and Adjustments Process Narrative. This Section does not include subsections for process steps executed solely by the GSA or the Agency, since those steps do not contain functional requirements for performance by the contractor. The title of each subsection of this Section C.3.6.3.2, Billing Disputes and Adjustments Functional Requirements, is based on the Step Number and Description of the process step identified in Section C.3.6.3.1.2, Billing Disputes and Adjustments Process Narrative.

**C.3.6.3.2.1 Step 2--Agency Consults with Contractor to Determine if Billing Inquiry become a Billing Dispute**

ID Number	Description
1	The contractor shall accept billing inquiries during normal business hours.
2	The contractor shall accept billing inquiries from Agencies in the media types specified in Section C.3.6.3.2.1 Billing Inquiry, as mutually agreed upon by the contractor and the Agency.
3	Government initiated Billing inquiries include the invoice number associated with the inquiry, date of invoice, contractor account number, contractor service number that applies, name of person making the inquiry, preferred method of communication, contact information, date the inquiry was sent and detailed description of the inquiry.
4	The contractor shall record all billing inquiries, including but not limited to, informal telephone inquiries.
5	Contractor personnel, knowledgeable in contractor's system configuration and

ID Number	Description
	procedures in support of Government billing, shall research the billing inquiry.
6	The contractor shall respond with an explanation or a recommendation to submit a billing dispute to the inquiry initiator.
6.1	The contractor shall respond within 1 business day of the sending of the billing inquiry.
6.2	The contractor shall respond in either the initiator's requested media or in the same media as the original inquiry.
7	The contractor shall provide "read only" access to a pricing tool to enable Government to verify pricing of billed charges with history available through all contract years.

#### C.3.6.3.2.2 Step 4--Agency or GSA Files a Billing Dispute with Contractor

ID Number	Description
1	The contractor shall accept billing disputes from Agencies during normal business hours.
2	The contractor shall accept billing disputes from Agencies in the media types specified in Section C.3.6.3.3.2.2 Billing Dispute, as mutually agreed upon by the Contractor and the Agency.
3	The contractor shall accept billing disputes from Agencies, containing the data elements specified in Section C.3.6.3.3.2.2. Billing Dispute.
4	The contractor shall assign a contractor tracking number to each dispute received from the Government.
5	The contractor shall accept and retain the Agency dispute number associated with the billing dispute.
6	The contractor shall provide confirmation of receipt for each dispute with the Agency dispute number and contractor's dispute number within one business day. (See Attachment J.12.5.2 Dispute Receipt Acknowledgement)
7	The contractor shall provide confirmation of receipt from the Government in the media types specified in Section C.3.6.3.3.5.1, Dispute Receipt Acknowledgement, as mutually agreed upon by the contractor and the Government.
8	The contractor shall provide confirmation of receipt from the Government, containing the data elements as specified in Section C.3.6.3.3.5.1, Dispute Receipt Acknowledgement.
9	The contractor shall resolve all disputes that are less than or equal to \$15,000 within 60 calendar days and disputes that are greater than \$15,000 within 90 calendar days.

#### C.3.6.3.2.3 Step 6--Contractor Manages the Billing Disputes

ID Number	Description
1	The contractor shall maintain a web-based system and database to manage billing disputes.
2	The contractor shall provide access to its system to Agencies to enable Agencies to directly and immediately enter new billing disputes, to inquire, view, track, and print existing disputes for their Agency only, and to download disputes that apply to their Agency alone.
3	The contractor shall update the database on a daily basis with status changes and new disputes received from Agencies.
4	The contractor shall accept and update the database with the Monthly New GSA Disputes file provided by GSA containing new GSA initiated disputes and Agency

ID Number	Description
	initiated disputes escalated to GSA.
5	The contractor shall accept new disputes from the GSA in the media types specified in Section C.3.6.3.3.1.1, Monthly New GSA Disputes file, as mutually agreed upon by the contractor and the GSA.
6	The contractor shall accept new disputes from the GSA, containing the data elements specified in Section C.3.6.3.3.1.1, Monthly New GSA Disputes file.
7	The contractor shall allow access to its dispute database to permit Agencies and the GSA to create Ad Hoc Reports.
8	The contractor shall provide training to Agencies and GSA regarding use of its system.
9	Within 5 business days after the end of the calendar month, the contractor shall provide a monthly Contractor Disputes File to GSA containing detailed information on each dispute opened during the month, each dispute closed within the last month, and all disputes still outstanding. See Section C.3.6.3.3.3.1 Contractor Disputes File
10	The contractor shall provide the Contractor Disputes File in the media types specified in Section C.3.6.3.3.3.1, Contractor Disputes File, as mutually agreed upon by the contractor and the GSA.
11	The contractor shall provide the Contractor Disputes File, containing the data elements specified in Section C.3.6.3.3.3.1, Contractor Disputes File.
12	The contractor shall provide a monthly Contractor Open Disputes Report to GSA in a matrix form with columns listing the age of the dispute in calendar days (0-15), (16-45), (46-60), (61-90), and 90+, rows with dispute value ranges (0-\$5,000), (\$5,000-\$15,000), (\$15,000-\$25,000) (\$25,000-\$50,000) and over \$50,000, and with each cell containing the following: By Agency and service, the number of open disputes and value of those disputes. See Section C.3.6.3.4.1.1, Contractor Open Disputes Report.
12.1	The contractor shall provide the Contractor Open Disputes Report to GSA in the media types specified in Section C.3.6.3.4.1.1, Contractor Open Disputes Report to GSA, as mutually agreed upon by the contractor and the GSA.
12.2	The contractor shall provide the Contractor Open Disputes Report to GSA containing the data elements specified in Section C.3.6.3.4.1.1 Contractor Open Disputes Report to GSA.
13	In those cases that show disputes not in compliance with the contract, the contractor shall provide GSA with an explanation and propose a resolution and timeframe to close the dispute.
14	The contractor shall provide a monthly Contractor Open Disputes Report to the Agency in a matrix form with columns listing the age of the dispute in calendar days (0-15), (16-45), (46-60), (61-90), and 90+, rows with dispute value ranges (0-\$5,000), (\$5,000-\$15,000), (\$15,000-\$25,000) (\$25,000-\$50,000) and over \$50,000, and with each cell containing the following: By service, the number of open disputes and value of those disputes for only the Agency requesting the report. See Section C.3.6.3.4.1.1
14.1	The contractor shall provide the Contractor Open Disputes Report to Agency in the media types specified in Section C.3.6.3.4.1.1, Contractor Open Disputes Report to Agency, as mutually agreed upon by the contractor and the Agency.
14.2	The contractor shall provide the Contractor Open Disputes Report to GSA containing the data elements specified in Section C.3.6.3.4.1.1, Contractor Open Disputes Report to Agency.
15	In those cases that show disputes not in compliance with the contract, the contractor will provide the Agency with an explanation and propose a resolution and timeframe for closing the dispute.
16	The contractor shall maintain copies of all letters, documents, memoranda, computer files and any other materials relating to billing disputes and adjustments for a period

ID Number	Description
	of ten years after termination or expiration of the contract.
17	The contractor shall provide reports and data fulfilling requests for archived information and data to the Government in a format acceptable to the Government within 5 business days after receiving the Government's request up to ten years after the expiration or termination of the contract.

#### C.3.6.3.2.4 Step 7--Agency Works with Contractor to Resolve the Billing Dispute

ID Number	Description
1	The contractor shall resolve the dispute by any one of the three following approaches:
1.1	The contractor shall issue a dispute resolution for the full amount (See Step 11 Contractor Sends Dispute Resolution confirmation to Agency) followed by an adjustment in the next invoice (See Step 13--Contractor Issues Adjustment) and retains information.
1.2	The contractor shall provide evidence acceptable to the Agency that the disputed amount should be reduced, shall issue a dispute resolution confirmation for that reduced amount and an adjustment in that reduced amount in the next invoice.
1.3	The contractor shall provide evidence acceptable to the Agency that the dispute is not valid, and contractor shall issue a dispute resolution confirmation.

#### C.3.6.3.2.5 Step 9--GSA Works with the Contractor to Resolve the GSA Filed Billing Disputes and Agency Escalated Billing Disputes

ID Number	Description
1	The contractor shall resolve the dispute by any one of the three following approaches:
1.1	The contractor shall issue a dispute resolution for the full amount followed by an adjustment in the next invoice (see Step 13--Contractor Issues Adjustment).
1.2	The contractor shall provide evidence acceptable to the GSA that the disputed amount should be reduced, issues a dispute resolution confirmation for that reduced amount, and an adjustment in that reduced amount in the next invoice.
1.3	The contractor shall provide evidence acceptable to GSA that the dispute is not valid, and issues a dispute resolution confirmation.
2	The contractor shall have an internal dispute escalation procedure.

#### C.3.6.3.2.6 Step 10--GSA Contracting Officer and Contractor Resolve the Billing Dispute when Escalated

ID Number	Description
1	The contractor shall resolve the dispute by any one of the three following approaches:
1.1	The contractor shall issue a dispute resolution for the full amount followed by an adjustment in the next invoice, (See Step 13--Contractor Issues Adjustment) and retains information
1.2	The contractor shall provide evidence acceptable to the Contracting Officer that the disputed amount should be reduced, issues a dispute resolution confirmation for that reduced amount, and an adjustment in that reduced amount in the next invoice.
1.3	The contractor shall provide evidence acceptable to the Contracting Officer that the dispute is not valid, and issues a dispute resolution confirmation.

#### C.3.6.3.2.7 Step 11--Contractor Sends Dispute Resolution Confirmation to the Agency

ID Number	Description
1	For Agency initiated disputes, the contractor shall send a dispute resolution confirmation to the Agency.
2	The contractor shall send the Dispute Resolution Confirmation in the media types specified in Section C.3.6.3.3.5.2, Dispute Resolution Confirmation, as mutually agreed upon by the contractor and the Agency.
3	The contractor shall send the Dispute Resolution confirmation containing the data elements specified in Section C.3.6.3.3.5.2, Dispute Resolution Confirmation.
4	The contractor shall send the Dispute Resolution Confirmation within 3 business days of resolving the dispute.

#### C.3.6.3.2.8 Step 13--Contractor Issues Adjustment and retains information

ID Number	Description
1	The contractor shall provide detailed information on adjustments applied to Agency invoices in the Agency Adjustment File by the 15 <sup>th</sup> business day after the conclusion of the contractor billing period.
2	The contractor shall send the Agency Adjustment File in according to Section C.3.6.3.3.5.3, Agency Adjustment File, as mutually agreed upon by the contractor and the Agency.
3	The contractor shall provide detailed information on adjustments applied to GSA invoices in the GSA Adjustment File.
4	The contractor shall send the GSA Adjustment File according to Section C.3.6.3.3.4.1, GSA Adjustment File, as mutually agreed upon by the contractor and the GSA.
5	The contractor shall indicate on a record-by-record basis which records are adjustments, and which records are dispute resolution confirmations if they are included in the same physical file as dispute resolution confirmations.
6	For adjustments to prior invoices, the contractor shall identify the service period and each separate charge type (recurring, nonrecurring, taxes, USF, surcharges, duties, other fees, etc.)
7	The contractor shall maintain and retain for ten years after termination or expiration of the contract copies of all data, letters, electronic mail, memorandums, adjustment data and other data pertaining to the billing of contract services as specified in Section G.5, Billing.
8	Within 5 business days after receiving the Government's request, the contractor shall provide reports and data fulfilling requests for archived information and data to the Government in a format acceptable to the Government for ten years after termination or expiration of the contract.
9	If an Agency has received a commercial invoice for switched access Voice Service which the Agency has ordered from the Networx contractor, the contractor shall credit in full the relevant charges back to the original commercial invoice and re-bill the Agency for the charges at the Networx Voice Service rates
9.1	These adjustments shall occur within the next two billing cycles after receiving the commercial invoice from the Agency.
9.2	The contractor shall provide the Agency a reference to the credit adjustment sufficient to prove that the adjustment has been applied.

### C.3.6.3.2.9 Step 14--GSA Notifies Contractor of Non-compliance Payment Reduction – Centralized Billing

ID Number	Description
1	The contractor shall not receive payment for a single billing charge or portion of a billing charge over 90 calendar days old, unless prior permission has been obtained from the GSA contracting officer.
2	The GSA contracting officer may authorize withholding of funds.
3	The contractor shall not receive payment for duplicate billing charges.
4	The Government will reduce payment for the next invoice for any disputed billing charge in dispute for more than 90 calendar days.
5	GSA will send the contractor a Monthly Non-Compliance Notification, including the contractor invoice number, contractor invoice date, contractor Invoice amount, amount withheld, reason withheld, amount added, reason added, payment total, and EFT expected date. See Section C.3.6.3.3.1.2, Monthly Non-Compliance Notification

### C.3.6.3.3 Billing Disputes and Adjustments Data Requirements

#### C.3.6.3.3.1 GSA Data Provided to Contractors

##### C.3.6.3.3.1.1 Monthly New GSA Disputes File

##### C.3.6.3.3.1.1.1 Frequency – Monthly New GSA Disputes File

- As required

##### C.3.6.3.3.1.1.2 Media/Transport/Format – Monthly New GSA Disputes File

Data		
Media	Transport	Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97</li> </ul>

Data		
Media	Transport	Format
	<ul style="list-style-type: none"> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	through 2003 <ul style="list-style-type: none"> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.3.3.1.1.3 Record Elements – Monthly New GSA Disputes File**

ID Number	Data Elements	Description
1		See Attachment J.12.5, Dispute

**C.3.6.3.3.1.2 Monthly Non-Compliance Notification**

**C.3.6.3.3.1.2.1 Frequency – Monthly Non-Compliance Notification**

- As required

**C.3.6.3.3.1.2.2 Media/Transport/Format – Monthly Non-Compliance Notification**

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between</li> </ul>



Data		
Media	Transport	Format
		GSA and contractor

**C.3.6.3.3.1.2.3 Record Elements – Monthly Non-Compliance Notification**

ID Number	Data Elements	Description
1		See C.3.6.3.2.9 Step 14 – GSA Notifies Contractor of Non-compliance Payment Reduction – Centralized Billing.

**C.3.6.3.3.2 Agency Data Provided to Contractors**

**C.3.6.3.3.2.1 Billing Inquiry**

**C.3.6.3.3.2.1.1 Frequency - Billing Inquiry**

- As required

**C.3.6.3.3.2.1.2 Media/Transport/Format – Billing Inquiry**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> </ul> Other secured or unsecured transport methods as mutually agreed between Agency and contractor	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Internet Attachment to E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> </ul>

Data		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	Not Applicable

**C.3.6.3.3.2.1.3 Record Elements – Billing Inquiry**

ID Number	Data Elements	Description
1		See C.3.6.3.2.1 Step 2 – Agency Consults with contractor to determine if Billing Inquiry becomes a billing dispute.

**C.3.6.3.3.2.2 Billing Dispute**

**C.3.6.3.3.2.2.1 Frequency - Billing Dispute**

- As required

**C.3.6.3.3.2.2.2 Media/Transport/Format – Billing Dispute**

Data		
Media	Transport	Data Format
Paper	<ul style="list-style-type: none"> <li>• Fax</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text</li> </ul>

Data		
Media	Transport	Data Format
	<ul style="list-style-type: none"> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	Fixed Record <ul style="list-style-type: none"> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.3.3.2.3 Record Elements – Billing Dispute**

ID Number	Data Elements	Description
1		See Attachment J.12.5.1, Unit 1: Dispute Data Elements

**C.3.6.3.3.3 Contractor Data Provided to Government**

**C.3.6.3.3.3.1 Contractor Disputes File**

**C.3.6.3.3.3.1.1 Frequency – Contractor Disputes File**

- Initial
  - To GSA Within 5 business days after the end of the first calendar month in which a dispute was submitted by an Agency
  - To Agency: Within 5 business days after the end of the first calendar month in which a dispute was submitted by the filing Agency
- Updated: Monthly, 5 business days after the end of the calendar month

**C.3.6.3.3.3.1.2 Deliver To - Contractor Disputes File**

- GSA PMO
- Filing Agency

**C.3.6.3.3.3.1.3 Media/Transport/Format – Contractor Disputes File**

**C.3.6.3.3.3.1.3.1 Media/Transport/Format – Contractor Disputes File sent to GSA**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	

Data		
Media	Transport	Data Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.3.3.1.3.2 Media/Transport/Format – Contractor Dispute File sent to Agency**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.3.3.1.4 Record Elements – Contractor Disputes File**

**C.3.6.3.3.1.4.1 Record Elements – Contractor Disputes File sent to GSA**

ID Number	Data Elements	Description
1		See Attachment J.12.5.1: Unit 1: Disputes Data Elements

**C.3.6.3.3.1.4.2 Record Elements – Contractor Disputes File sent to Agency**

ID Number	Data Elements	Description
1		See Attachment J.12.5 1, Unit 1: Dispute Data Elements

**C.3.6.3.3.4 Contractor Data Provided to GSA**

**C.3.6.3.3.4.1 GSA Adjustment File**

**C.3.6.3.3.4.1.1 Frequency – GSA Adjustment File**

- Monthly, with invoice and Detail Billing files

**C.3.6.3.3.4.1.2 Deliver To - GSA Adjustment File**

- GSA PMO

**C.3.6.3.3.4.1.3 Media/Transport/Format – GSA Adjustment File**

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	

**C.3.6.3.3.4.1.4 Record Elements – GSA Adjustment File**

ID Number	Data Elements	Description
1		See Attachment J.12.6 Adjustments.

**C.3.6.3.3.5 Contractor Data Provided to Agency**

**C.3.6.3.3.5.1 Dispute Receipt Acknowledgement**

**C.3.6.3.3.5.1.1 Frequency – Dispute Receipt Acknowledgement**

- Within 1 business day of receiving a dispute from an Agency

**C.3.6.3.3.5.1.2 Deliver To - Dispute Receipt Acknowledgement**

- Agency
- Direct-Billed Agency

**C.3.6.3.3.5.1.3 Media/Transport/Format – Dispute Receipt Acknowledgement**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and</li> </ul>

Data		
Media	Transport	Format
		contractor
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	Not Applicable

\*Media type changes per section C.3.1.2

**C.3.6.3.3.5.1.4 Record Elements – Dispute Receipt Acknowledgement**

ID Number	Data Elements	Description
1		See Attachment J.12.5.2, Unit 2: Dispute Receipt Acknowledgement

**C.3.6.3.3.5.2 Dispute Resolution Confirmation**

**C.3.6.3.3.5.2.1 Frequency – Dispute Resolution Confirmation**

- Within 3 business days of resolving a dispute

**C.3.6.3.3.5.2.2 Deliver To - Dispute Resolution Confirmation**

- Direct-Billing Agency
- Agency

**C.3.6.3.3.5.2.3 Media/Transport/Format – Dispute Resolution Confirmation**

Data		
Media	Transport	Format
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

Data		
Media	Transport	Format
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.3.3.5.2.4 Record Elements – Dispute Resolution Confirmation**

ID Number	Data Elements	Description
1		See Attachment J.12.5.3, Unit 3: Dispute Resolution Confirmation

**C.3.6.3.3.5.3 Agency Adjustment File**

**C.3.6.3.3.5.3.1 Frequency – Agency Adjustment File**

- Monthly, with Invoice File, Detail Billing File

**C.3.6.3.3.5.3.2 Deliver To - Agency Adjustment File**

- Agency
- Direct-Billed Agency

**C.3.6.3.3.5.3.3 Media/Transport/Format – Agency Adjustment File**

Data		
Media	Transport	Format
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text</li> </ul>



Data		
Media	Transport	Format
		Tab delimited • ASCII Text Fixed Record • XML • Other formats as mutually agreed between Agency and contractor
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.3.3.5.3.4 Record Elements – Agency Adjustment File**

ID Number	Data Elements	Description
1		See Attachment J.12.6, Adjustments.

**C.3.6.3.4 Billing Disputes and Adjustments Report Requirements**

**C.3.6.3.4.1 Contractor Reports Provided to Government**

**C.3.6.3.4.1.1 Contractor Open Disputes Report**

**C.3.6.3.4.1.1.1 Frequency - Contractor Open Disputes Report**

- Initial:
  - Sent to GSA: Within 5 business days after the end of the first calendar month in which a dispute was submitted by an Agency
  - Sent to Agency: Within 5 business days after the end of the first calendar month in which a dispute was submitted by the submitting Agency
- Updated: Monthly, 5 business days after the end of the calendar month

**C.3.6.3.4.1.1.2 Deliver To – Contractor Open Disputes Report**

- GSA PMO
- Agency

**C.3.6.3.4.1.1.3 Media/Transport/Format – Contractor Open Disputes Report**

**C.3.6.3.4.1.1.3.1 Media/Transport/Format – Contractor Open Disputes Report sent to GSA**

Reports		
Media	Transport	Format
File Server	<ul style="list-style-type: none"> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Attachment to Internet E-Mail</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.6.3.4.1.1.3.2 Media/Transport/Format – Contractor Open Disputes Report sent to Agency**

Reports		
Media	Transport	Format
File Server	<ul style="list-style-type: none"> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>HTML</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Attachment to Internet E-Mail</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> </ul>
Reports		
Media	Transport	Format
		<ul style="list-style-type: none"> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.3.6.3.4.1.1.4 Content – Contractor Open Disputes Report**

ID Number	Information Elements	Description
1	Contractor Open Disputes Report	Open Monthly Dispute Report to GSA in a matrix form with columns listing the age of the dispute in calendar days (0-15), (16-45), (46-60), (61-90), and 90+, rows with dispute value ranges (0-\$5,000), (\$5,000-\$15,000), (\$15,000-\$25,000), (\$25,000-\$50,000), and over \$50,000; and with each cell containing the following: For all Agencies: By Agency and service, the number of open disputes and value of those disputes. In those cases that show disputes not in compliance with the contract, the contractor will provide an explanation.
2	Contractor	Name and Contract Number

**C.3.6.4 Shared Tenant Billing**

The contractor provides services to tenants in a building or complex sharing the same channels on the access circuit. These tenants may be either centrally billed or direct billed and ordering uses the Direct Ordering process with each order identified as a Shared Tenant Order (See Sections C.3.6.1, Direct Ordering, C.3.6.2, Centralized Billing, and C.3.5, Service Ordering). The shared access channels are those that may be used by different users at different times and this includes services such as Voice Services (VS) access channels to a location shared by two or more Agencies. For billing shared access services where Automatic Number Identification (ANI) is known, the Government will provide to the contractor an electronic file containing a list of 10-digit telephone numbers and corresponding AHCs. This list facilitates the contractor process of assigning an AHC to each call record. The contractor bills the actual usage directly to the end-users, but the monthly recurring charges (MRC) need to be allocated across the shared tenants. Likewise, for billing non-ANI shared access services, the Government will provide to the contractor the total count of active switched lines in allocation percentage (called Shared Tenant Allocation Percentage File) for billing both usage and MRC across the shared tenants. If a switched access arrangement exists, the 10-digit telephone number must be added to the contractor provisioning system database to ensure billing under contractual pricing structure.

The shared tenant billing process and requirements described herein apply to the Government managed location that follows processes for shared tenant billing services.

**C.3.6.4.1 Shared Tenant Billing Process Definition****C.3.6.4.1.1 Shared Tenant Billing Process Description**

There are two methods of allocation percentage billing: Fixed and Dynamic. Fixed Allocation (For Non-ANI) - The contractor ensures that the monthly percentage allocations provided by the Government will be utilized in the contractor's billing for the following month's invoice for the service. The Fixed Allocation Percentage billing method is used in shared access circuits where the ANI is unknown or not available to the contractor.

Dynamic Allocation (For ANI) - Billing charges are calculated by the contractor based upon the percentage of actual usage on each active ANI lines at a shared tenant location (i.e. outbound usage for non-toll free, inbound usage for toll free). The monthly recurring charges (MRC) are allocated across all the Government tenants on a shared access circuit based upon their total usage for the month. The Dynamic Allocation Percentage billing method is used in shared access circuits where the ANI is known or available to the contractor.

**C.3.6.4.1.2 Shared Tenant Process Narrative**

Step Number	Description	Executing Entities
1	Agency in a Government managed shared access circuit submits a Direct Order for shared tenant local and long distance telecommunication services.	GSA/Agency contractor
2	Contractor processes the Direct Order for shared tenant service and follows the service ordering requirements as stated in Section C.3.5.1, Direct Ordering.	Contractor
3	Government sends a Shared Tenant Fixed Percentage Allocation File to contractor for Non-ANI channels by the 15 <sup>th</sup> calendar day of each month.	GSA/Agency
4	Contractor accepts the Shared Tenant Fixed Allocation File from GSA and processes billing for non-ANI active lines by utilizing the percentage allocation data across Agencies in a shared tenant arrangement.	Contractor
5	Contractor performs Dynamic Allocation for ANI active lines and processes billing by allocating usage percentage across Agencies in a shared tenant arrangement for both usage and dedicated access.	Contractor
6	Contractor accepts and manages Government billing inquiries and billing disputes for shared tenant services.	Contractor

**C.3.6.4.2 Shared Tenant Billing Functional Requirements**

This Section C.3.6.4.2 contains the steps and functional requirements that pertain only to the contractor as the executing entity in a shared tenant billing process (See Section C.3.6.4.1.2 Shared Tenant Process Narrative). This Section does not include subsections for process steps executed solely by the GSA or the Agency, since those steps do not contain functional requirements for performance by the contractor. The title of each subsection of this Section C.3.6.4.2 Shared Tenant Billing Functional Requirements is based on the Step Number and Description of the process step identified in Section C.3.6.4.1.2 Shared Tenant Process Narrative.

**C.3.6.4.2.1 Step 2--Contractor processes the direct order for shared tenant service and follows the ordering requirements as stated in Section C.3.5.1 – Direct Ordering.**

ID Number	Description
1	The contractor shall provide contract services to tenants in a building or complex sharing the same channels on the Government managed integrated access circuit.
2	Upon receipt of a direct order for shared tenant service, the contractor shall immediately update its billing system with the validated data contained in a Direct Order file and the contractor shall follow the same service ordering procedures as stipulated in the

ID Number	Description
	requirements in Section C.3.5.1, Direct Ordering.

**C.3.6.4.2.2 Step 4--Contractor accepts Shared Tenant Fixed Percentage Allocation File from Government and processes billing for non-ANI active lines.**

ID Number	Description
1	The Government will designate shared and non-shared Non-ANI active channels where necessary to ensure correct billing in accordance with functional requirements listed below and those specified in Section C.3.6.1, Direct Billing and Section C.3.6.2, Centralized Billing.
2	For the shared Non-ANI active channels the Government will provide to the contractor the percentage allocation file by the 15 <sup>th</sup> calendar day of the month.
3	Where the ANI (or equivalent) is not available or unknown to the contractor, the Government will provide Shared Tenant Allocation Percentage File that contains two allocation factors specific for Government shared tenant locations: a) Agency Hierarchy Code (AHC) b) Percentage Allocation Value up to three (3) decimal places.
4	Percentage Allocation Value (PAV) represents the percentage allocation value for each Billable AHC as provided by the Government.
4.1	The contractor shall validate the Shared Tenant Fixed Allocation Percentage File provided by the Government to ensure that the summation of the Percentage Allocation Value of all AHCs in a shared tenant arrangement must be equal to one hundred percent (100%).
4.2	If the total percentage of all AHCs in a shared tenant arrangement does not equal to one hundred percent (100%), the contractor shall reject the Shared Tenant Fixed Allocation Percentage File immediately and notify the Government to re-submit a corrected Shared Tenant Fixed Allocation Percentage File with the correct summation of PAV equal to one hundred percent (100%).
5	The contractor shall review and validate each Shared Tenant Fixed Allocation Percentage File submitted by Government and determine whether the data elements contained in the Shared Tenant Fixed Allocation Percentage File are valid according to the requirements in Section C.3.6.4.3.1.1, Shared Tenant Fixed Allocation Percentage File.
6	Usage - The contractor shall utilize the fixed percentage allocation data up to three (3) decimal places to allocate the total usage charges, total number of calls, and total called minutes on the invoice data and charge to the proper levels of the AHC.
7	MRC – The contractor shall utilize the fixed percentage allocation data up to three (3) decimal places to allocate the monthly recurring charge (MRC) for the access circuit across shared tenants in a non-ANI active lines and charge to the proper levels of the AHC.
8	The contractor shall ensure that the allocation percentage data, received within fifteen (15) calendar days of the current billing period, shall be utilized in the contractor's billing for the current month's charges (invoice) for the service.
9	The contractor shall accept the Shared Tenant Fixed Allocation Percentage File from the Government Agency specified in Section C.3.6.4.3.2.1, Agency Shared Tenant Fixed Allocation Percentage File, as mutually agreed upon by the contractor and the Government.
10	The contractor shall accept the GSA Shared Tenant Fixed Allocation Percentage File from the Government in Section C.3.6.4.3.1.1, GSA Shared Tenant Fixed Allocation Percentage File.

ID Number	Description
11	The allocation for shared Non-ANI active channels shall include at a minimum, (a) allocations at Government consolidated switches and/or (b) data presented for allocation by an exclusive-use hosting service.
12	The Government reserves the right to provide allocation factors for any shared tenant location to be used in lieu of all other allocation methods.

**C.3.6.4.2.3 Step 5--Contractor performs Dynamic Allocation for ANI active lines and processes billing by allocating usage percentage across Agencies for ANI active lines in a shared tenant arrangement for both usage and dedicated access.**

ID Number	Description
1	The Government will designate shared and non-shared ANI active channels where necessary to ensure correct billing.
2	The contractor shall follow the process for submitting and processing shared tenant service for ANI active channels as specified in the service ordering requirements in Section C.3.5.1, Direct Ordering.
3	Where the ANI (or equivalent) is available or known to the contractor, the Government will provide appropriate station identification data to allow the contractor to associate stations with billed parties.
4	Each month the contractor shall ensure the identification and allocation for billing of ANI channels in an integrated access.
5	The contractor shall perform dynamic allocation billing method at the end of each billing period and prior to producing the current month's invoice.
6	The contractor shall collect inbound and outbound usage data from Government managed location and shall allocate the billing charges across all active ANI switched lines and active ANI dedicated channels.
7	Usage – For ANI shared channels, the contractor shall bill the usage charges directly to the appropriate levels of the AHC as designated by the Government by allocating charges to the AHC based upon actual usage on each of the active ANI lines.
8	MRC - For ANI shared channels, the contractor shall perform dynamic allocation method for dedicated access before billing each Agency for the monthly recurring charges (MRC). The contractor shall allocate dynamically all the usage percentage across Agencies in a shared tenant location by billing the monthly recurring charges to the proper levels of the AHC according to how much each end-user (Agency/tenant) used the service for the current billing period.
8.1	Percentage Allocation Value - The dynamic percentage allocation value shall be calculated by the contractor based on the total cost of the MRC for each active ANI channels shared by end-user (Agency/tenant) in a Government managed location.
9	The contractor shall provide billing invoice and billing detail information of all shared

ID Number	Description
	tenant billing data elements to the Agencies and sub-Agencies in a shared tenant service and shall follow the process for providing billing invoice and billing detail information according to the requirements in Section C.3.6.1, Direct Billing and in Section C.3.6.2 Centralized Billing.
10	The Government reserves the right to provide allocation factors for any shared tenant location to be used in lieu of all other allocation methods.
11	The allocation for shared active channels includes at a minimum, (a) allocations at GSA managed locations and/or (b) data presented for allocation by an exclusive-use hosting service.

**C.3.6.4.2.4 Step 6--Contractor accepts and manage Government billing inquiries and billing disputes for shared tenant services**

ID Number	Description
1	The contractor shall accept billing inquiries and billing disputes submitted by the Government specific to shared tenant services and shall follow the process to resolve billing disputes according to the requirements in Section C.3.6.3, Billing Disputes and Adjustments.

**C.3.6.4.3 Shared Tenant Billing Data Requirements**

**C.3.6.4.3.1 GSA Data Provided to Contractors**

The Government will provide two types of data to the contractor for a shared tenant billing services.

- Direct Order File (see Section C.3.5.1, Direct Ordering)
- Shared Tenant Fixed Allocation Percentage File (Non-ANI)

**C.3.6.4.3.1.1 GSA Shared Tenant Fixed Allocation Percentage File**

**C.3.6.4.3.1.1.1 Frequency – GSA Shared Tenant Fixed Allocation Percentage File**

- As required

**C.3.6.4.3.1.1.2 Media/Transport/Format – GSA Shared Tenant Fixed Allocation Percentage File**

Data		
Media	Transport	Data Format
Paper	<ul style="list-style-type: none"> <li>• Fax</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> </ul>	



Data		
Media	Transport	Data Format
File Server	<ul style="list-style-type: none"> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
	<ul style="list-style-type: none"> <li>Internet File Transfer Protocol (FTP)</li> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

\*Media type changes per section C.3.1.2

#### C.3.6.4.3.1.1.3 Percentage File

ID Number	Data Elements	Description
1	Agency Hierarchy Code	Also known as the "Billable Agency Hierarchy Code," will be utilized by the contractor to bill each active ANI in a shared tenant service.
2	Percentage Allocation Value	The Percentage Allocation Value will be calculated up to three (3) decimal places to allocate a percentage to each proper level of the "Billable Agency Hierarchy Code" based from the total number of active switched and/or dedicated lines in a shared tenant arrangement.

#### C.3.6.4.3.2 Agency Data Provided to Contractor

The Agency will provide two types of data to the contractor for a shared tenant billing services: Shared Tenant Fixed Allocation Percentage File

- Direct Order File (see Section C.3.5.1, Direct Ordering)
- Shared Tenant Fixed Allocation Percentage File (Non-ANI)

#### C.3.6.4.3.2.1 Agency Shared Tenant Fixed Allocation Percentage File

##### C.3.6.4.3.2.1.1 Frequency - Agency Shared Tenant Fixed Allocation Percentage File

- As required

**C.3.6.4.3.2.1.2 Media/Transport/Format – Agency Shared Tenant Fixed Allocation Percentage File**

Data		
Media	Transport	Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	Not Applicable

\*Media type changes per section C.3.1.2

**C.3.6.4.3.2.1.3 Record Elements – Agency Shared Tenant Fixed Allocation Percentage File**

ID Number	Data Elements	Description
1	Agency Hierarchy Code	Also known as the "Billable Agency Hierarchy Code," will be utilized by the contractor to bill each active ANI in a shared tenant service.
2	Percentage Allocation Value	The Percentage Allocation Value will be calculated up to three (3) decimal places to allocate a percentage to each proper level of the "Billable Agency Hierarchy Code" based from the total number of active switched and/or dedicated lines in a shared tenant arrangement.

**C.3.6.4.3.3 Contractor Provided Data to GSA and Agency**

The contractor provides Shared Tenant billing data to GSA as part of the billing files described in Section C.3.6.1, Direct Billing and C.3.6.2, Centralized Billing.

**C.3.6.4.4 Shared Tenant Billing Report Requirements**

None

**C.3.7 Training**

**C.3.7.1 Training Process Definition**

**C.3.7.1.1 Training Process Description**

The contractor develops a training program that it submits to GSA for approval. The contractor makes the training program available to all Government staff. On an ongoing basis, the contractor registers students and delivers the program. GSA evaluates the program by monitoring classes and by receiving training reports. The contractor makes changes to the program over time as needed. NOTE: Land Mobile Radio Service (LMRS) has unique requirements outlined in Section C.2, Technical Requirements, for training, trouble handling, and network management. As such, those portions of the Management and Operations requirements DO NOT apply to LMRS (that is, Sections C.3.3.1, Network Management, C.3.4.2, Trouble and Complaint Handling, and C.3.7, Training).

**C.3.7.1.2 Training Process Narrative**

Step Number	Description	Executing Entities
1	Contractor develops training program	Contractor
2	Contractor makes training available to the Government	Contractor
3	Contractor registers students	Contractor
4	Contractor delivers course or any portion of a training class	Contractor GSA
5	GSA monitors contractor course and students evaluate the course	GSA Contractor Agency
6	Contractor maintains training program throughout the life of the contract	Contractor

### C.3.7.2 Training Functional Requirements

#### C.3.7.2.1 Step 1--Contractor Develops Training Program

ID Number	Description
1	To ensure all Government customers are receiving or have access to current information about the contract, the contractor shall develop a training program.
2	The contractor shall develop and submit to GSA a Network Training Plan describing the contractor's training program.
3	A training course shall be provided and individually tailored for both of the Government population groups listed below:
3.1	<ul style="list-style-type: none"> <li>Designated Agency Representatives (DARs), who are Agency representatives with the authorization to order services and products</li> </ul>
3.2	<ul style="list-style-type: none"> <li>Network Operations, who are Agency representatives with network monitoring responsibilities.</li> </ul>
4	Group training for Designated Agency Representatives shall be required, but not limited to, the following topics:
4.1	<ul style="list-style-type: none"> <li>Overview of Network services, including, at a minimum, services and products, service features, security offerings, and Government roles and responsibilities</li> </ul>
4.2	<ul style="list-style-type: none"> <li>Operational Support Systems, including, at a minimum, service order and tracking system, billing / dispute system, trouble and complaint handling system, and an overview of network management and monitoring systems</li> </ul>
4.3	<ul style="list-style-type: none"> <li>Processes and procedures, including, at a minimum, placing and tracking orders, reporting and tracking troubles and complaints, escalation procedures for problem resolution, resolving billing disputes, obtaining credit adjustments, fraud prevention, including customer premises safeguards, proper service assistance methods, and coordinating with the contractor's Customer Service Office</li> </ul>
4.4	<ul style="list-style-type: none"> <li>Transition, including, at a minimum, contractor and Government roles and responsibilities, preparation activities, ordering and tracking, timeframes, and contract exceptions that apply during transition.</li> </ul>
5	Group training for Network Operations people shall include, but not be limited to, the following:
5.1	a. Overview of Network Services, including, at a minimum, services and products, service features, security offerings, and Government roles and responsibilities
5.2	b. Operational Support Systems, including, at a minimum, trouble and complaint handling system, and an overview of network management and monitoring systems
5.3	<ul style="list-style-type: none"> <li>Processes and procedures, including, at a minimum, reporting and tracking troubles and complaints, escalation procedures for problem resolution, fraud prevention, including customer premises safeguards, proper service assistance methods, and coordinating with the Contractor's Customer Service Office</li> </ul>
5.4	<ul style="list-style-type: none"> <li>Transition, including, at a minimum, contractor and Government roles and responsibilities, preparation activities, timeframes, and contract exceptions that apply during transition.</li> </ul>
6	The contractor's Network Training Plan shall address training delivery methods including: meeting and briefings, classroom, seminars, instructor-led and non-instructor on-line web based, self study, and manuals or desk top guides.
7	The contractor shall provide classes with a maximum class size of 32 and a minimum class size of 10.
8	The contractor shall provide self-study training instructions in the following formats:
8.1	<ul style="list-style-type: none"> <li>Audio/Video tapes</li> </ul>

ID Number	Description
8.2	<ul style="list-style-type: none"> <li>• CD ROM/DVD</li> </ul>
8.3	<ul style="list-style-type: none"> <li>• On-line web based.</li> </ul>
9	The contractor's training plan shall include training evaluation forms to complete requirements of Section C.3.7.2.5, Step 5--GSA Monitors The Course And Students Evaluate The Course.

### C.3.7.2.2 Step 2 -- Contractor Makes Training Available To The Government

ID Number	Description
1	The contractor shall provide all training and training materials as presented and approved in the Networx Training Plan.
2	The contractor shall provide training that is easily accessible to ensure maximum distribution, usefulness and availability.
3	The contractor shall make this training available throughout the life of the contract.
4	The contractor shall make all class room training available at no cost to the Government for up to the following number of students: DARs--1,500 students Network Operations -- 500 students.
5	Once No-Cost classroom training has been delivered to the maximum number of students stated in ID 4, the contractor shall provide for Agencies to directly order classroom training and may charge for that classroom training.
6	The contractor shall make available, at no cost to the Government throughout the life of the contract, training through the following delivery methods: meetings, briefings, seminars, self-study, video-teleconference, and on-line web based.
7	Training shall begin upon Agency's selection of the contractor. Transition training shall end upon Agency transition completion.
8	When requested by GSA, contractor shall provide GSA all the training material used for its training sessions. The Government reserves the right to copy or duplicate any training material used under the Networx program.

### C.3.7.2.3 Step 3--Contractor Registers Students

ID Number	Description
1	The contractor shall manage the registration of attendees and scheduling of classes.
2	The contractor shall provide a Course Catalog within 30 calendar days after Notice to Proceed on its website with information relating to training schedules, course name, classes, location of class, short course description and any information necessary for student attendance. The contractor shall update the Course Catalog as class schedules are added for the courses offered.
3	The contractor shall provide for on-line registration through a website provided by the contractor.
4	The contractor shall include on its website the latest due date for students to cancel enrollment for a scheduled training class without charge.
5	The contractor's training registration website shall allow students to cancel enrollment.
6	The contractor shall notify students by phone or e-mail of registration confirmation, class cancellation or rescheduling of any classes.
6.1	The contractor shall accept student's cancellation of enrollment up to 5 business days prior to the scheduled training date without charge.

ID Number	Description
6.2	In the case of a student cancelling classroom training enrollment past the cancellation due date, the contractor shall notify the student by email that the cancellation is beyond the acceptable time for cancellation. The student will be counted against the class size and either the student will be counted against maximum number allowed without charge or if the Government has exceeded the maximum then the Government will be charged for this student.
6.3	If the student's enrollment cannot be cancelled because the cancellation date was missed, the contractor shall allow transfer of the enrollment to a student currently on the waiting list or another student from the same agency.
6.4	Once the maximum number of students has registered for a class, the contractor shall accept student registration on a waiting list status and notify the student of the waiting list status.
6.5	Contractor Training Cancellation and Rescheduling: In the event the contractor is unable to conduct training on a scheduled training date, the contractor shall notify the registered students at least 3 business days before the scheduled training date.

#### C.3.7.2.4 Step 4--Contractor Delivers the Training

ID Number	Description
1	To ensure all Government customers are receiving or have access to information about the contract, the contractor shall deliver training to the Government.
2	The contractor shall make all classroom training available in all GSA regions (CONUS), where services are offered.
3	The contractor shall be responsible for all expenses incurred by the contractor, including, but not limited to, per diem, transportation, and training facilities. The Government will be responsible for all travel expenses incurred by the Government, including, but not limited to, per diem, and transportation.
4	The contractor shall provide all facilities for training, unless otherwise requested by the Government.
5	If the classroom training will be delivered at a Government facility, the contractor shall make arrangements with the Government's local facility representative and adhere to local requirements.
6	The contractor shall provide all logistics support required for training at the contractor's location.
7	The contractor shall provide training through a variety of delivery methods. The Government reserves the right to determine the delivery method for training to be used. Methods of delivery to be used include, but are not limited to: meetings and briefings, classroom, seminars, instructor-led and non-instructor on-line web based, self study, video-teleconference, and manuals/desk top guides.
8	The contractor shall provide all training in the English language.
9	GSA will, at its discretion, present Government related training topics as part of the contractor's training classes. The contractor shall coordinate the training class syllabus with GSA for those training classes.
10	In order to assist GSA in tracking the satisfaction of the No-Cost training limits, the contractor shall provide a Quarterly Classroom Training Report for all training delivered by a classroom method. Once No-Cost classroom training has been delivered to the maximum number of students stated in C.3.7.2.2, Contractor Makes Training Available To The Government, the contractor may cease delivery of the Quarterly Classroom Training Report.

**C.3.7.2.5 Step 5--GSA Monitors The Course And Students Evaluate The Course**

ID Number	Description
1	GSA reserves the right to monitor training classes to ensure appropriateness of material and presentation.
2	GSA will provide the contractor prior written notice that a training class is being monitored and will identify the individuals (not to exceed two) performing the monitoring.
3	The contractor shall not count attendance of the monitor(s) against the class size or the student attendance.
4	The contractor will be notified by the Contracting Officer in writing of any training that is deemed unacceptable.
5	This notification will identify the portion(s) of the training that are unacceptable.
6	The contractor shall be responsible for correcting the unacceptable issues.
7	The contractor shall provide evaluation forms to be completed (either electronic or paper) at each training class for each attendee.
7.1	Questions on the evaluation form shall pertain to, but not limited to, the following topics: Course objectives, Training material, Instructor, Length of the training class, Training facility, Overall evaluation.
7.2	Ratings shall range from 1 to 5, 5 being the highest, with sections available for specific comments.
7.3	The contractor shall provide a Summary Training Evaluation Report for each training class.
7.4	The Summary Training Evaluation Report will condense each attendee's completed evaluation form showing overall class scores for each question.
7.5	Specific comments shall also be included in the summary training evaluation report.
7.6	This information shall be made available to GSA throughout the life of the contract.

**C.3.7.2.6 Step 6 -- Contractor Maintains The Training Program Throughout The Life of The Contract**

ID Number	Description
1	The contractor shall update and make available all training material within 30 business days of any changes that would precipitate a modification in the training program at no cost to the Government.

**C.3.7.3 Training Data Requirements**

**C.3.7.3.1 GSA Data Provided to Contractor**

**C.3.7.3.1.1 Notification of Training Monitor**

**C.3.7.3.1.1.1 Frequency – Notification of Training Monitor**

- As required

**C.3.7.3.1.1.2 Deliver To – Notification of Training Monitor**

- CSO

**C.3.7.3.1.1.3 Media/Transport/Format – Notification of Training Monitor**

Data		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• Letter size document (8" x11")</li> </ul>
Voice	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• In person</li> </ul>	<ul style="list-style-type: none"> <li>• Not Applicable</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> </ul>	<ul style="list-style-type: none"> <li>• E-Mail Attachment (MS Word 97 through 2003)</li> <li>• Within E-mail (Rich Text Format)</li> </ul>

**C.3.7.3.1.1.4 Record Elements -- Notification of Training Monitor**

ID Number	Data Elements	Description
1	Course Titles	Title of course to be monitored
2	Class Schedules	Date, time, and location of classes to be monitored
3	Name(s)	Name of monitors
4	Contact information	Telephone number and e-mail address of monitors

**C.3.7.3.1.2 Notification of Unacceptable Training****C.3.7.3.1.2.1 Frequency – Notification of Unacceptable Training**

- As required

**C.3.7.3.1.2.2 Deliver To – Notification of Unacceptable Training**

- CSO

**C.3.7.3.1.2.3 Media/Transport/Format – Notification of Unacceptable Training**

Data		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• Letter size document (8" x11")</li> </ul>
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• Rich Text Format</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> </ul>	<ul style="list-style-type: none"> <li>• E-Mail Attachment (MS Word 97 through 2003)</li> <li>• Within E-mail (Rich Text Format)</li> </ul>



**C.3.7.3.1.2.4 Record Elements -- Notification of Unacceptable Training**

ID Number	Data Elements	Description
1	Course Titles	Title of unacceptable course
2	Class Schedule	Date, time, and location of class(es) that were unacceptable
3	Comments	Description of unacceptable results
4	Response Date	Due date to submit recommendation back to CO
5	CO Contact	CO name and mailing address

**C.3.7.3.2 Contractor Data Provided to GSA**

**C.3.7.3.2.1 Course Catalog**

**C.3.7.3.2.1.1 Frequency – Course Catalog**

- Initial: Within 30 days after Notice to Proceed
- Updated: As class schedules are added and course topics modified

**C.3.7.3.2.1.2 Deliver To – Course Catalog**

- Available on-line on contractor’s Subscriber website

**C.3.7.3.2.1.3 Media/Transport/Format – Course Catalog**

Data		
Media	Transport	File Format
File Server	<ul style="list-style-type: none"> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> </ul>	<ul style="list-style-type: none"> <li>• HTML</li> <li>• PDF</li> <li>• Other electronic formats as mutually agreed between GSA and contractor</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

**C.3.7.3.2.1.4 Record Elements-- Course Catalog**

ID Number	Data Elements	Description
1	Course Titles	Course Title
2	Class Schedules	Schedule and location of class offerings for each course
3	Course Descriptions	Short description of course content and prerequisites
4	Other	Any other information necessary

**C.3.7.3.2.2 Training Material**

**C.3.7.3.2.2.1 Frequency – Training Material**

- b. Initial: Upon request
- c. Updated: Upon request

**C.3.7.3.2.2.2 Deliver To – Training Material**

- a. GSA COR
- b. Registered Government Students

**C.3.7.3.2.2.3 Media/Transport/Format – Training Material**

Data		
Media	Transport	File Format
File Server	<ul style="list-style-type: none"> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> </ul>	<ul style="list-style-type: none"> <li>• HTML</li> <li>• PDF</li> <li>• Other electronic formats as mutually agreed between GSA and contractor</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• Rich Text Format</li> </ul>

**C.3.7.3.2.2.4 Record Elements -- Training Material**

Shall contain material to be presented during training

**C.3.7.4 Training Report Requirements**

**C.3.7.4.1 Contractor Reports Provided to GSA**

**C.3.7.4.1.1 Networx Training Plan**

**C.3.7.4.1.1.1 Frequency - Networx Training Plan**

- a. Initial: Included at Contract Award
- b. Final: Reply within the later of 15 business days after receiving GSA comments or 10 days after Notice to Proceed
- c. Updated: Annually, 30 business day after the end of each contract year

**C.3.7.4.1.1.2 Delivery To - Networx Training Plan**

d. GSA COR

**C.3.7.4.1.1.3 Media/Transport/Format - Networx Training Plan**

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• Rich Text Format</li> </ul>
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> </ul>	<ul style="list-style-type: none"> <li>• E-Mail Attachment (MS Word 97 through 2003)</li> </ul>

**C.3.7.4.1.1.4 Content -- Networx Training Plan**

ID Number	Information Elements	Description
1	Title	Networx Training Plan
2	Contractor	Name of Contractor
3	Date	Date of Plan
4	Contents	<p>Networx Training Plan information required in Section C.3.7.2.1:</p> <ul style="list-style-type: none"> <li>Intended student population</li> <li>Topics to be discussed</li> <li>Delivery methods for material</li> <li>Locations for courses</li> <li>Class size</li> <li>Use of self-study training</li> </ul> <p>Course evaluation and improvement methodology and sample training evaluation form</p> <p>Training schedule and procedures for accessing schedule and registering</p> <p>Procedures for ordering additional training above No-Cost limits</p>

**C.3.7.4.1.2 Summary Training Evaluation Report**

**C.3.7.4.1.2.1 Frequency - Summary Training Evaluation Report**

e. Within 15 business days after the end of every calendar month in which training was completed

**C.3.7.4.1.2.2 Delivery To - Summary Training Evaluation Report**

f. GSA COR

**C.3.7.4.1.2.3 Media/Transport/Format - Summary Training Evaluation Report**

Report		
Media	Transport	File Format

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
File Server	<ul style="list-style-type: none"> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

#### C.3.7.4.1.2.4 Content - Summary Training Evaluation Report

ID Number	Information Elements	Description
1	Title	Summary Training Evaluation Report
2	Contractor	Name of Contractor
3	Date	Reporting Period
4	Contents	Summary Training Evaluation Report information required in Section C.3.7.2.5: List of classes delivered and dates Results compiled from each Training Evaluation Form for each class, including numeric scores as well as additional comments Analysis and corrective actions

#### C.3.7.4.1.3 Quarterly Classroom Training Report

##### C.3.7.4.1.3.1 Frequency - Quarterly Classroom Training Report

- g. Within 15 business days after the end of every calendar quarter in which No-Cost training was completed

##### C.3.7.4.1.3.2 Delivery To – Quarterly Classroom Training Report

- h. GSA COR

##### C.3.7.4.1.3.3 Media/Transport/Format - Quarterly Classroom Training Report

Report		
Media	Transport	File Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually</li> </ul>
File Server	<ul style="list-style-type: none"> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> </ul>	

Report		
Media	Transport	File Format
		agreed between GSA and contractor
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

#### C.3.7.4.1.3.4 Content -- Quarterly Classroom Training Report

ID Number	Information Elements	Description
1	Title	Quarterly Classroom Training Report
2	Contractor	Name of Contractor
3	Date	Date of Reporting Period
4	Contents	For each course delivered: Course Titles Agencies Attending Trainees Names Dates of Classes Total number of Trainees trained to date

### C.3.8 Inventory Management

#### C.3.8.1 Inventory Management Process Definition

##### C.3.8.1.1 Inventory Management Process Description

The contractor establishes, maintains, and keeps current a database containing a complete and accurate inventory of all Networkx services being provided to user Agencies. The contractor provides a secure Web-based electronic interface and makes the interface available to the Government so that the Government will be able to access the data, make queries, obtain reports and perform periodic downloads as needed for audits, billing verification, and other Government program management purposes.

The contractor maintains the inventory for all Networkx contract services provided to all its customers; the Government intends also to maintain a separate inventory based on input from the contractor.

##### C.3.8.1.2 Inventory Management Process Narrative

Step Number	Description	Executing Entities
1	GSA identifies the minimum inventory data elements required by service as part of the Service Order Completion Notice (SOCN) requirements Section C.3.5 Service Ordering	GSA

Step Number	Description	Executing Entities
2	As new or enhanced services are added by contract modification, additional inventory data elements will added to the SOCN requirements	GSA
3	The contractor provides the Government with the minimum inventory data elements in the SOCN	Contractor
4	The contractor establishes a inventory for all Networkx services provided to its customers	Contractor
5	The contractor maintains and updates the Networkx Inventory for all Networkx services provided to its customers	Contractor
6	The contractor makes the Networkx Inventory data available to the Government	Contractor
7	The Government uses the inventory data provided by the contractor for audits, billing verification, and other program management purposes	GSA Agency
8	The Government audits the Networkx Inventory data provided to it and advises the contractor of noted discrepancies in the Networkx Inventory data	GSA Agency
9	The contractor investigates Networkx Inventory data discrepancies reported by the Government and works with the Government to resolve them	Contractor
10	The contractor makes corrections to the Networkx Inventory as needed to maintain its accuracy and completeness and issues corrected SOCNs as needed	Contractor
11	The contractor provides Networkx Inventory management system reports	Contractor

### C.3.8.2 Inventory Management Functional Requirements

#### C.3.8.2.1 Step 3--The Contractor provides the Government with the minimum inventory data elements in the Service Order Completion Notice (SOCN)

ID Number	Description
1	The contractor shall deliver the Service Order Completion Notice (SOCN) to the Government electronically as specified in Section C.3.5, Service Ordering
2	The contractor shall use and fully populate in the Networkx Inventory Database the data elements of the SOCN as defined in Attachment J.12.2.5, Service Order Completion Notice .

#### C.3.8.2.2 Step 4--The Contractor establishes a Networkx Inventory for all Networkx services provided to its customers

ID Number	Description
1	The contractor shall establish a database system to contain a Networkx Inventory for all Networkx services provided to its customers
2	The contractor shall demonstrate, by means of an Operational Support System (OSS) Verification Test (Section C.3.9, Operational Support Systems), that the Network Inventory database system capabilities meet or exceed contractual requirements. The contractor shall neither issue a Service Order Confirmation nor proceed with Networkx orders until it successfully completes OSS verification testing.
3	The contractor shall initially populate the Networkx Inventory within one business day of the issuance of Service Order Completion Notices (SOCN) for Networkx services delivered to customers

ID Number	Description
4	The contractor shall populate records of Networkx services in the Networkx Inventory with, at a minimum, all the data elements required in the SOCN for that service
5	The contractor shall meet or exceed the security requirements specified in Section C.3.3.2 Security Management for the database system used for the Networkx Inventory
6	The contractor shall meet or exceed the performance requirements specified in Section C.3.9 Operational Support Systems for the database system used for the Networkx Inventory

**C.3.8.2.3 Step 5--The Contractor maintains and updates the Networkx Inventory for all Networkx services provided to its customers.**

ID Number	Description
1	The contractor shall maintain in the Networkx Inventory the current view of the Networkx services being provided to customers
2	The contractor shall update the Networkx Inventory current view to reflect all additions, deletions or changes in Networkx services being provided within one business day of the issuance of the Service Order Completion Notice (SOCN) for every addition, deletion or change
3	The contractor shall create an electronic snapshot of the Networkx Inventory in its entirety each month as of the date that monthly invoices are created
4	The contractor shall retain all monthly snapshots as part of the Networkx Inventory
5	If desired, the contractor may archive monthly snapshots after three (3) months

**C.3.8.2.4 Step 6--The Contractor makes the Networkx Inventory Data Available to the Government.**

ID Number	Description
1	The contractor shall provide to Government users for the purpose of extracting formatted information, secure web-based query access to the current view and to the monthly snapshots of Networkx services in the contractor maintained Networkx Inventory.
2	The contractor shall limit Agency user access to data in the contractor maintained Networkx Inventory to data relative to the Agency.
3	For access to the contractor maintained Networkx Inventory by Government users, the contractor shall support secure web-based queries using secure browsers with a minimum of 128-bit encryption.
4	For secure web-based queries against the contractor maintained Networkx Inventory, the contractor shall, as a minimum, provide Government users the option to select a user choice of on-line viewing, data file downloading, and data file delivery via e-mail when extracting formatted information from the contractor maintained Networkx Inventory.
5	For secure web-based queries against to the contractor maintained Networkx Inventory, the contractor shall provide Government users the option to allow running a query after business hours and having a data file delivered the next day.
6	For data file downloading or data file delivery in response to a secure web-based query against the contractor maintained Networkx Inventory, the contractor shall, at a minimum, support file formats for Microsoft Access 2002, Microsoft Excel 2002, Comma Separated Values (CSV) with field names included, and tab delimited ASCII text file with field names included.
7	For data file downloading or data file delivery in response to a secure web-based

ID Number	Description
	query against the contractor maintained Networkx Inventory, the contractor shall neither impose any limit on the number of records in files in MS Access, CSV, or tab delimited formats nor impose a limit of less than 65,500 records of requested data on a file in the MS Excel file format.
8	If older monthly snapshots of the Networkx Inventory have been archived, the contractor shall make them available for query access, within three business days of a Government request.
9	The contractor shall retain the monthly snapshots of the Networkx Inventory and provide to the Government as requested for ten (10) years following the expiration or termination of the contract.
10	The contractor shall provide the Government all user documentation needed for secure web-based query access to the Networkx Inventory information.
11	The contractor shall provide on its Networkx web site a link for secure, web-based query access to the contractor-maintained Networkx Inventory information.
12	The contractor shall maintain a link for secure web-based query access to the contractor-maintained Networkx Inventory on its Networkx Web home page.
13	The contractor shall meet or exceed the access security requirements specified in Section C.3.3.2, Security Management for the database system used for the Networkx Inventory.
14	The contractor shall meet or exceed the access performance requirements specified in Section C.3.9, Operational Support Systems for the database system used for the Networkx Inventory .
15	If requested by an Agency, the contractor shall, at no additional expense to the Government, provide a copy of the records, with data field labels, in the current Networkx Inventory or any of the monthly snapshots for that Agency either in their entirety or for a subset specified in the Agency request.
16	If requested by GSA, the contractor shall, at no additional expense to the Government, provide a copy of the record in the current Networkx Inventory in whole or Agency-specific.
17	If the Government has a need to collect data other than what is already provided through the requirements of this contract, the Government may elect to have the contractor collect and provide the data by doing an ICB site survey. Therefore, if the Government orders a site survey, the contractor shall perform the survey and deliver a report in accordance with the elements the ordering Agency requests at the time of ordering. See deliverables requirements for the Site Survey Report in Section C.3.5.1, Direct Ordering.
18	For data file downloading or data file delivery in response to a Government request for a copy of records, the contractor shall, at a minimum, support file formats for Microsoft Access 2002, Microsoft Excel 2002, Comma Separated Values (CSV) with field names included, or tab delimited ASCII text file with field names included.
19	For data file downloading or data file delivery in response to a Government request for a copy of records, the contractor shall neither impose any limit on the number of records in files in MS Access, CSV, and tab delimited formats nor impose a limit of less than 65,500 records of requested data on a file in the MS Excel file format.
20	The contractor shall not restrict the use by the Government of any and all Networkx Inventory data related to this contract during the contract and for ten (10) years following the expiration or termination of the contract.

**C.3.8.2.5 Step 9--The Contractor investigates Networkx Inventory data discrepancies reported by the Government, and works with the Government to resolve them.**



ID Number	Description
1	The contractor shall investigate Networkx Inventory data discrepancies reported by the Government
2	If the contractor does not agree to a correction for Networkx Inventory data discrepancies reported by the Government, the contractor shall advise the Government and shall work with the Government to resolve the issue
3	If the Networkx Inventory discrepancy is escalated to the Networkx Contracting Officer (CO) for resolution, the contractor shall work with the CO to resolve the issue.

**C.3.8.2.6 Step 10--The Contractor makes corrections to the Networkx Inventory as needed to maintain its accuracy and completeness.**

ID Number	Description
1	The contractor shall institute internal verification and audit procedures to ensure that the Networkx Inventory is complete and correct
2	When the contractor discovers a Networkx Inventory data discrepancy, agrees with a Government report of a Networkx Inventory data discrepancy, or is directed by the CO, the contractor shall correct, at no additional cost to the Government, the Networkx Inventory maintained by the contractor
3	When the contractor discovers a Networkx Inventory data discrepancy, agrees with a Government report of a Networkx Inventory data discrepancy, or is directed by the CO as a result of formal discrepancy resolution, the contractor shall also investigate whether or not the Networkx Inventory data elements in the Service Order Completion Notices (SOCN) issued to the Government were correct or in error
4	If the Networkx Inventory data elements in the SOCN issued to the Government were in error, the contractor shall issue, at no additional cost to the Government, a corrected SOCN or a new correct SOCN that clearly references the original error

**C.3.8.2.7 Step 11--The Contractor provides Networkx Inventory management System Reports.**

ID Number	Description
1	The contractor shall provide monthly reports on Networkx Inventory management to the Networkx Program Management Office (PMO)
2	The contractor shall include in Networkx Inventory management report information on the security of the Networkx Inventory system to the PMO
3	The contractor shall include in Networkx Inventory management report information on the performance the Networkx Inventory system to the PMO
4	The contractor shall include in Networkx Inventory management report information on the status of the Networkx Inventory system to the PMO

**C.3.8.3 Inventory Management Data Requirements**

**C.3.8.3.1 GSA Data Provided to Contractor**

**C.3.8.3.1.1 GSA Inventory Data Discrepancies**

**C.3.8.3.1.1.1 Frequency – GSA Inventory Data Discrepancies**

1. As discrepancies occur

**C.3.8.3.1.1.2 Deliver To – GSA Inventory Data Discrepancies**

2. As designated by contractor

**C.3.8.3.1.1.3 Media/Transport/Format – GSA Inventory Data Discrepancies**

Data		
Media	Transport	Data Format
Paper	<ul style="list-style-type: none"> <li>Fax</li> <li>Courier</li> <li>Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>Courier</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>Postal Service</li> <li>Courier</li> <li>Postal</li> </ul>	<ul style="list-style-type: none"> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
Magnetic Tape	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>Internet File Transfer Protocol (FTP)</li> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

\*Media type changes per section C.3.1.2

**C.3.8.3.1.1.4 Record Elements – GSA Inventory Data Discrepancies**

ID Number	Data Elements	Description
1		See Section J.12.5, Disputes

**C.3.8.3.2 Agency Data Provided to Contractor**

**C.3.8.3.2.1 Agency Inventory Data Discrepancies**

**C.3.8.3.2.1.1 Frequency – Agency Inventory Data Discrepancies**

1. As discrepancies occur

**C.3.8.3.2.1.2 Deliver To – Agency Inventory Data Discrepancies**

2. As designated by contractor

**C.3.8.3.2.1.3 Media/Transport/Format – Agency Inventory Data Discrepancies**

The Agency shall provide and deliver Agency Inventory Data Discrepancies to the contractor in accordance with the procedures and in any of the media, transport, and format types described in the Data table in the Data table in Section C.3.1.2, Data and Report Requirements.

**C.3.8.3.2.1.4 Record Elements – Agency Inventory Data Discrepancies**

ID Number	Data Elements	Description
1		See Section J.12.5 Disputes

**C.3.8.3.3 Contractor Data Provided to Government**

**C.3.8.3.3.1 Responses to On-Line Queries**

**C.3.8.3.3.1.1 Frequency – Responses to On-Line Queries**

- As response are required

**C.3.8.3.3.1.2 Deliver To - Responses to On-Line Queries**

- Authorized users as specified by the DAR Administrator

**C.3.8.3.3.1.3 Media/Transport/Format – Responses to On-Line Queries**

**C.3.8.3.3.1.3.1 Media/Transport/Format – Responses to On-Line Queries sent to GSA**

Data		
Media	Transport	Data Format
Paper	<ul style="list-style-type: none"> <li>• Fax</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> <li>• Other formats as mutually</li> </ul>

Data		
Media	Transport	Data Format
		agreed between GSA and contractor

\*Media type changes per section C.3.1.2

### C.3.8.3.3.1.3.2 Media/Transport/Format – Responses to On-Line Queries sent to Agency

The contractor shall provide and deliver the Responses to On-Line Agency Queries to the Agency in accordance with the procedures and in any of the media, transport, and format types described in the Data table in Section C.3.1.2, Data and Report Requirements

### C.3.8.3.3.1.4 Record Elements -- Responses to On-Line Queries

ID Number	Data Elements	Description
1		As defined by the contractor's Data Dictionaries for ordering (Section C.3.5) and for billing (Section C.3.6) and as specified in the Government Query.

### C.3.8.3.3.2 Copy of Records in the Network Inventory

As defined by the contractor for the Network Inventory and as specified in the GSA request.

#### C.3.8.3.3.2.1 Frequency – Copy of Records in the Network Inventory

- As requested, not to exceed one per month

#### C.3.8.3.3.2.2 Deliver To - Copy of Records in the Network Inventory

- GSA requestor
- To be designated by Agency

#### C.3.8.3.3.2.3 Media/Transport/Format – Copy of Records in the Network Inventory

Data		
Media	Transport	Data Format
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• XML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> </ul>

Data		
Media	Transport	Data Format
	(SMTP) <ul style="list-style-type: none"> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>ASCII Text Tab delimited</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

Media type changes per section C.3.1.2.

#### C.3.8.3.3.2.4 Record Elements -- Copy of Records in the Network Inventory

ID Number	Data Elements	Description
1		As defined by the contractor's Data Dictionaries for ordering (Section C.3.5) and for billing (Section C.3.6) and as specified in the Government Query.

#### C.3.8.4 Inventory Management Report Requirements

##### C.3.8.4.1 Contractor Reports Provided to Government

##### C.3.8.4.1.1 User Documentation for Secure, Web-Based Query Access to Network Inventory

##### C.3.8.4.1.1.1 Frequency - User Documentation for Secure, Web-Based Query Access to Network Inventory

- Initial: Included at time of Contract Award
- Updated: As needed to address changes to the database interface, but not more than once every two calendar months, unless with the express consent of the GSA COR

##### C.3.8.4.1.1.2 Delivery To - User Documentation for Secure, Web-Based Query Access to Network Inventory

- Networkx Subscriber Website

##### C.3.8.4.1.1.3 Media/Transport/Format - User Documentation for Secure, Web-Based Query Access to Network Inventory

Report		
Media	Transport	File Format
File Server	<ul style="list-style-type: none"> <li>Internet File Transfer Protocol (FTP)</li> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>PDF</li> <li>HTML</li> <li>Other formats as mutually agreed between</li> </ul>

Report		
Media	Transport	File Format
		GSA and contractor

**C.3.8.4.1.1.4 Content -- User Documentation for Secure, Web-Based Query Access to Networx Inventory**

ID Number	Information Elements	Description
1	Title	User Documentation for Secure, Web-Based Query Access to Networx Inventory
2	Version	Version of Query Interface for which documentation applies
3	Effective Date	Date when document applies
4	Contents	A description of the query process and tools for Networx Inventory Management including searching, sorting, filtering, reporting, downloading and other capabilities available to users.

**C.3.8.4.2 Contractor Reports Provided to GSA**

**C.3.8.4.2.1 Monthly Inventory Management System Reports**

**C.3.8.4.2.1.1 Frequency - Monthly Inventory Management System Reports**

- Initial: Within 10 business days of calendar month in which first SOCN is delivered
- Updated: Monthly, within 10 business days of end of calendar month

**C.3.8.4.2.1.2 Delivery To - Monthly Inventory Management System Reports**

- GSA COR

**C.3.8.4.2.1.3 Media/Transport/Format - Monthly Inventory Management System Reports**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• PDF</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• Other formats as mutually agreed between</li> </ul>

Report		
Media	Transport	File Format
		GSA and contractor

#### C.3.8.4.2.1.4 Content -- Monthly Inventory Management System Reports

ID Number	Information Elements	Description
1	Security Information	See C.3.3.2, Security Management for security information required
2	OSS Performance	See C.3.9, Operational Support Systems for performance information required
3	Record Count	Total Number of Records in Current Inventory
4	Change in Record Count	Change in Number of Records from Last Monthly Report
5	GSA Queries Processed	Number of GSA Queries Processed during Report Period
6	Agency Queries Processed	Number of Agency Queries Processed during Report Period
7	GSA Copy Requests	Number of GSA Network Inventory Copy Requests Processed during Report Period
8	Agency Copy Requests	Number of Agency Network Inventory Copy Requests Processed during Report Period

### C.3.9 Operational Support Systems

#### C.3.9.1 Operational Support Systems Process Definition

##### C.3.9.1.1 Operational Support Systems Process Description

To support this contract, the contractor must have a set of OSS to perform billing, service ordering, customer support, service management, inventory management, training and program management. These functions are a minimum set that will require automation to meet the Government requirements for this contract. Prior to issuing any Service Order Confirmations or proceeding with fulfilling orders, the contractor must demonstrate to the Government, using Government data if provided, that the functionality of these OSS meet the requirements of this contract. The OSS referred to in Section C.3.9 is the Network contract OSS.

The Government will not pay for or otherwise finance the development or maintenance of the contractor's OSS.

##### C.3.9.1.2 Operational Support Systems Process Narrative

Step Number	Description	Executing Entities
1	The contractor determines that the OSS are secure and function at an acceptable level of performance.	Contractor
2	The contractor develops and executes an OSS Verification Test.	Contractor
3	The contractor implements configuration control of its OSS.	Contractor
4	The contractor performs maintenance and restoration of its OSS.	Contractor

### C.3.9.2 Operational Support Systems Functional Requirements

#### C.3.9.2.1 Step 1--Security and Performance

ID Number	Description
1	The contractor shall ensure security requirements are met for all automated operational support systems (OSS) at a moderate impact level and shall support Government security assessments and authorization efforts. General security and deliverable requirements are defined in Section C.3.3.2, Security Management, and detailed requirements are defined in Section C.3.9.5, Operations Support Systems Security Requirements.
2	The contractor shall describe its methods for securing these systems as part of the overall Security Plan.
3	Once approved by the Government, the contractor shall implement and maintain the approved security for these systems. The Government will verify that the required security controls and processes are implemented as approved.
4	The OSS systems shall meet performance requirements for the following:
4.1	Each system shall be available 24x7
4.2	Each system shall have 99% availability, measured as a ratio of time during which the system is available to the user to the total time in the calendar month less scheduled maintenance time
4.3	Each system response to a user input shall be fast enough so as not cause user dissatisfaction according to best commercial practices
4.4	Each system shall meet the requirements addressed elsewhere in this contract such as security management, fault management, and trouble handling

#### C.3.9.2.2 Step 2--Verification Testing

ID Number	Description
1	The contractor shall provide an OSS Verification Test Plan, in accordance with Section E, Inspection and Acceptance at contract award. The Government reserves 15 business days from the date of contract award to reject the plan. During this period the Government will provide the data files for use in the test. The contractor will be given the opportunity to update the plan based on Government comments.
1.1	The contractor shall provide updates to the OSS Verification Test Plan within 10 business days of receipt of Government comments. The Government reserves 15 business days after receipt of the updated plan to reject it. The contractor may repeat this process according to requirements of Section E, Inspection and Acceptance.
2	The contractor shall perform OSS verification testing according to the accepted OSS Verification Test Plan at a mutually agreeable date with the Government. The Government reserves the right to observe all acceptance tests.
2.1	The contractor shall provide an OSS Verification Test Results report, including analysis, within 5 business days after performance of the tests. The Government reserves 10 business days to reject, in part or completely, the test results.
2.2	The contractor shall rerun tests in part or completely, as deemed necessary by the Government, to verify that the Government's comments on the test results have been satisfactorily addressed. The contractor may repeat this process according to requirements of Section E, Inspection and Acceptance.
2.3	The contractor shall complete the verification test process within 60 calendar days of the Notice to Proceed or 60 calendar days after the Government approves the contractor's OSS Verification Test Plan, whichever is later.
2.4	The contractor shall provide a written request to exceed the deadline for completion of the verification test process. The Government reserves the right to reject a request to



ID Number	Description
	exceed the deadline.
3	The contractor shall neither issue a Service Order Confirmation nor proceed with Network orders until it successfully completes OSS verification testing, as indicated by receipt of official Government acceptance of the verification test results. Notice to Proceed is not a substitute for acceptance of verification test results.
4	The contractor shall update the OSS Verification Test Plan per Section E.2.1, OSS Verification Test Plan.
5	If the Government requests, the contractor shall perform and meet the acceptance criteria in Table E.3-1 each time a new service is offered or the contractor modifies the OSS.
5.1	If the Government requests ID #5 be accomplished then the contractor shall provide an OSS Verification Test Results report, including analysis, within 5 business days after performance of the tests. The Government reserves 10 business days to reject, in part or completely, the test results.
5.2	The contractor shall rerun tests in part or completely, as deemed necessary by the Government, to verify that Government comments on the test results have been satisfactorily addressed. The contractor may repeat this process to satisfy the acceptance criteria of Table E.3-1.
5.3	The contractor shall retain test results for each test performed for a minimum of two years.

#### C.3.9.2.3 Step 3--Change Control

Changes to the contractor OSS can take the form of design changes or changes due to system maintenance, depending on the system and nature of the changes. Changes that affect the human or system interface of the contractor's OSS with the Government will most likely have the greatest impact and are the changes being addressed here. It is important that the Government is made aware of such changes in advance so that it can properly assess the impact and manage those changes.

ID Number	Description
1	The contractor shall deliver an OSS Change Management Plan. The OSS change management requirements shall include, at a minimum, how the contractor will conduct the following:
1.1	Informing the Government when OSS design changes are planned and when maintenance changes are required
1.2	Managing and controlling OSS changes
1.3	Incorporating Government review and approval by the Government into the contractor's change management process
1.4	Government training, if required by the changes
1.5	Retesting with the Government to ensure functionality of any impacted interface.
2	The contractor shall notify the Government at least 30 calendar days in advance of any scheduled change to its OSS due to maintenance.
3	In the event of an emergency change, the contractor shall notify the Government as soon as it is known that a change is required.
4	The contractor shall update all relevant Network services documents and information posted on its Website, affected by OSS changes, at no additional cost to the Government and within 5 business days of completing the change.

#### C.3.9.2.4 Step 4--System Failures

ID Number	Description
1	The contractor shall correct outages or impairments of the OSS according to the requirements of Section C.3.3.1, Fault Management, and Section C.3.4.2, Trouble Handling.

### C.3.9.3 Operational Support Systems Data Requirements

#### C.3.9.3.1 GSA Data Provide to Contractors

##### C.3.9.3.1.1 GSA Data for Ordering Systems Test

###### C.3.9.3.1.1.1 Frequency - GSA Data for Ordering Systems Test

- As required by approved OSS Verification Test Plan

###### C.3.9.3.1.1.2 Media/Transport/Format – GSA Data for Ordering Systems Test

Data		
Media	Transport	Data Format
E-Mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Other unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>CSV</li> <li>ASCII Text Tab delimited</li> <li>ASCII Text Fixed Record</li> <li>XML</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

###### C.3.9.3.1.1.3 Record Elements – GSA Data for Ordering Systems Test

Ordering Data Representative of Selected Agencies.

#### C.3.9.3.2 Contractor Data Provided to GSA

- As required by approved OSS Verification Test Plan.

#### C.3.9.3.3 Contractor Data Provided to Agency

- As required by approved OSS Verification Test Plan

### C.3.9.4 Operational Support Systems Report Requirements

#### C.3.9.4.1 Contractor Reports Provided to GSA

##### C.3.9.4.1.1 OSS Verification Test Plan

###### C.3.9.4.1.1.1 Frequency - OSS Verification Test Plan

- Initial: Included at contract award
- Revised: Within 10 business days of Government comments

###### C.3.9.4.1.1.2 Deliver To – OSS Verification Test Plan

- GSA COR

**C.3.9.4.1.1.3 Media/Transport/Format – OSS Verification Test Plan**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

Media type changes per section C.3.1.2

**C.3.9.4.1.1.4 Content – OSS Verification Test Plan**

As required by Section E.3, Verification Testing of Contractor’s Operational Support System.

**C.3.9.4.1.2 OSS Verification Test Results**

**C.3.9.4.1.2.1 Frequency - OSS Verification Test Results**

- Within 5 business days of completion of tests

**C.3.9.4.1.2.2 Deliver To – OSS Verification Test Results**

- GSA COR

**C.3.9.4.1.2.3 Media/Transport/Format – OSS Verification Test Results**

Report
--------

Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• HTML</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>
DVD ROM	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal</li> </ul>	
Magnetic Tape	<ul style="list-style-type: none"> <li>• Courier</li> <li>• Postal Service</li> </ul>	
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	
E-Mail Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97 through 2003</li> <li>• MS Excel 97 through 2003</li> <li>• PDF</li> <li>• ASCII Text</li> <li>• E-Mail Text Message</li> <li>• Other formats as mutually agreed between GSA and contractor</li> </ul>

Media type changes per section C.3.1.2

**C.3.9.4.1.2.4 Content – OSS Verification Test Results**

- As required by approved OSS Verification Test Plan

**C.3.9.4.1.3 OSS Change Management Plan**

**C.3.9.4.1.3.1 Frequency - OSS Change Management Plan**

- Initial: Included at contract award
- Updated: Within 5 business days of completing a change

**C.3.9.4.1.3.2 Deliver To – OSS Change Management Plan**

- a. GSA COR

**C.3.9.4.1.3.3 Media/Transport/Format – OSS Change Management Plan**

Report		
Media	Transport	File Format
Paper	<ul style="list-style-type: none"> <li>• Facsimile</li> <li>• Courier</li> <li>• Postal Service</li> </ul>	Not Applicable
CD ROM	<ul style="list-style-type: none"> <li>• Courier</li> </ul>	<ul style="list-style-type: none"> <li>• MS Word 97</li> </ul>

Report		
Media	Transport	File Format
	<ul style="list-style-type: none"> <li>Postal Service</li> </ul>	through 2003
DVD ROM	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal</li> </ul>	<ul style="list-style-type: none"> <li>MS Excel 97 through 2003</li> </ul>
Magnetic Tape	<ul style="list-style-type: none"> <li>Courier</li> <li>Postal Service</li> </ul>	<ul style="list-style-type: none"> <li>PDF</li> <li>ASCII Text</li> <li>HTML</li> </ul>
File Server	<ul style="list-style-type: none"> <li>Internet File Transfer Protocol (FTP)</li> <li>Secure Internet File Transfer Protocol (FTPS)</li> <li>Internet Hypertext Transfer Protocol (HTTP)</li> <li>Internet Secure Socket Layer (SSL, HTTPS)</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>
E-mail Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between GSA and contractor</li> </ul>	<ul style="list-style-type: none"> <li>MS Word 97 through 2003</li> <li>MS Excel 97 through 2003</li> <li>PDF</li> <li>ASCII Text</li> <li>E-Mail Text Message</li> <li>Other formats as mutually agreed between GSA and contractor</li> </ul>

Media type changes per section C.3.1.2

#### C.3.9.4.1.3.4 Content – OSS Change Management Plan

As defined in the OSS Change Control document described in Section C.3.2.2.1.4 Contractor Policies and Procedures.

#### C.3.9.4.2 Contractor Reports Provided to Agency

As required by approved Networkx Services Verification Test Plan, which includes the approved Acceptance Test Plan.

#### C.3.9.5 Operational Support Systems Security Requirements

The contractor will comply with the security requirements (directives, standards, policies, reporting requirements, guides, laws and regulations) referenced in each subsection of Section C.3.9, as they apply to the Networkx OSS defined boundary in Section C.3.9.

#### C.3.9.5.1 Security Assessment and Authorization (formerly known as Certification and Accreditation [C&A]) Requirements

In providing services under the Networkx Contract, the Contractor will be subject to all federal and GSA IT security directives, standards, policies, and reporting requirements. The contractor will comply with Federal Information Security Management Act

associated guidance and directives to include all applicable Federal Information Processing Standards (FIPS), NIST Special Publication (SP) 800 series guidelines (FIPS and NIST SPs available at: <http://csrc.nist.gov/>), GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of Government IT. Compliance references will include:

- Federal Information Security Management Act (FISMA) of 2002; available at: <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996"; available at: [http://www.cio.gov/Documents/it\\_management\\_reform\\_act\\_feb\\_1996.html](http://www.cio.gov/Documents/it_management_reform_act_feb_1996.html).
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors", August 27, 2004; available at: <http://www.idmanagement.gov/>.
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", and Appendix III, "Security of Federal Automated Information Systems", as amended; available at: [http://www.whitehouse.gov/omb/circulars\\_a130\\_a130trans4/](http://www.whitehouse.gov/omb/circulars_a130_a130trans4/).
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." (Available at: [http://www.whitehouse.gov/omb/memoranda\\_2004](http://www.whitehouse.gov/omb/memoranda_2004)).
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems."
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems."
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."
- NIST Special Publication 800-18 Rev 1, "Guide for Developing Security Plans for Federal Information Systems."
- NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."
- NIST Special Publication 800-34 Revision 1, "Contingency Planning Guide for Information Technology Systems."
- NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."
- NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems."
- NIST Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations."
- NIST Special Publication 800-53A, Revision 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans."
- NIST Special Publication 800-88, "Guidelines for Media Sanitization"
- NIST Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems."
-

In addition to complying with the requirements identified in the Government policies, directives and guides specified above, the contractor will comply with the current GSA policies, directives and guides listed below (the current documents are referenced within the GSA IT Security Policy and are available upon request submitted to the GSA CO):

- GSA Information Technology (IT) Security Policy, CIO P 2100.1( )
- GSA Order CIO P 2181.1 "GSA HSPD-12 Personal Identity Verification and Credentialing Handbook" GSA Order CIO 2104.1, "GSA Information Technology (IT) General Rules of Behavior"
- GSA Order CPO 1878.1, "GSA Privacy Act Program"
- GSA IT Security Procedural Guide 01-01, "Identification and Authentication"
- GSA IT Security Procedural Guide 01-02, "Incident Response"
- GSA IT Security Procedural Guide 01-05, "Configuration Management"
- GSA IT Security Procedural Guide 01-07, "Access Control"
- GSA IT Security Procedural Guide 01-08, "Audit and Monitoring"
- GSA IT Security Procedural Guide 04-26, "FISMA Implementation"
- GSA IT Security Procedural Guide 05-29, "IT Security Training and Awareness Program"
- GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing"
- GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk"
- GSA IT Security Procedural Guide 06-32, "Media Protection Guide"
- GSA IT Security Procedural Guide 07-35, "Web Application Security Guide"
- GSA IT Security Procedural Guide 08-39, "FY 2011 IT Security Program Management Implementation Plan"
- GSA IT Security Procedural Guide 08-43, "Key Management Guide"
- GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)"
- GSA IT Security Procedural Guide 10-50, "Maintenance Guide"
- GSA IT Security Procedural Guide 11-51, "Conducting Penetration Test Exercise Guide"

#### C.3.9.5.2 GSA Security Compliance Requirements

FIPS 200, “*Minimum Security Requirements for Federal Information and Information Systems*”, is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in eighteen security-related areas. Contractor systems supporting GSA must meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 3 (hereafter described as NIST 800-53) “*Recommended Security Controls for Federal Information Systems*.”

To comply with the federal standard, GSA has determined the security category of the information and information system in accordance with FIPS 199, “*Standards for Security Categorization of Federal Information and Information Systems*”, to be established at the Moderate Impact Level and baseline security controls must be established as identified in NIST 800-53 and other associated directives and guides identified and/or provided by GSA. All deliverables identified in this section are an attachment or appendix to the Security Plan (commonly known as the System Security Plan [SSP]).

#### C.3.9.5.3 Security Assessment and Authorization (formerly known as Certification and Accreditation)

The implementation of a new federal government IT system requires a formal approval process known as Assessment and Authorization. NIST Special Publication 800-37, Revision 1 (hereafter listed as NIST 800-37) and GSA IT Security Procedural Guide 06-30, “*Managing Enterprise Risk*”, provides guidance for performing the security assessment and authorization process. The contractor’s system must have a valid assessment and authorization (approved by GSA) prior to being placed into operation and processing government information. Failure to obtain and maintain a valid assessment and authorization will be grounds for termination of the contract. The system must have a new security assessment and authorization conducted (and approved by GSA) at least every three (3) years or at the discretion of the Authorizing Official (AO) when there is a significant change to the system’s security posture. All NIST 800-53 controls must be tested and assessed no less than every 3 years unless otherwise determined by the AO.

#### C.3.9.5.4 Step 1 -- Security Plan (hereafter referred to as the System Security Plan [SSP])

ID Number	Description
1	The Contractor shall comply with all security assessment and authorization requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security assessment and authorization is based on the System’s NIST FIPS Publication 199 categorization. At a minimum, the contractor shall create, maintain and update the following security assessment and authorization documentation:
2	The Security Plan will be completed in accordance with NIST Special Publication 800-18, Revision 1 (hereafter listed as NIST SP 800-18 R1) and other relevant guidelines. The



**GS00T07NSD0038**  
**Modification No. PS661**

ID Number	Description
	SSP shall also include, at a minimum, the following appendices consisting of required policies and procedures across 18 control families mandated per FIPS 200.
3	The Contractor shall develop and maintain a Security Accreditation Boundary Scope Document (BSD) Update as identified in NIST 800-37, Rev 1. A template will be provided upon request submitted to the GSA CO.
4	The Contractor shall develop and maintain Interconnection Agreements developed in accordance with NIST Special Publication 800-47.
5	The Contractor shall develop and maintain a GSA NIST 800-53 R3 Control Tailoring Worksheet as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk". A template will be provided upon request submitted to the GSA CO. Column E of the worksheet titled "Contractor Implemented Settings" shall document all contractor implemented settings that are <u>different</u> from the GSA defined settings and where the GSA defined setting allows a contractor to deviate.
6	The Contractor shall develop and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk". A template will be provided upon request submitted to the GSA CO.
7	The Contractor shall develop and maintain a Rules of Behavior for information system users as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk" and GSA Order CIO 2104.1, "GSA IT General Rules of Behavior".
8	The Contractor shall develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk".
9	The Contractor shall develop and maintain a Contingency Plan (including Disaster Recovery Plan and Business Impact Assessment) completed in agreement with NIST Special Publication 800-34.
10	The Contractor shall develop and maintain a Contingency Plan Test Plan and Report completed in agreement with GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing."
11	The Contractor shall perform a Privacy Impact Assessment completed as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk".
12	The Contractor shall develop and maintain a Plan of Action and Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)." The applicable NIST SP 800-53 Rev 3 is Control CA-5.
13	All FIPS 199 Low, Moderate and High impact information systems must complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. GSA will provide for the scheduling and performance of these penetration tests. All penetration test exercises must be coordinated through the GSA Office of the Senior Agency Information Security Officer (OSAIISO) at itsecurity@gsa.gov per the GSA IT Security. Applicable NIST SP 800-53 R3 Controls are CA-7 and RA-5.
14	All FIPS 199 Low, Moderate, and High impact information systems are encouraged (not a requirement) by GSA OSAISO to conduct a code analysis using tools to examine the software for common flaws and document results in a Code Review Report.
15	The government will be responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk."
16	The Contractor shall develop and maintain a System(s) Baseline Configuration Standard Document Reference: NIST 800-53 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05 The Contractor shall provide a well defined, documented, and up-to-date specification to

ID Number	Description
	which the information system is built.
17	<p>The Contractor shall develop and maintain System Configuration Settings Reference: NIST 800-53 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05</p> <p>The Contractor shall establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements.</p> <p>Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical, NIST guidelines, CIS guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the AO. System configuration settings will be updated or reviewed on an annual basis.</p>
18	<p>The Contractor shall develop and maintain a Configuration Management Plan Reference: NIST 800-53 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05</p> <p>The Contractor shall provide an initial Configuration Management Plan for the information system to include annual updates.</p>
19	<p>The government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test. The Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct security assessment and authorization activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, "<i>Managing Enterprise Risk</i>". Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Government information. This includes the general support system infrastructure.</p>
20	<p>All identified gaps between required 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked by the contractor for mitigation in a POA&amp;M document completed in accordance with GSA IT Security Procedural Guide 09-44, "<i>Plan of Action and Milestones (POA&amp;M)</i>." Depending on the severity of the gaps, the government may require them to be remediated before an Authorization to Operate (ATO) is issued.</p>
21	<p>The Contractor is responsible for mitigating all security risks found during the security assessment and authorization and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The government will determine the risk rating of vulnerabilities.</p>
22	<p>Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the Contractor's system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables shall be updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.</p>
23	<p>The Contractor shall deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "<i>FISMA Implementation</i>". Each fiscal year the annual assessment will be completed in accordance with instructions provided by GSA.</p>

**C.3.9.5.5 Step 2 -- Security Plan Contract Deliverables**

ID Number	Description
1	<p>Deliverables to be provided to the GSA COTR/ISSO/ISSM on a Quarterly basis:</p> <ol style="list-style-type: none"> <li>1. Plan of Action &amp; Milestones (POA&amp;M) Updates (Monthly updates/reviews are required for any vulnerabilities identified as a high or critical). (NIST SP 800-53 R3; CA-5)</li> <li>2. Vulnerability scanning reports for Operating System, Web Application, and Database scans (as applicable). (NIST SP 800-53 R3; RA-5)</li> </ol> <p>Note: Vulnerability scanning results shall be managed and mitigated in the POA&amp;M and submitted together with the quarterly POA&amp;M submission. (NIST SP 800-53 R3; PM-4 and GSA CIO-IT Security Guide 09-44 R1)</p>
2	<p>Deliverables to be provided to the GSA COTR/ISSO/ISSM initially and as updates (if required) on an Annual basis:</p> <ol style="list-style-type: none"> <li>1. System Security Plan (NIST SP 800-53 R3: PL-2)</li> <li>2. Security Accreditation Boundary Document (BSD) (NIST SP 800-37 R1)</li> <li>3. User Certification/Authorization Review (Annotated on POA&amp;M) (NIST SP 800-53 R3: AC-2)</li> <li>4. Information Security Awareness and Training (NIST SP 800-53 R3: AT-1)</li> <li>5. System(s) Baseline Configuration Standard Document (NIST SP 800-53 R3: CM-2)</li> <li>6. System Configuration Settings (NIST SP 800-53 R3: CM-6)</li> <li>7. Contingency Plan (NIST SP 800-53 R3: CP -2)</li> <li>8. Configuration Management Plan (NIST SP 800-53 R3: CM-9)</li> <li>9. Contingency Plan Test Plan (NIST SP 800-53 R3: CP-4)</li> <li>10. Contingency Plan Test Report (NIST SP 800-53 R3: CP-4)</li> <li>11. Incident Response Test Report (NIST SP 800-53 R3: IR-3)</li> <li>12. Information System Interconnection Agreements (NIST SP 800-53 R3: CA-3)</li> <li>13. Rules of Behavior (NIST SP 800-53 R3: PL-4)</li> <li>14. GSA NIST 800-53 R3 Control Tailoring Worksheet (NIST SP 800-53 R3: AC-1)</li> <li>15. GSA NIST SP 800-53 rev3 Baseline Summary of Controls Table (NIST SP 800-53 R3: AC-1)</li> <li>16. Independent penetration test and report (NIST SP 800-53 R3: CA-7 &amp;RA-5)</li> <li>17. Annual FISMA Assessment (NIST SP 800-53 R3: CA-2)</li> </ol>
3	<p>Deliverables to be provided to the GSA COTR/ISSO/ISSM Biennially:</p> <p>The Contractor shall develop and keep current the deliverables listed below, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides. The GSA Control Tailoring Worksheet shall be used by the contractor to meet the deliverable requirements listed below. A template for the GSA NIST 800-53 R3 Control Tailoring Worksheet will be provided upon request submitted to the GSA CO and shall be used as a guide to maintain update requirements.</p> <ol style="list-style-type: none"> <li>1. Access Control Policy and Procedures (NIST SP 800-53 R3: AC-1)</li> <li>2. Security Awareness and Training Policy and Procedures (NIST SP 800-53 R3: AT-1)</li> <li>3. Audit and Accountability Policy and Procedures (NIST 800-53 R3: AU-1)</li> <li>4. Identification and Authentication Policy and Procedures (NIST SP 800-53 R3: IA-1)</li> <li>5. Incident Response Policy and Procedures (NIST SP 800-53 R3: IR-1, reporting timeframes are documented in GSA CIO IT Security Procedural Guide 01-02, Incident Handling)</li> <li>6. System Maintenance Policy and Procedures (NIST SP 800-53 R3: MA-1)</li> <li>7. Media Protection Policy and Procedures (NIST SP 800-53 R3: MP-1)</li> <li>8. Physical and Environmental Policy and Procedures (NIST SP 800-53 R3: PE-1)</li> <li>9. Personnel Security Policy and Procedures (NIST SP 800-53 R3: PS-1)</li> <li>10. System and Information Integrity Policy and Procedures (NIST SP 800-53 R3: SI-1)</li> <li>11. System and Communication Protection Policy and Procedures (NIST SP 800-53 R3: SC-1)</li> </ol>

ID Number	Description
	12. Key Management Policy (NIST SP 800-53 R3: SC-12)

### C.3.9.5.6 Step 3 -- Additional Security Requirements

ID Number	Description
1	The Contractor shall ensure that proper privacy and security safeguards are adhered to in accordance with the FAR Part 52.239-1, see Section I.
2	The deliverables identified in Section C.3.9.5.5 shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or Contractor selected designation per document sensitivity. External transmission/dissemination of For Official Use Only (FOUO) and CUI data to or from a GSA computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."
3	Where appropriate, the contractor shall ensure implementation of the requirements identified in the FAR (see Section I, 52.224-1, "Privacy Act Notification" and FAR 52.224-2, "Privacy Act."
4	The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government's agent.
5	<p>The government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the Contractor shall be responsible for the following privacy and security safeguards:</p> <ol style="list-style-type: none"> <li>The Contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this task order or otherwise provided by the government. <i>Exception - Disclosure to a Consumer Agency for purposes of security assessment and authorization verification.</i></li> <li>To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by the Contractor, the Contractor shall afford the government logical and physical access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods: <ul style="list-style-type: none"> <li>Authenticated and unauthenticated operating system/network vulnerability scans.</li> <li>Authenticated and unauthenticated web application vulnerability scans.</li> <li>Authenticated and unauthenticated database application vulnerability scans.</li> </ul> </li> <li>Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may, at the government's discretion, be accepted in lieu of government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the government. In addition, the results of vendor-conducted scans shall be provided, in full, to the government.</li> </ol>

### C.3.9.5.7 Step 4 -- Personnel Security / Suitability

ID Number	Description
1	The contractor shall perform personnel security / suitability in accordance with the FAR Part 52.204-9, see Section I.

ID Number	Description
2	The Contractor will comply with agency personal identity procedures identified in the contract that implements Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.
3	The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.
4	GSA credentials will only be required for contractor personnel who must have access to GSA facilities on a daily basis and / or access to GSA's network systems to assist in the performance of their work.

### C.3.9.5.8 Step 5 – Personnel Background Investigation Requirements

The contractor will require access to Government information and/or access to Government contracted systems. For the purpose of this Section C.3.9.5.8, "Government Information" is defined as information provided by Government Clients pursuant to their use of the contractor's Operational Support Systems (OSS) as defined in the System Security Plan (SSP) that is within the Security Assessment and Authorization scope. All contractor personnel with access to the contractor's OSS as defined in the System Security Plan (SSP) that is within the Security Assessment and Authorization scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, M-11-11 and as specified in GSA CIO Order 2100.1I and GSA Directive 9732.1D Suitability and Personnel Security for background investigations to provide services under this contract. These background investigations will be funded and processed by GSA. The respective Networx CO/COR/Program Management staff will initiate and coordinate the appropriate background investigation process.

## C.4 Transition

### C.4.1 Transition Process Definition

Transition is the process for the coordinated transfer of service from a specified GSA FTS incumbent contractor, such as FTS2001, Crossover, and FTS satellite service and wireless contracts, to a Networx contract.

### **C.4.1.1 Transition Process Description**

#### **C.4.1.1.1 Transition Project Management**

Transition project management is the planning, staffing, executing and controlling of all aspects of transition activity to achieve the Government's objectives. The requirements of Section C.3.2, (Program Management) apply to all transition activities. Certain transitioning services, or groups of services, as specified by the Government, will receive special project management attention, based on their size, complexity, importance, or mission criticality. These services or groups of services will be managed together and be designated by the Government as "Transition Projects."

Transition Project Specific Plans (see Section C.4.3.3.3) will be required only for the transition of services that comprise a Transition Project.

#### **C.4.1.1.2 Government Role in Transition**

GSA will oversee all Contractor Networkx transition activities to ensure that Agencies receive the services that they have ordered and to assist Agencies with Networkx transition activities as resources permit. The functions to be performed by GSA include the following:

- (a) Monitor contractor's transition project management performance and initiate corrective action if required
- (b) When requested by the Agency, assist with Networkx transition activities as resources permit
- (c) Monitor and facilitate coordination between the contractor, Agencies, and other GSA FTS contractors
- (d) Assist the Agencies in resolving any conflicts with the contractor and other GSA FTS contractors.

The Agency will monitor and control all Agency ordered Networkx transition activities to ensure that it receives the services that it has ordered. The functions to be performed by the Agency regarding transition activities for services ordered include the following:

- 1. Exercise project management responsibility for Agency transition actions
- 2. Monitor Contractor's transition project management performance and coordinate corrective actions with GSA if required
- 3. Monitor and facilitate coordination between the contractor and local Government contacts (LGCs) and other Agency service providers
- 4. Assist the contractor in resolving any conflicts with LGCs and other Agency service providers

Other transition-related functions to be performed by the Government are identified in various C.4.2 sections below.

Many Government organizations are decentralized, so multiple entities within a Department or an independent Agency may perform the functions of an "Agency." The

Agency's responsibilities and functions may be delegated to another Agency, to a Sub-Agency or an Agency component, or to a contractor authorized to act on behalf of the Agency. The LGC identified by the Agency will serve as the Government's point of contact for any site-specific planning and coordination activities. An LGC may or may not actually be located at the location(s) acquiring service from the contractor. The LGCs will:

- a. Assist the contractor by providing available telecommunications information about the site and providing other assistance required, such as obtaining building and room access
- b. Assist the contractor in coordinating with other Agency service providers (e.g., private branch exchange (PBX), network management, information system)
- c. Upon notification by the contractor of changes regarding the date of scheduled activities or site requirements, coordinate with users and with other contractor(s) who are providing that location with telephone switching or other telecommunications facilities

#### **C.4.1.1.3 Transition Planning**

Project management of Network transition activities will be based on Government-approved contractor-provided plans. The following plans must be provided by the contractor:

- (a) The Transition Management Plan (TMP). This plan describes the contractor's proposed general approach to the project management of transition, including the contractor's project management process, procedures, and tools for all Network transition activities. The TMP is a Government-wide plan applicable to all transition activities for all Agencies.
- (b) An Agency-Level Transition Plan (ALTP). When required by the Agency, this plan identifies the project management process, procedures, and tools for a set of Network transition activities in support of that Agency.
- (c) A Transition Project Specific Plan (TPSP). This plan identifies the project management process, procedures, and tools for a Transition Project. For a Transition Project, a TPSP is used rather than a Service Delivery Project Plan (SDPP) as cited in Section C.3.2, Program Management.

**C.4.1.1.4 Transition Inventory**

A Transition Inventory is a complete description of the services, equipment, location data and environmental data necessary to facilitate the transition of an Agency's services. The Transition Inventory is also required to support transition status tracking and reporting.

**C.4.1.1.5 Transition Orders**

Transition Orders are orders placed by an Agency to obtain Network services intended to replace services provided by an incumbent contractor and contain additional information to facilitate transition.

Transition Orders will be created and processed in accordance with Section C.3.5.1, Direct Ordering.

**C.4.1.1.6 Transition Notices**

Transition Notices provided by the contractor keep the Government informed of the status of transition activities. Transition Notices will be sent by the contractor to GSA, to Agencies, to LGCs, and to incumbent contractors. There are two types of Transition Notices:

- (a) The Transition Action Notice. This notice alerts all concerned of projected and planned future transition activities including any changes in earlier schedules and advises recipients of actions required to complete transition.
- (b) The GO/NO GO Transition Notice. This notice alerts recipients to the status of imminent transition cutovers or other significant activities. The GO/NO GO Transition Notice indicates whether the status of a scheduled transition activity is "GO", that is, all (including coordinated actions with the incumbent contractor and the LGC or site contacts) is in readiness and that the activity will proceed as scheduled or "NO GO", that is, activity will not proceed as scheduled.

**C.4.1.1.7 Transition Execution**

Transition Execution involves the actions required to complete the ordered transition activity including coordination with the incumbent contractor, conducting the cutover of service, conducting verification testing of the delivered services and acceptance of the service by the Government.

Transition Execution also includes the placement of an order to disconnect the service being replaced by the Agency with the incumbent contractor.

**C.4.1.2 Transition Process Steps**

The Transition Process consists of the nine steps in the following table. The functional requirements are organized around these steps in Section C.4.2, Transition Functional Requirements.



Step Number	Description	Executing Entities
•	Initiate transition planning upon Notice to Proceed	GSA Contractor Agency
•	Create the Transition Management Plan (TMP).	Contractor
•	Create the Agency Level Transition Plan (ALTP).	Contractor
•	Create the Transition Project Specific Plan (TPSP) (When required).	Contractor
•	Create a Transition Inventory of existing services.	GSA Agency Contractor
•	Process Transition Orders.	Agency Contractor
•	Notify GSA and Agency of transition activities.	Contractor
•	Execute transition.	GSA Agency Contractor
•	Report on planning and progress of transition.	Contractor

**C.4.2 Transition Functional Requirements**

**C.4.2.1 Step 1 – Initiate Transition Planning**

With respect to transition planning, the functions to be performed by GSA include the following:

- Provide comments for development of the Contractor's Transition Management Plan (TMP)
- Review and approve or reject the Contractor's TMP and any changes to it
- Assist with the Agency review of Transition Project Specific Plans (TPSPs) and ALTPs when requested by the Agency

The functions to be performed by the Agency regarding transition planning for services ordered include the following:

- Designate those activities that will be managed as Transition Projects
- Review and approve or reject the contractor's Agency Level Transition Plans (ALTPs) and TPSPs, and any changes to them
- Assist the contractor by providing available telecommunications information about Agency requirements
- Assist the contractor in coordinating with other Agency service providers (e.g., PBX, network management, information system)

The following table lists the contractor’s requirements for initiating Transition planning:

ID Number	Description
1	The contractor shall comply with the provisions of Section C.4, Transition in its entirety with regard to planning, notifying the Government, executing, and reporting to the Government all transition activities.
2	The contractor shall designate a person of sufficient authority and project management experience within its Contractor Program Organization (CPO) to have overall responsibility for all Networkx transition project management activities.
3	The contractor shall provide management, planning, and field personnel sufficient in number and qualifications to ensure that transition activities are completed as ordered.
4	The contractor shall coordinate and exchange information on transition activities as required by this contract with GSA and the Agencies, bearing in mind that since many Government organizations are decentralized, multiple entities within a Department or an independent Agency may perform the responsibilities of an “Agency.”
5	The contractor shall have support systems in place according to Sections C.3.9, Operational Support Systems, and E.3, Verification Testing of Contractor’s Operational Support System before issuing a Service Order Confirmation or proceeding with any transition orders.

**C.4.2.2 Step 2 – Create Transition Management Plan (TMP)**

ID Number	Description
(a)	The contractor shall develop and provide a Transition Management Plan (TMP) that shall include the project management of all transition activities for all services, provisioned and non-provisioned, provided by the contractor.
(b)	The contractor shall develop and provide at no cost to the Government, the TMP in accordance with the data and media requirements in Section C.4.4.2.1, Transition Management Plan (TMP) within 30 calendar days of notice to proceed. GSA, in coordination with the Agencies, will review the contractor’s TMP within 15 calendar days after its submission and provide comments to the contractor.
(c)	The contractor shall base the TMP on the information contained in the contractor’s Preliminary Transition Management Plan (PTMP) included at contract award, Government comments, the requirements of this Contract for transition activities, and the contractor’s normal business practices.
(d)	The contractor shall submit a revised TMP for approval within 15 calendar days after receiving the review from GSA.
(e)	The contractor shall neither issue a Service Order Confirmation for nor proceed with any orders for transition until the TMP has been approved. The Government may consider the contractor’s PTMP and/or TMP when making Fair Opportunity decisions.
(f)	The contractor shall update the TMP to address new or enhanced service types as they are introduced or as significant changes become necessary in the overall approach to transition.
(g)	The contractor shall identify any special technical requirements such as those described in the narrative below this table.

Special technical requirements may exist such as those in the areas of Direct Station-to-Station Dialing and Private Dialing Plans that must be met during all periods that transition activities are ongoing and therefore need to be addressed in all planning. The following are examples that may apply to voice services:

**Direct Station-to-Station Dialing**

During periods that transition activities are ongoing, the contractor must maintain the ability for any Networkx Circuit Switched Data Service/ Voice Service (CSDS/VS) user to directly dial any other CSDS/VS user who uses a 10-digit number following the North American Number Plan (NANP). Similarly, during periods that transition activities are ongoing, the contractor must maintain the ability for any Networkx CSDS/VS user who uses a 10-digit number following the North American Number Plan (NANP) to receive calls from any other 10-digit number CSDS/VS NANP user. Additionally, during periods that transition activities are ongoing, the contractor shall maintain the ability for any Networkx CSDS/VS user to directly dial and to receive calls from international CSDS/VS user provided that appropriate international access and country codes are used.

**Private Dialing Plans**

Whenever a private number dialing arrangement is ordered by the Government, the contractor must develop and provide as part of the TPSP, a private dialing plan for stations that require contractor-specific private numbers. The Government understands that number portability cannot be guaranteed when transitioning or migrating private number dialing arrangements.

**C.4.2.3 Step 3 – Create Agency-Level Transition Plan (ALTP)**

ID Number	Description
1	When requested by an Agency, the contractor shall develop and provide an Agency-Level Transition Plan (ALTP) that shall include the project management of all transition activities pertinent to a particular Agency for all Transition Orders the Agency has placed with the contractor.
2	The contractor shall develop and provide, at no cost to the Government, the ALTP in accordance with the data and media requirements in C. 4.4.3.1, Agency-Level Transition Plan within 45 calendar days of the request by the Agency. The Agency will provide comments to the contractor within 15 calendar of the submission by the contractor.
3	The contractor shall submit a revised ALTP for approval within 15 calendar days after receiving the comments from the Agency.
4	The contractor shall base the ALTP on the information contained in the contractor's Transition Management Plan (TMP), other requirements of this Contract, the Agency's specific requirements, and the contractor's normal business practices.
5	The contractor shall describe plans to meet special technical requirements such as <ul style="list-style-type: none"> <li>a. direct station-to-station dialing</li> <li>b. private dialing plans</li> </ul>

**C.4.2.4 Step 4 – Create Transition Project Specific Plans (TPSP)**

ID Number	Description
1	The contractor shall develop and provide, at no cost to the Government, a Transition Project Specific Plan (TPSP) for all transition activities that are required by an Agency to be managed as a Transition Project unless the TPSP requirement is waived or changed by the Agency in writing. The Government will normally designate transition activities deemed as mission-critical by the Agency as a Transition Project.
2	The contractor shall include in all TPSPs all of the information identified in Section

ID Number	Description
	C.4.4.3.2., Transition Project Specific Plan.
3	The contractor shall complete transition projects by the baseline completion dates of the TPSP mutually agreed upon with the Agency at the time orders are placed and acknowledged by the contractor. The baseline dates will be the Firm Order Commitment dates for each order within the project, which shall meet the provisioning objectives in Attachment J.12.3, Service Provisioning Intervals, for routine or Class B expedited orders unless the Agency otherwise agrees to different intervals (see Section C.3.5.1, Direct Ordering).
4	The contractor shall submit the TPSP to the Agency no later than 30 calendar days prior to the Customer Want Date (see Section C.3.5.1, Direct Ordering).
5	The contractor shall describe plans to meet special technical requirements such as <ul style="list-style-type: none"> <li>a. direct station-to-station dialing</li> <li>b. private dialing plans</li> </ul>

**C.4.2.5 Step 5 – Create Transition Inventory**

The Agency will compile its own Transition Inventory of the incumbent contractor's provided services. GSA will share with the Agency any available information on the incumbent contractor's services being provided to the Agency. GSA will assist the Agency in obtaining information on the incumbent contractor's services being provided to the Agency from the incumbent contractor. Upon request of the contractor, the Agency will share with the contractor all available information on the incumbent contractor's services being provided to the Agency that are to be transitioned to the contractor's services including any service location changes.

ID Number	Description
a.	Beginning with the information provided by the Agency, the contractor shall compile and maintain a Transition Inventory of all incumbent contractors' services by location, including those for which the contractor is also the incumbent, that are to be transitioned to the contractor's services.
b.	In those cases in which the contractor is also the incumbent, the contractor shall compile and maintain the portion of the Transition Inventory pertaining to the services being provided as an incumbent at no charge to the Government.
c.	Further, in those cases in which the contractor is also the incumbent, the contractor shall share the portion of the Transition Inventory pertaining to the services being provided as an incumbent with GSA and to the served Agency when requested at no charge to the Government in accordance with Section C.4.3.3.1, Transition Inventory Data.
d.	The contractor shall obtain from the order, supplemented by other Government sources, or by means of a site visit all information on incumbent telecommunications services needed to transition services whether or not that information is specified as a Transition Inventory data element in Section C.4.3.3.1, Transition Inventory Data.
e.	The contractor shall include in the Transition Inventory all information needed to complete the transition activity including, as a minimum, the elements identified in Section C.4.3.3.1, Transition Inventory Data.

**C.4.2.6 Step 6 – Process Transition Orders**

The functions to be performed by the Agency regarding Transition Orders include the following:

- 1 Submit Transition Orders identified as such in accordance with C.3.5.1, Direct Ordering
- 2 Provide information on incumbent services being transitioned
- 3 Designate those activities that will be managed as Transition Projects
- 4 Identify the Agency’s LGC for each location involved in a particular project or other activity in the order, if possible
- 5 Provide authorization as needed to allow access providers to accept Primary Interexchange Carrier (PIC) orders from the contractor
- 6 Place orders with incumbent contractors to disconnect services that are transitioned.

ID Number	Description
1	The contractor shall accept and process orders for transition in accordance with Section C.3.5.1, Direct Ordering.
2	The contractor shall accept and maintain the transition data elements as specified in Section C.4.3.2, Agency Data Provided to contractors.
3	The contractor shall identify within seven (7) calendar days of issuing an Order Receipt Acknowledgement (see Section C.3.5.1, Direct Ordering) the specific individual who has primary and direct responsibility for the project management of the activities required to complete that order and authority to serve as a single point of contact to the Government for the completion of the order.
4	The contractor shall coordinate all information-gathering needed to complete ordered activities with Agencies, Agency components, or other Agency service providers identified by the Agency.
5	The contractor shall coordinate traffic routing and management at user locations.
6	The contractor shall coordinate all desired on-site visits to user locations needed to complete ordered activities with Agencies or Agency components, LGCs, and other Agency service providers identified by the Agency. Site visits shall be at no charge to the Government.
7	Where switched access is used, contractor shall place PIC orders with the access service provider and report the access status in the Weekly Transition Planning Report to GSA and the Agencies as specified in Section C.4.4.1.1, Weekly Transition Planning Report.

**C.4.2.7 Step 7 – Notify GSA and Agency of Transition activities.**

Transition Notices will be used by the contractor to keep the Government and incumbent contractors informed of projected, planned and pending transition activities.

The GSA will use Notices to monitor and oversee transition activity. The GSA will help resolve conflicts in scheduling between the Agency and the contractor revealed by the Notices.

The Agency will use the Notices to monitor and oversee transition activity and to schedule their activities associated with the transition. This includes notifying the users

of the maintenance window, configuring Government Furnished Property (GFP) for the new service, supporting the transition to the ordered service, and preparing to start the Agency acceptance process.

The Notices are a key element in the required coordination between the contractor and the incumbent contractor.

ID Number	Description
•	The contractor shall ascertain the readiness of all involved parties and include that information in all Transition Notices.
•	The contractor shall distribute required Transition Notices as follows: <ul style="list-style-type: none"> <li>• GSA shall be a required recipient on all Transition Notices</li> <li>• The notices distributed to each incumbent contractor will address only the transition activity related to the incumbent contractor's services.</li> <li>• The notices distributed to each Agency will address only the transition activity related to the services used by that Agency.</li> <li>• The notices distributed to each LGC will address only the transition activity with which the LGC is concerned.</li> </ul>
•	For each <u>future</u> scheduled transition event (or project, if requested by the Agency), the contractor shall provide 60-days prior to the event a Transition Action Notice to alert GSA, the Agency, the LGC and the incumbent contractor of projected and planned future transition activities including any changes in earlier schedules, and to advise recipients of actions required to complete transition.
•	If any of the information in the Transition Action Notice changes, the contractor shall provide an update to GSA, the Agency, the LGC, and the incumbent contractor within a week of becoming aware of the change.
•	For each <u>imminent</u> scheduled transition event (or project, if requested by the Agency), the contractor shall provide a GO/NO GO Transition Notice to GSA, the Agency, the LGC and the incumbent contractor not less than 24 hours before each scheduled cutover or other significant transition activity indicating whether the status is "GO", that is, all is in readiness and activity will proceed as scheduled or "NO GO", that is, activity will not proceed as scheduled.
•	The contractor shall provide a NO GO Transition Notice to GSA, the Agency, the LGC and the incumbent contractor as soon as possible after becoming aware that the activity will not proceed as scheduled.
•	If any of the information in a GO/NO GO Transition Notice changes, particularly status, the contractor shall provide an update to GSA, the Agency, the LGC, and the incumbent contractor by phone or email as soon as possible.
•	The contractor shall provide Notices in the media and with the contents specified for each type of notice as specified in Section C.4.3.4.1., Transition Action Notice and Section C.4.3.4.2, GO/NO GO Transition Notice.

**C.4.2.8 Step 8 – Execute Transition**

The Agency will monitor and control all Agency ordered Network transition activities to ensure that it receives the services that it has ordered. The functions to be performed by the Agency regarding transition execution include the following:

- Exercise project management responsibility for Agency transition actions

- Monitor contractor’s transition project management performance and coordinate corrective actions with GSA if required
- Monitor and facilitate coordination between the contractor and LGCs and other Agency service providers
- Assist the contractor in resolving any conflicts with LGCs and other Agency service providers, including the incumbent contractor
- As necessary, direct the activities of the incumbent contractor and other Agency contractor
- Accept or reject services in accordance with Section E, Inspection and Acceptance.

ID Number	Description
1	The contractor shall coordinate and manage workflow between elements of the contractor’s organization, subcontractors, and access providers as needed to complete transition activities within the required service provisioning intervals.
2	The contractor shall designate a representative for each location where ordered activities are to occur and ensure that this representative be available to communicate with the Agency’s LGC prior to, during, and immediately following these activities to answer any questions related to the transition activities at the location(s) for which the contractor’s designated site representative is responsible. Contractor’s designated site representative is not required to be on-site.
3	The contractor shall coordinate transition activities with the incumbent contractor to minimize any disruptions of service.
4	The contractor shall coordinate traffic routing and management at user locations.
5	The contractor shall coordinate with the LGC and other Agency service providers (e.g., PBX, network management, information system) as needed to complete transition activities including ordering of access.
6	Except for projects with an approved TPSP, the contractor shall follow the approved TMP and ALTP procedures and meet the requirements of Section C.3.5.1, Direct Ordering when conducting transition activities, unless otherwise arranged with, or requested by, the Agency in writing.
7	In those cases where a TPSP has been approved for a specific project, the contractor shall follow the approved TPSP procedures when conducting transition activities for that project.
8	The contractor shall ensure adequate management and planning staffs and the field personnel staffs are on-hand as needed to complete transition activities.
9	When ordered by the Government, the contractor shall work with the incumbent contractor to establish gateways or other interconnections between the contractor’s network and the incumbent’s network so that calls (e.g., 700 number) may be completed across network boundaries in both directions until the last site is successfully transitioned.
10	The contractor shall complete any number conversions that are required to complete calls in either direction through gateways.
11	The contractor shall meet special technical requirements such as: <ul style="list-style-type: none"> <li>a. Direct Station-to-Station Dialing</li> <li>b. Private Dialing Plans.</li> </ul>
12	The contractor shall initiate and complete all transition activities outside of Agency’s normal office/business hours at the site, unless otherwise arranged with, or requested by, the user location’s LGC or other authorized Agency representative.

ID Number	Description
13	The contractor shall complete all transition activities at a location within 12 hours after initiation unless special approval is obtained in advance from the Agency.
14	The contractor shall update project management, Service Ordering, Inventory Management, and Billing support system databases as transition activities are completed.
15	During transition the contractor shall comply with the Service Level Agreements as specified in Attachment J.13, Service Level Agreements.
16	If the service does not pass the contractor's end-to-end verification testing as defined in Section E, Inspection and Acceptance, the contractor shall notify and advise the Agency of proposed corrective actions and the estimated time to complete them. If the Agency has already experienced two or more hours of downtime, it may request restoration of incumbent services. The contractor will then implement and follow processes and procedures to provide for complete restoration to the incumbent contractor's service within four hours.

**C.4.2.9 Step 9 – Report on Transition Planning and Execution**

Transition reports are required for the contractor to keep the Government informed of the planning and progress of transition execution. In addition to the transition reports, meetings with the contractor will be required to keep the Government informed of progress in completing transition activities.

ID Number	Description
1	The contractor shall provide the Government with reports of progress in transition execution as described in Sections C.4.3, Transition Data Requirements and C.4.4. Transition Report Requirements.
2	The contractor shall begin reporting on transition no later than one week following acknowledgement of its first Transition Order by providing GSA two transition reports: <ul style="list-style-type: none"> <li>• Weekly Transition Planning Report of transition planning and preparation</li> <li>• Weekly Transition Execution Report of progress in transition execution.</li> </ul>
3	The contractor shall deliver subsequent transition reports no later than the second Government business day following a weekly reporting period ending Sunday night,
4	Concurrent with the weekly reports to GSA, the contractor shall provide to each Agency the same information for only the Agency's locations and services, unless the Agency requests that transition reporting to it be discontinued or suspended. The suspension or discontinuance by one Agency/Sub-Agency shall not impact the provision and receipt of this report to other Agencies/Sub-Agencies or the contract requirement.
5	Additionally, the contractor shall comply with any reporting and requirements identified in an approved TPSP.
6	Representatives of the contractor shall meet with Government representatives when requested by GSA to report the contractor's progress in completing ordered transitions.
7	The contractor shall be responsible for coordinating all meetings requested by the Government and establishing an agenda if requested by the Government.

**C.4.3 Transition Data Requirements**

**C.4.3.1 GSA Data Provided to Contractors**

GSA will provide guidance to contractors regarding transition planning.



**C.4.3.2 Agency Data Provided to Contractors**

When requested by the contractor, the Agencies will share with the contractor all available information on the incumbent contractor’s services being provided to the Agency that the contractor’s services will replace. Refer to the Transition Inventory process requirements in Section C.4.2.5, Step 5—Create Transition Inventory. The media, transport mechanism, and format of the service inventory information will be determined at the time of the request and will be selected from one of the ways cited in the Data Table in Section C.3.1.2, Data and Report Requirements.

The Agency will provide supplemental transition information to the contractor in the transition type order. Orders for transition will contain the following information in Unit 4: Additional Instruction (See Attachment J.12.1, Table J.12.1-1, Ordering Data Elements):

Incumbent contractor
FTS2001 Agency hierarchy code (AHC)
FTS2001 SDP ID, if applicable
Service provided by incumbent contractor (SVS, DTS, etc.)
Details of service applicable to type of service being replaced e.g., circuit IDs, toll free number, toll free enhanced call routing (ECR) Application ID, calling card number and user name, audio conference calling account number, audio conference call authorization code, telephone numbers.
Government Equipment Connected to incumbent’s service
5. Type, make and model
6. Number, type and speed of ports
7. Incumbent contractor’s access information
8. Access service contractor(s)
9. Quantity, bandwidth and Commercial Circuit Numbers of access circuits if dedicated access is used
10. Incumbent contractor-provided equipment, if any, that each circuit (or each channel in a multiplexed circuit) is terminated in (e.g., data service unit, channel bank.)
11. Telephone numbers presubscribed to incumbent contractor if switched access is used.

**C.4.3.3 Contractor Data Provided to Government**

**C.4.3.3.1 Transition Inventory Data**

When the contractor is also the incumbent, it shall provide the portion of the Transition Inventory pertaining to the services being provided as an incumbent to GSA in accordance with the deliverable specifications that follow in this section. The information provided will be for all Agencies.

**C.4.3.3.1.1 Frequency – Transition Inventory Data Initial**

- (a) Initial: Within 90 calendar days of Notice to Proceed
- (b) Updates: Quarterly up to 8 quarter after Notice to Proceed

**C.4.3.3.1.2 Deliver To – Transition Inventory Data**

- a. GSA Transition Manager
- b. Agency Transition Manager

**C.4.3.3.1.3 Media/Transport/Format – Transition Inventory Data**

**C.4.3.3.1.3.1 Media/Transport/Format – Transition Inventory Data sent to GSA**

Data		
Media	Transport	Data Format
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.4.3.3.1.3.2 Media/Transport/Format – Transition Inventory Data sent to Agency**

The contractor shall provide and deliver the Transition Inventory Data to the Agency in accordance with the procedures and in any of the media, transport, and format types described in Section C.3.1.2, Data and Report Requirements.

**C.4.3.3.1.4 Record Elements -- Transition Inventory Data to GSA**

ID Number	Data Elements	Description
1	Incumbent Contractor	Name of Incumbent contractor
2	Date	Date of data transmission
3	Incumbent AHC	FTS 2001 Agency hierarchy code (AHC)
4	FTS2001 SDP	FTS2001 SDP ID, if applicable
5	Service	Service provided by incumbent contractor (SVS, DTS, etc.)
6	Service Details	Details of service applicable to type of service being replaced e.g., circuit IDs, toll free number, toll free ECR Application ID, calling card number and user name, audio conference calling account number, audio conference call authorization code, telephone numbers.
7	Access Contractor	Access service contractor
8	Access Details	Details of Access such as (a) quantity, bandwidth and Commercial Circuit Numbers of access circuits if dedicated access is used (b) Incumbent contractor-provided equipment, if any, that each circuit (or each channel in a multiplexed circuit) is terminated in (e.g., data service unit, channel bank (c) Telephone numbers presubscribed to incumbent contractor if switched access is used
9	Cross-Ref	Cross-references to the replacing service in the contractor's Service Ordering, Billing, and Inventory Management support

ID Number	Data Elements	Description
		systems if the incumbent is also replacing the service.

**C.4.3.4 Contractor Data Provided to Agency**

**C.4.3.4.1 Transition Action Notice**

The contractor shall provide Transition Action Notices in accordance with the deliverable specifications that follow in this section.

If the event for which the Transition Action Notice is being given is included in an approved TPSP plan, cross-references to the TPSP may be used for data elements which are addressed in the TPSP.

**C.4.3.4.1.1 Frequency – Transition Action Notice**

- 5. Initial: 60 calendar days prior to the transition event such as a service cutover
- 6. Updated: Within a week of becoming aware of a change in the transition activity or event.

**C.4.3.4.1.2 Deliver To – Transition Action Notice**

- 7. Agency Transition Manager
- 8. LGC

Provide a copy:

- 9. GSA Transition Manager
- 10. Incumbent contractor

**C.4.3.4.1.3 Media/Transport/Format – Transition Action Notice**

The contractor shall provide and deliver Transition Action Notices to the Agency Transition Managers, LGCs, and incumbent contractors in accordance with the procedures and in any of the media, transport, and format types described in the Data table in Section C.3.1.2, Data and Report Requirements.

The contractor shall provide and deliver Transition Action Notices to GSA in the following ways:

Data		
Media	Transport	Data Format
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> </ul>

Data		
Media	Transport	Data Format
Email Server	<ul style="list-style-type: none"> <li>Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>Encrypted Internet E-Mail</li> <li>Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>Other formats as mutually agreed between Agency and contractor</li> </ul>

#### C.4.3.4.1.4 Record Elements – Transition Action Notice

ID Number	Data Elements	Description
(a)	Title	Transition Action Notice
(b)	Contractor	Name
(c)	Agency	Name
(d)	LGC	Name and contact info
(e)	Date	Date of notice
(f)	ASRN	Agency Service Request Number
(g)	Service Order Number	contractor's tracking number for this order
(h)	Schedule Event Date	Scheduled date of event
(i)	Contractor's Local Representative	Name and commercial telephone number
(j)	Service Cross-Reference	Cross-references between new contractor service to the incumbent contractor's service that is being replaced
(k)	Access Requirements	Access circuits and facilities required at the location
(l)	Site Prep Requirements	Government site preparation requirements
(m)	Transition Activities	A transition activities list with dates and times for all contractor, including sub-contractors, activity, including but not limited to cabling, wiring, and the installation of contractor equipment, that will take place prior to the actual cutover of service(s). List of all activities that will require coordination with the incumbent contractor
(n)	LGC Assistance	Description of assistance required by the contractor from the LGC in order to complete transition activities
(o)	User Activities	List of all activities required of site users and their contractors
(p)	Special Procedures during transition	Special procedures to be followed for trouble reporting and escalation during transition activities
(q)	Special Procedures after cutover	Procedures to be followed for trouble reporting and escalation following transition cutover.

#### C.4.3.4.2 GO/NO GO Transition Notice

The contractor shall provide GO/NO GO Transition Notices in accordance with the deliverable specifications that follow in this section.

##### C.4.3.4.2.1 Frequency – GO/NO GO Transition Notice

- Initial: Not less than 24 hours before each scheduled cutover or other significant transition activity or as soon as possible after becoming aware that the activity will not proceed as scheduled

**C.4.3.4.2.2 Deliver To – GO/NO GO Transition Notice**

- Agency Transition Manager
- LGC

Provide a copy to:

- GSA Transition Manager
- Incumbent contractor

**C.4.3.4.2.3 Media/Transport/Format – GO/NO GO Transition Notice**

The contractor shall provide and deliver GO/NO GO Transition Notices to the Agencies, LGCs, and incumbent contractors in accordance with the procedures and in any of the media, transport, and format types described in the Data table in Section C.3.1.2, Data and Report Requirements.

The contractor shall provide and deliver GO/NO GO Transition Notices to GSA in the following ways:

Data		
Media	Transport	Data Format
File Server	<ul style="list-style-type: none"> <li>• Internet File Transfer Protocol (FTP)</li> <li>• Secure Internet File Transfer Protocol (FTPS)</li> <li>• Internet Hypertext Transfer Protocol (HTTP)</li> <li>• Internet Secure Socket Layer (SSL, HTTPS)</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• ASCII Text Tab delimited</li> <li>• ASCII Text Fixed Record</li> <li>• XML</li> </ul>
Email Server	<ul style="list-style-type: none"> <li>• Internet E-Mail – Simple Mail Transfer Protocol (SMTP)</li> <li>• Encrypted Internet E-Mail</li> <li>• Other secured or unsecured transport methods as mutually agreed between Agency and contractor</li> </ul>	<ul style="list-style-type: none"> <li>• Other formats as mutually agreed between Agency and contractor</li> </ul>

**C.4.3.4.2.4 Record Elements-- GO/NO GO Transition Notice**

ID Number	Data Elements	Description
•	Title	GO/NO GO Transition Notice
•	Contractor	Name
•	Agency	Name
•	LGC	Name and contact info
•	Date	Date of notice
•	TAN Date	Date of Transition Action Notice
•	ASRN	Agency Service Request Number
•	Service Order Number	contractor's tracking number for this order

ID Number	Data Elements	Description
•	Scheduled Activity Date/Time	Update to Scheduled Date and Time of Activity
•	Activity Update	Update of service and scheduled activity from Action Notice
•	Preparation Update	Update of Status of preparation for required coordinated action with the incumbent contractor from Action Notice
•	GO/NO GO	Confirmation (GO or NO GO)
•	GO Status	If status is GO: (a) Commercial Circuit Number(s) if applicable (b) Update of site preparation requirements (c) Update of assistance required from Agency or LGC
•	NO-GO Status	If status is NO GO: (a) Synopsis of the reason (b) Projection of when the activity will be re-scheduled

**C.4.4 Transition Report Requirement**

**C.4.4.1 Contractor Reports Provided to Government**

**C.4.4.1.1 Weekly Transition Planning Report**

The contractor shall provide the Weekly Transition Planning Report to GSA and Agencies in accordance with the deliverable specifications that follow in this section.

**C.4.4.1.1.1 Frequency - Weekly Transition Planning Report**

- (a) Initial: No later than one week following acknowledgement of its first Transition Order
- (b) Updated: Weekly no later than the second Government business day following a weekly reporting period ending Sunday night

**C.4.4.1.1.2 Deliver To – Weekly Transition Planning Report**

- (a) GSA Transition Manager
- (b) Agency Transition Manager

**C.4.4.1.1.3 Media/Transport/Format – Weekly Transition Planning Report**

**C.4.4.1.1.3.1 Media/Transport/Format – Weekly Transition Planning Report sent to GSA**

Report		
Media	Transport	File Format
Email Server	Internet E-Mail – Simple Mail Transfer Protocol (SMTP)	MS Word 97 through 2003

**C.4.4.1.1.3.2 Media/Transport/Format – Weekly Transition Planning Report sent to Agency**

The contractor shall provide and deliver Weekly Transition Planning Reports to the Agencies in accordance with the procedures and in any of the media, transport, and format types described in the Report table in Section C.3.1.2, Data and Report Requirements.

**C.4.4.1.1.4 Content – Weekly Transition Planning Report**

ID Number	Information Elements	Description
1	Title	Weekly Transition Planning Report for [specify week]
2	Contractor	Name of contractor
3	Date	Date of Report
4	Agency	For Agency-specific report, Name of Agency for which report is submitted
5	AHC	For Agency-specific report, AHC of Agency for which report is submitted
6	Content	<b>Section I: For Cutovers Sixty Calendar days to Six Months In The Future</b>
	Content	<ul style="list-style-type: none"> <li>Projected activity by Agency, by week, by service and by locations.</li> </ul>
	Content	<ul style="list-style-type: none"> <li>Status of Agency Orders (Number of Transition Orders anticipated by type, and number actually received), TPSP preparation, contractor readiness, and the contractor's orders for access</li> </ul>
	Content	<b>Section II: For Cutovers Two Weeks to Sixty Calendar days In The Future</b>
	Content	Projected and planned activity by Agency, by date (if known, week if not), by location, by service:
	Content	(a) Cross-references between new contractor service to the incumbent contractor's service that is being replaced
	Content	(b) If available, quantity, type, and commercial circuit numbers of new access circuits and facilities required at the location. If not available yet, number and bandwidth of access circuits and special access arrangements required, if any
	Content	(c) Status of Agency readiness and Agency orders
		(d) Status of TPSP preparation, contractor readiness, and the contractor's orders for access
	Content	(e) Status of the incumbent contractor's readiness
	Content	(f) Activities at risk of not meeting planned dates with reason and mitigation planned
	Content	<b>Section III: For Cutovers in Current Week and Next Week</b>
	Content	Projected and planned activity by Agency, by date and <u>time</u> , by location, by service:
	Content	1 Cross-references between new contractor service to the incumbent contractor's service that is being replaced
	Content	2 Quantity, type, and commercial circuit numbers of new access circuits and facilities required at the location
	Content	3 Status of Agency readiness and Agency orders

ID Number	Information Elements	Description
	Content	4 Status of contractor readiness, and the contractor's orders for access
	Content	5 Status of the incumbent contractor's readiness
	Content	6 Activities at risk of not meeting planned dates with reason and mitigation planned
	Content	<b><i>For Changes</i></b>
	Content	Information changed from the previous week shall be highlighted.

**C.4.4.1.2 Weekly Transition Execution Report**

The contractor shall provide the Weekly Transition Execution Report to GSA and Agencies in accordance with the deliverable specifications that follow in this section.

**C.4.4.1.2.1 Frequency – Weekly Transition Execution Report**

- 10. Initial: No later than one week following acknowledgement of its first Transition Order
- 11. Updated: Weekly no later than the second business day following a weekly reporting period ending Sunday night

**C.4.4.1.2.2 Deliver To – Weekly Transition Execution Report**

- 12. GSA Transition Manager
- 13. Agency Transition Manager

**C.4.4.1.2.3 Media/Transport/Format – Weekly Transition Execution Report**

**C.4.4.1.2.3.1 Media/Transport/Format – Weekly Transition Execution Report to GSA**

Report		
Media	Transport	File Format
Email Server	Internet E-Mail – Simple Mail Transfer Protocol (SMTP)	MS Word 97 through 2003

**C.4.4.1.2.3.2 Media/Transport/Format – Weekly Transition Execution Report to Agency**

The contractor shall provide and deliver Weekly Transition Execution Reports to the Agencies in accordance with the procedures and in any of the media, transport, and format types described in Section C.3.1.2, Data and Report Requirements.



#### C.4.4.1.2.4 Content – Weekly Transition Execution Report

ID Number	Information Elements	Description
1	Title	Weekly Transition Execution Report to GSA for [specify period]
2	Contractor	Name of contractor
3	Date	Date of report
4	Agency	For Agency-specific report, Name of Agency for which report is submitted
5	AHC	For Agency-specific report, AHC of Agency for which report is submitted
6	Content	Count of transitions <u>ordered to date</u> by:
	Content	(a) Agency by incumbent contractor by location and service
	Content	(b) Total of all Agencies by incumbent contractor by: location and service
	Content	Count of transitions identified in the <u>Transition Inventory</u> by:
		(a) Agency by incumbent contractor by location and service
	Content	(b) Total of all Agencies by incumbent contractor by: location and service
	Content	Count of transitions <u>ordered to date</u> that have been <u>scheduled</u> by:
	Content	(a) Agency by incumbent contractor by location and service
	Content	(b) Total of all Agencies by incumbent contractor by: location and service
	Content	Count of transitions <u>ordered to date</u> that have not been <u>scheduled over 60 days</u> by:
	Content	<ul style="list-style-type: none"> <li>Agency by incumbent contractor by service and location</li> </ul>
	Content	<ul style="list-style-type: none"> <li>Total of all Agencies by incumbent contractor by: location and service</li> </ul>
	Content	Count of transitions <u>ordered to date</u> that have been <u>cutover</u> by:
	Content	(a) Agency by incumbent contractor by location and service
	Content	(b) Total of all Agencies by incumbent contractor by: location and service
	Content	Count of transitions <u>ordered to date</u> that have been <u>not been cutover (are pending)</u> by:
	Content	<ul style="list-style-type: none"> <li>Agency by incumbent contractor by location and service</li> </ul>
	Content	<ul style="list-style-type: none"> <li>Total of all Agencies by incumbent contractor by: location and service</li> </ul>
	Content	Percentage of transitions <u>ordered to date</u> of those in <u>Transition Inventory</u> by:
	Content	(a) Agency by incumbent contractor by location and service
	Content	(b) Total of all Agencies by incumbent contractor by location and service:

ID Number	Information Elements	Description
	Content	Percentage of transitions <u>scheduled</u> to date of those <u>in Transition Inventory</u> by:
	Content	(a) Agency by incumbent contractor by location and service
	Content	(b) Total of all Agencies by incumbent contractor by: location and service
	Content	Percentage of transitions <u>cutover</u> to date of those <u>in Transition Inventory</u> by:
	Content	(a) Agency by incumbent contractor by location and service
	Content	(b) Total of all Agencies by incumbent contractor by: location and service
	Content	Percentage of transitions <u>scheduled</u> during the <u>weekly period</u> being reported that were <u>cutover</u> by:
	Content	1. Agency by incumbent contractor by location and service
	Content	2. Total of all Agencies by incumbent contractor by: location and service
	Content	Description of transitions by Agency, incumbent contractor, location, and service that were <u>cutover</u> successfully during the <u>weekly period</u> being reported
	Content	Description and status of services by Agency, incumbent contractor, location, and service that were <u>not cutover</u> as originally scheduled and are still <u>pending</u>
	Content	For transitions that are <u>in jeopardy</u> of not meeting the current transition cutover schedules for any reason, description, status, and cause by Agency, location, and service
	Content	Statistics showing by service and by total the <u>mean time</u> from date of Service Order Confirmation to cutover for all transitions <u>to date</u>
	Content	Statistics showing by service and by total the <u>mean time</u> from date of Service Order Confirmation to cutover for all transitions cutover during the <u>weekly period</u> being reported
	Content	Discussion of any other <u>issues</u> affecting the timely completion of transition activities
	Content	Reports of impaired or degraded quality of any contractor service or on gateways or other connections established between Networx and incumbent contractors' networks which may <u>adversely impact the progress</u> of transition
	Content	Discussion of any <u>issues</u> affecting the timely completion of all transition activities regardless of cause
	Content	Any other information identified by the contractor as relative to the status of transition activity.

#### C.4.4.2 Contractor Reports Provided to GSA

##### C.4.4.2.1 Transition Management Plan (TMP)

The contractor shall provide the TMP to GSA in accordance with the deliverable specifications that follow in this section.

##### C.4.4.2.1.1 Frequency - TMP

- 14. Initial: Within 30 calendar days of Notice-to-Proceed
- 15. Revised: Within 15 days after receiving review comments from GSA. GSA comments will be provided to the contractor within 15 days of receiving the Initial Plan
- 16. Updated: As transition operational experience is gained and/or operational circumstances change

**C.4.4.2.1.2 Deliver To – TMP**

17. GSA Transition Manager

**C.4.4.2.1.3 Media/Transport/Format -TMP**

Report		
Media	Transport	File Format
Email Server	Internet E-Mail – Simple Mail Transfer Protocol (SMTP)	MS Word 97 through 2003

**C.4.4.2.1.4 Content--TMP**

ID Number	Information Elements	Description
(a)	Title	Transition Management Plan
(b)	Contractor	Name of contractor
(c)	Date	Date of Plan
(d)	Content	The contractor's transition project management organization including:
	Content	(a) Key transition personnel with telephone numbers
	Content	(b) Roles and responsibilities of key transition personnel
	Content	(c) Organizational and control relationship of the contractor's transition project management organization with the contractor's senior corporate and contractor Program Office (CPO)
	Content	(d) Organizational and control relationship of the contractor project management organization's management and planning staff(s) with the field personnel executing the transition activities
	Content	(e) Description of coordination and workflow between elements of the contractor's transition project management organization, the contractor's subcontractors, access providers, GSA, Agency, incumbent provider, LGC, and other Agency providers (e.g., PBX, network management, information systems)
	Content	(f) Description of how the contractor has addressed in their transition staffing plan the impact of the expected levels of activity on both the management and planning staffs and the field personnel staffs and the contractor's approach to identifying the need for and employing additional staffing when needed to complete additional orders
	Content	(g) Processes and procedures to meet personnel security for all personnel, including field personnel, involved in transition activities if they are different from the processes and procedures used for the program
	Content	(h) Transition escalation procedures with names and

ID Number	Information Elements	Description
		telephone numbers of back-up/escalation personnel
	Content	The contractor's processes and procedures for transition activity scheduling
	Content	The contractor's processes and procedures for creating required transition notifications as described in Sections C.4.3.3.1, Transition Action Notice and C.4.3.3.2, GO/NO GO Notice
	Content	The contractor's processes and procedures for meeting any special technical requirements during transition such as: (a) Direct Station-to-Station Dialing (b) Private Dialing Plans
	Content	The contractor's transition processes and procedures for site surveys should they be ordered by the Agency in support of transition
	Content	List of services contractor is offering
	Content	The contractor's site preparation requirements to include logistical support such as equipment required to be at Agency location receiving the service in time to meet the expedited pace of the transition schedule.
	Content	The contractor's description of the activities required, by all parties, to complete the cutover of service from the incumbent contractor to the contractor by service types offered
	Content	The contractor's processes and procedures for preparation of Transition TPSPs, and ALTPs when required, to include: (c) How they will identify concrete schedules, milestones, and additional support plans that may be required (d) Identifying other information that may be required (e) Format with brief descriptions of contents for each part
	Content	For provisioned services using dedicated access, the contractor's processes and procedures to be used at each location to ensure that continuity and quality of service is maintained through the cutover in each of the following situations:
	Content	(a) Operation of services in parallel, i.e., operation on Agency's existing legacy network(s) concurrent with operation on contractor's network
	Content	(b) Cutover of services when parallel access is available but Agency cannot support or does not want to operate services in parallel
	Content	(c) Cutover of services when parallel access is not available, i.e., access facilities used for incumbent services will need to be used for the contractor's replacement services
	Content	For provisioned services using switched access, the contractor's processes and procedures to be used at each location to ensure that continuity and quality of service is maintained through the cutover
	Content	The contractor's description of the arrangements needed to achieve interconnectivity between the incumbent provider's network and the contractor's network during the transition of service

ID Number	Information Elements	Description
	Content	Key areas of transition risk and the contractor's process and procedures to minimize adverse impact
	Content	The contractor's process and procedures to establish, maintain, operate and update the consolidated Transition Inventory
	Content	The contractor's processes and procedures to provide for 100 percent fall-back to incumbent contractor's service within four hours if the service does not pass the contractor's end-to-end verification testing as defined in Section E, Inspection and Acceptance.
	Content	The contractor's process and procedures to make the transition as transparent as possible to the users and to reduce the overall cost to the Government

**C.4.4.3 Contractor Reports Provided to Agency**

**C.4.4.3.1 Agency-Level Transition Plan (ALTP)**

The contractor shall provide ALTPs in accordance with the deliverable specifications that follow in this section.

The ALTP supplements the TMP. The information in response to the ALTP elements shall be tailored to reflect the perspective of the Agency for which the ALTP is submitted. In addition, the Agency may identify specific elements to be included in the ALTP to meet unique Agency requirements

**C.4.4.3.1.1 Frequency - ALTP**

- (a) Initial: As requested by Agencies
- (b) Updated: As agreed with the Agencies

**C.4.4.3.1.2 Deliver To – ALTP**

- iv. Agency Transition Manager

**C.4.4.3.1.3 Media/Transport/Format – ALTP**

The contractor shall provide and deliver the ALTPs to the Agencies in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements

**C.4.4.3.1.4 Content --ALTP**

ID Number	Information Elements	Description
iv.	Title	Agency-Level Transition Plan for [specific Agency]
v.	Contractor	Name of contractor
vi.	Date	Date of Plan
vii.	Content	List of services covered by this plan
	Content	The contractor's Agency transition project management organization including:

ID Number	Information Elements	Description
	Content	ii.Key Agency transition personnel with telephone numbers
	Content	iii.Roles and responsibilities of key Agency transition personnel
	Content	iv.Organizational and control relationship of the contractor's Agency transition project management organization with the contractor's senior corporate and CPO
	Content	v.Organizational and control relationship of the contractor Agency project management organization's management and planning staff(s) with the field personnel executing the transition activities
	Content	vi.Description of coordination and workflow between elements of the contractor's Agency transition project management organization, the contractor's subcontractors, access providers, GSA, Agency, incumbent provider, LGC, and other Agency

ID Number	Information Elements	Description
	Content	providers (e.g., PBX, network management, information systems).
	Content	vii. Description of how the contractor has addressed in their Agency transition staffing plan the impact of the expected levels of activity on both the management and planning staffs and the field personnel staffs and the contractor's approach to identifying the need for and employing additional staffing when needed to complete additional orders
	Content	viii. Agency Transition escalation procedures with names and telephone numbers of back-up/escalation personnel
	Content	ix. Other TMP content elements identified by the Agency

**C.4.4.3.2 Transition Project Specific Plan (TPSP)**

The contractor shall provide TPSPs in accordance with the deliverable specifications that follow in this section.

The TPSP contains some of the same elements as the TMP and ALTP. However, the information in response to the TPSP elements shall be tailored to reflect the perspective of the specific project for which the TPSP is provided. In addition, the Agency may elect to tailor the TPSP to contain a subset of the information elements listed in the table below.

**C.4.4.3.2.1 Frequency – TPSP**

- (c) Initial: As required Agency for transition activities designated by the Agency. Submit to the Agency no later than 30 calendar days prior to the Customer Want Date

**C.4.4.3.2.2 Deliver To - TPSP**

- (d) Agency Transition Manager

**C.4.4.3.2.3 Media/Transport/Format – TPSP**

The contractor shall provide and deliver TPSPs to the Agencies in accordance with the procedures and in any of the media, transport, and format types described in the Reports table in Section C.3.1.2, Data and Report Requirements.

**C.4.4.3.2.4 Content –TPSP**

ID Number	Information Elements	Description
(a)	Title	Transition Project-Specific Plan for [specific Agency]
(b)	Contractor	Name of contractor
(c)	Date	Date of Plan
(d)	TPSP Identifier	A number assigned by the contractor that uniquely identifies the specific TPSP

ID Number	Information Elements	Description
(e)	Content	The contractor's Project Specific Management organization
	Content	1 Designated Project Manager
	Content	2 POC information (normal business hours and after hours)
	Content	3 Escalation procedures with names and telephone numbers of back-up/escalation personnel
	Content	List of services and respective ASRNs included in the project
	Content	Project schedules and milestones
	Content	a. The contractor's services to be provided by location (specific street address, building, and room)
	Content	b. Specific and concrete schedules by location
	Content	c. Additional support plans that may be required
	Content	The contractor's processes and procedures to meet special Agency requirements and circumstances impacting the specific Transition Project completion
	Content	The contractor's description of the specific activities required to prepare the location(s) for transition to include logistical support
	Content	The contractor's description of the specific activities required by all parties to complete the transitions
	Content	The contractor's description of Government equipment (hardware/software) involved by location for this specific project
	Content	The contractor's description of contractor equipment required to be at Agency site for this specific project
	Content	The contractor's processes and procedures to meet special technical requirements if required such as: 1. Direct Station-to-Station Dialing 2. Private Dialing Plans
	Content	Key areas of risk for the specific project and the contractor's processes and procedures to minimize risk
	Content	Unresolved issues that apply to this specific project that may require contractual or management action such as:
	Content	1. Billing
	Content	2. Application of Service Initiation Charges (SICs)
	Content	3. Service Ordering processing
	Content	4. Service changes or enhancements needed.
	Content	Other project specific matters that the contractor considers necessary to include
	Content	Results of the Section C.4.2.5, Step 5—Create Transition Inventory for the services and locations pertinent to the project
	Content	Cross-references between contractor's services being implemented and incumbent contractor's service as inventoried for the specific project
	Content	The contractor's description of the specific activities required, by all parties, to complete the transitions
	Content	1 Identify the specific coordination required with the incumbent contractor
	Content	2 Identify the specific coordination required with the access service provider(s)



ID Number	Information Elements	Description
	Content	3 Identify the specific coordination required with the Agency, the LGC and other Agency service provider(s)
	Content	For provisioned services using dedicated access, the contractor's approach to dealing with any of the following situations that apply to the specific project:
	Content	(a) Operation of services in parallel, i.e., operation on Agency's existing legacy network(s) concurrent with operation on contractor's network
	Content	(b) Cutover of services when parallel access is available but Agency cannot support or does not want to operate services in parallel
	Content	(c) Cutover of services when parallel access is not available, i.e., access facilities used for incumbent services will need to be used for the contractor's replacement services
	Content	For provisioned services using switched access, the contractor's approach to the specific project to ensure that continuity and quality of service is maintained through the cutover for each location
	Content	Arrangements proposed to achieve interconnectivity between the incumbent contractor's network and the contractor's network during the transition of service for this specific project
	Content	Activities required to complete the cutover of service from incumbent contractor to the contractor
	Content	The contractor's processes and procedures to provide for 100 percent fall-back to incumbent contractor's service within four hours if the service does not pass the contractor's end-to-end verification testing as defined in Section E, Inspection and Acceptance.

## C.5 NATIONAL SECURITY AND EMERGENCY PREPAREDNESS (NS/EP)

### C.5.1 Introduction

Telecommunications requirements for NS/EP are based on a set of telecommunications policies and procedures established by the National Communications System (NCS) in accordance with Executive Order 12472, developed to ensure critical Government and industry needs are met when an actual or potential emergency threatens the security or socio-economic structure of the U.S.

A national emergency is any circumstance or crisis (local, national, or international) that causes, or could cause, injury or harm to the population, damage to or loss of property, or that degrades or threatens the NS/EP posture of the U.S. under conditions of natural and man-made disasters and emergencies. Within the context of telecommunications services, emergency preparedness is the maintenance of a telecommunications capability in a state of readiness to meet the needs of Government (state, local, tribal, and Federal) during national emergencies.

To meet the NS/EP telecommunications requirements, the NCS administers<sup>7</sup> the Telecommunications Service Priority (TSP), Telecommunications Electric Service Priority (TESP)<sup>8</sup>, Government Emergency Telecommunications Service (GETS), and Wireless Priority Service (WPS).

Executive Order 12472 states that GSA “shall ensure that federally owned or managed domestic communications facilities and services meet the national security and emergency preparedness requirements of the Federal civilian departments, Agencies, and entities.” Therefore, the Networx program will adhere to NS/EP guidelines and requirements.

As a critical component of the national telecommunications infrastructure, the Networx program will interoperate with, utilize, and complement the NCS NS/EP programs. Because the Networx service extends into thousands of Government offices throughout the country, the Networx networks represent a key resource for coping with emergency and disaster situations, and the Networx networks are required to be maintained in a state of readiness for any emergencies.

The following definitions are used in this section:

1. The term contractor's Networx network includes all infrastructures, SDP to SDP, used by the contractor to provide Networx services, whether or not that infrastructure is owned by the contractor.

Critical users of NS/EP telecommunications are key Government officials whose position requires special access and network treatment to assure telecommunications services during emergencies. During an emergency, critical users at Federal Agencies generally interact with the management of critical industries, other Federal Agencies, and state, local, and tribal Governments, on both an individual and regional basis, for developing emergency response options. It is estimated that the number of Networx NS/EP critical users will not exceed 10,000 and, for the purposes of traffic analyses, it may be assumed that they are distributed uniformly among the Networx users. The list of Networx NS/EP critical users is independent of the list maintained by the NCS, although the lists may overlap.

The following documents provide backgrounds and standards as applicable:

1. NCS “Technical Information Bulletin 02-1, February 2002”
2. NCS “National Communications System: 1963-1998, April 1998”

---

<sup>7</sup> FCC Network Reliability and Interoperability Council (NRI), Homeland Security, Physical Security, NCS-administered Priority Services (NRI VI-1A-08) [<http://www.nric.org/fg/nricvfg.html>]

<sup>8</sup> NCS administers TESP program, which promotes (on a voluntary basis) the inclusion of critical telecommunications facilities in electric service providers priority restoration plans. [<http://www.ncs.gov> and Footnote 1 above]

3. CTF "Report of the Convergence Task Force, December 2000"
4. ANSI T1.TR.79-2003, "Overview of Standards in Support of Emergency Telecommunication Service (ETS)"
5. ITU-TSS E.106, "Description of an International Emergency Preference Scheme"
6. ITU-TSS Draft F.706, "Service Description for an International Emergency Multimedia Service (IEMS)"
7. ANSI T1.631-1993 (R 1999) and Telcordia GR-2931-Core, "High Probability of Completion (HPC) Network Capability"
8. NCS "WPS FOC Requirements for GSM-Based Systems, September 2002"
9. NCS "WPS Industry Requirements for FOC for CDMA-Based Systems – Home Locations Registers (HLR), Issue 1.0; June 4, 2004"
10. NCS "GETS Legacy Functional Requirements Specification, August 2003"
11. 3GPP: 3<sup>rd</sup> generation mobile multimedia standards
12. IETF RFC 3131, IETF standardization collaboration for 3GPP
13. FCC "The Network Reliability and Interoperability Council (NRIC), Focus Group 1A, Physical Security Recommendations (specifically VI-IA-05 through VI-IA-10)", March 5, 2003
14. ANSI T1A1, ATIS TMOC and ITU standards on Emergency Telecommunications Service (ETS)
15. All new versions, amendments, and modifications to the above documents and standards as they become applicable.

Detailed NS/EP requirements for Network are described below.

## C.5.2 NS/EP Technical Requirements

### C.5.2.1 Basic Functional Requirements (As Applicable)

The following 14 basic functional requirements for NS/EP telecommunications and IT services are identified by the NCS and the Office of Science and Technology Policy for NS/EP telecommunications services and are now being endorsed by ANSI T1 and ITU-TSS standard bodies and widely supported by vendor communities:

1. Enhanced Priority Treatment. Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.
2. Secure Networks. Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
3. Non-Traceability. Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).

4. Restorability. Should a service disruption occur, voice and data services must be capable of being reprovisioned, repaired, or restored to required service levels on a priority basis.
5. International Connectivity. Voice and data services must provide access to and egress from international carriers.
6. Interoperability. Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award.
7. Mobility. The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e., Personal Communications Service (PCS), cellular, satellite, high frequency (HF) radio).
8. Nationwide Coverage. Voice and data services must be readily available to support the national security leadership and inter- and intra- Agency emergency operations, wherever they are located.
9. Survivability/Endurability. Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
10. Voice Band Service. The service must provide voice band service in support of presidential communications.
11. Broadband Service. The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, web access, multimedia).
12. Scaleable Bandwidth. NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
13. Affordability. The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).
14. Reliability/Availability. Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

#### **C.5.2.2 Network Services for NS/EP (As Applicable)**

The following Network services, at a minimum, shall be supported during emergencies:

1. Voice Services (VS) [see contract Section C.2.2.1] (if provided)
2. Cellular/Personal Communications Service (CPCS) [see Contract Section C.2.14.1] (if provided)
3. Toll Free Service (TFS) [see Contract Section C.2.2.3] (if provided)
4. Audio Conference Service (ACS) [see contract Section C.2.8.2] (if provided)
5. Video Teleconferencing Service (VTS) [see Contract Section C.2.8.1] (if provided)
6. Frame Relay Service (FRS) [see Contract Section C.2.3.1] (if provided)
7. Internet Protocol Service (IPS) [see Contract Section C.2.4.1]
8. Network Based IP VPN Service (NBIP-VPNS) [see Contract Section C.2.7.3]

9. Premises Based IP VPN Service (PBIP-VPNS) [see Contract Section C.2.7.2] (if provided)
10. Asynchronous Transfer Mode Service (ATMS) [see Contract Section C.2.3.2] (if provided)
11. Secured Managed E-Mail Service (SMEEMS) [see Contract Section C.2.10.8] (if provided)
12. Private Line Service (PLS) [see Contract Section C.2.5.1] (if provided)
13. Ethernet Service (EthS) [see Contract Section C.2.7.1] (if provided)
14. Layer 2 VPN Service (L2VPNS) [see Contract Section C.2.7.12] (if provided)
15. Internet Protocol Telephony Service (IPTelS) [see Contract Section C.2.7.10] (if provided)
16. Voice over Internet Protocol Transport Services (VOIPTS) [see Contract Section C.2.7.8]
17. Converged IP Services (CIPS) [see Contract Section C.2.7.11] (if provided)

The contractor shall support 14 basic functional requirements (see Section C.5.2.1) for the above Network services as specified in Section C.5.2.2.1.1 as follows:

3. VS, TFS, ACS, FRS, IPS, NBIP-VPNS, ATMS, and CPCS on contract award because commercial feasibility for these services is already available<sup>9</sup>
4. For the rest of the services (i.e., VTS, PBIP-VPNS, SMEEMS, PLS, ES, L2VPNS, IPTelS, VOIPTS, and CIPS) after ANSI T1 and ITU standards are formally approved and commercial feasibility is developed.

The contractor shall provide an NS/EP Functional Requirements Implementation Plan (NS/EP FRIP) on contract award. Part A of the NS/EP FRIP shall include technical systems, administration, management, and operational areas in the contract addressing how the 14 basic functional requirements will be supported for the above services (See Section C.7 for format). Part B of the NS/EP FRIP addresses assured service in the National Capital Region and is discussed in Section C.5.2.7. The contractor shall revise the complete plan as required by the Network PMO not later than 15 business days after notification by the Government. The complete NS/EP FRIP shall be updated at least annually and provided to the Network PMO for approval.

---

<sup>9</sup> GSA FTS Office of Information Assurance and Critical Infrastructure Protection, "NS/EP Telecommunications Applications, July 2002"

**C.5.2.2.1 NS/EP Basic Functional Requirements Matrix for Network Services**

	NS/EP Basic Functional Requirements													
	Req #1	Req #2	Req #3	Req #4	Req #5	Req #6	Req #7	Req #8	Req #9	Req #10	Req #11	Req #12	Req #13	Req #14
VS	x	x	x	x	x	x	x	x	x	x			x	x
CPCS	x	x	x	x	x	x	x	x	x	x			x	x
TFS	x	x	x	x			x	x	x				x	x
ACS	x	x	x	x	x	x	x	x	x				x	x
VTs	x	x	x	x	x	x	x	x	x		x		x	x
FRS	x	x	x	x		x	x	x	x		x	x	x	x
IPS	x	x	x	x	x	x	x	x	x		x	x	x	x
NBIP_VP														
NS	x	x	x	x		x	x	x	x		x	x	x	x
PBIP-VPNS						x	x	x	x		x	x	x	x
ATMS	x	x	x	x		x	x	x	x		x	x	x	x
SMES	x	x	x	x	x	x		x	x				x	x
PLS	x	x	x	x	x	x	x	x	x		x		x	x
EthS	x	x	x	x		x	x	x	x		x	x	x	x
L2VPNS	x	x	x	x		x	x	x	x		x	x	x	x
IPTelS	x	x	x	x	x	x	x	x	x				x	x
VOIPs	x	x	x	x		x	x	x	x				x	x
CIPS	x	x	x	x		x	x	x	x		x	x	x	x

**C.5.2.3 Relationship with the NCS NS/EP Programs (As Applicable)**

The contractor's Network network during NS/EP events shall interoperate with, utilize, and complement the NCS NS/EP initiatives and programs as follows:

- i. Interoperate. The functional requirements (i.e., recognize dialing sequence and handover the call) for interoperability with the NCS GETS and WPS for end-to-end call completion during network congestions in the wireline and/or wireless networks during times of stress are described below.
  - a. NCS GETS. The GETS provides authorized government and industry NS/EP users with a nationwide switched voice and voice band data communications priority service during periods of network congestion. The GETS universal access number is 710-NCS-GETS (710-627-4387).
 

Therefore, the Network contractor shall recognize the GETS dialing sequence and hand-over the GETS calls to NCS-identified GETS Local Exchange Carriers (LECs) for priority call processing. The contractor shall employ best effort for high probability of completion while handing over the call to the PSN.
  - b. NCS WPS. The WPS provides authorized government and industry NS/EP users the ability to complete the call during periods of wireless networks congestion. The WPS provides end-to-end solution, fully integrated with

GETS, for nationwide coverage. The WPS universal access code prefix is “\*272”, which needs to be dialed before the destination number (e.g., \*272 703 555-1234) for priority call processing. If landline networks are also congested, dial “\*272” plus the GETS access number (i.e., \*272 710-NCS-GETS) to get priority in both wireless and landline networks.

Therefore, the Network shall recognize the WPS dialing sequence and shall treat WPS calls as follows:

2. If the Network contractor currently supports WPS, the contractor shall recognize the WPS dialing sequence and handover the WPS calls logically to the commercial (i.e., PSN) arm of the contractor’s cellular service for priority call processing.
3. If the Network contractor does not currently support WPS, the contractor shall treat the WPS dialing sequence as invalid and shall return appropriate announcement to the user. However, if in the future, the contractor supports WPS, the contractor shall treat WPS calls as above, from that time onward.
  - ii. Utilize. The contractor shall have reserve and emergency power as per best commercial practices and whenever possible shall utilize NCS TESP for priority restoration of electric power in all transmission, switching, signaling, and major facility nodes.
  - iii. Complement. After contract award, the Network contractor shall participate, upon Government request and on an individual case basis, in studies to determine appropriate ways in which Network network assets, and especially the many Network dedicated access lines, may be used to support GETS.

#### **C.5.2.4 Telecommunication Service Priority (As Applicable)**

The TSP System (FCC 88-341) provides a framework for telecommunications services vendors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunication services. The TSP System applies to common carriers, to Government, and to private systems that interconnect with commercially provided services or facilities. The TSP System is intended to apply to all aspects of end-to-end NS/EP telecommunication services. The TSP system allows five levels of priorities for restoration and provisioning.

The contractor shall fully comply with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level for design change of circuits, including coordination between local access providers and the transport segment. The contractor shall also fully comply with any future TSP replacement system.

Should the contractor's network experience significant degradation or failure, the contractor shall provide priority restoration of affected Network services in accordance with the TSP system five levels of priorities. In addition, the contractor shall ensure that the restored circuits retain the property of the original circuits (i.e., TSP levels). [Note that the contractor is only obligated for priority restoration and provisioning of those circuits that Agencies have obtained TSP priorities from NCS.]

#### **C.5.2.5 Protection of SS7 Signaling System and Satellite Command Link (As Applicable)**

Protection of SS7 Signaling System. The contractor shall protect common channel signaling (ITU-TSS No. 7 or SS7) paths by using either encryption equipment endorsed under the National Security Agency (NSA) Commercial COMSEC Endorsement Program (CCEP) or any other National Institute of Standards and Technology (NIST)/NSA approved encrypted/non-encrypted forms of protection or by using other equally effective methods, such as physical isolation, message throttling, screening, and tunneling.

Protection of Satellite Command Link. If satellite communications are used in providing any Network services (see Section C.5.2.2), the contractor shall encrypt the command and control link to any satellite launched after June 17, 1990, (in accordance with the National Telecommunications InterAgency Security Subcommittee, No. 1). However, if there are other measures available that can mitigate command-link takeover, they shall be utilized wherever economical and approved on a prior basis by the Government.

#### **C.5.2.6 Protection of Classified and Sensitive Information**

The NS/EP related information includes, but is not limited to, databases for classified information; critical users' locations, identifications, authorization codes, and call records; and, customer profiles. In addition, the contractor will be provided access to certain classified and sensitive materials required for the planning, management, and operations for NS/EP. That information will be in various forms, including hardcopy and electronic media. It will be identified as to its classification and shall be protected by the contractor in accordance with applicable industrial security regulations (National Industrial Security Program Operating Manual [NISPOM] and NSA approved standards as applicable for Safeguarding Classified Information). The level of classification may be up to Top Secret, and will be identified by the Government.

#### **C.5.2.7 Assured Service in National Capital Region**

Because of the high concentration of traffic into and out of the National Capital Region, the contractor shall use at least two geographically separate network switches/routers to serve the National Capital Region and the loss of one of these switches/routers shall not result in a loss of more than 15 percent of total network traffic.

In addition, the contractor shall assure the service-specific performance levels when the PSN in the U.S. is in severe overload condition. However, appropriate adjustments in the requirements will be made in areas where network damage has occurred.



If the National Capital Region is covered in the contract, the contractor shall:

1. Provide Part B of the NS/EP FRIP addressing the strategy for assured service in the National Capital Region
2. The NS/EP FRIP Part B shall address technical systems and administration, management, and operations requirements for the National Capital Region.

#### **C.5.2.8 Network Evolution**

The contractor shall identify to the Networx PMO the emerging technical standards for emergencies as being developed and approved by ANSI T1, ITU-TSS, and 3GPP that may impact the interoperability and reliability of any network element inserted into the mix of technologies due to technology refreshment.

#### **C.5.3 NS/EP Management Requirements**

##### **C.5.3.1 NS/EP Interface with the Contractor**

The Disaster Recovery Officer, as defined in Section 3.3, shall also serve as the NS/EP Emergency Liaison Officer. This requirement shall also apply to any contractor personnel designated as the liaison officer after contract award if deemed necessary by the Networx PMO. The liaison officer's top priority will be the coordination of the contractor's corporate capabilities with the Networx PMO.

#### **C.6 SECTION 508 REQUIREMENTS**

##### **C.6.1 Background**

Section 508 is the statutory section of the Rehabilitation Act of 1973 that requires federally procured Electronic Information Technology (EIT) to provide disabled federal employees with access to and use of information that is comparable to information provided to nondisabled federal employees (EIT is defined in FAR 2.101). Section 508 also requires federal Agencies to provide disabled public citizens with access to and use of information that is comparable to information provided to nondisabled public citizens. See [www.section508.gov](http://www.section508.gov) for additional information.

The Access Board, an independent federal Agency, establishes the standards that federally procured EIT products and services are required to meet. These consist of Technical Standards (Section 508, Subpart B), Functional Performance Criteria (Section 508, Subpart C), and Information, Documentation, and Support (Section 508, Subpart D).

Agencies may accept EIT that uses designs and/or technologies that do not meet applicable Technical Standards of Subpart B but do provide disabled federal employees or citizens with equivalent or greater access to information. This is referred to as "equivalent facilitation" and vendors offering equivalent facilitation will be considered along with those that strictly meet the Technical Standards of Subpart B.

### **C.6.2 Voluntary Product Accessibility Template (VPAT)**

The Government requests that contractor submit a Voluntary Product Accessibility Template for each service identified in paragraphs C.6.4 below to demonstrate that offerings comply with Section 508 standards (refer to <http://www.gsa.gov/networx>) This will assist the Government in evaluating services for Section 508 standard compliance.

### **C.6.3 Section 508 Applicability to Technical Requirements**

The Technical Requirements section (Section C.2) of the contract identifies the technical provisions for Networx services used by an Agency to execute mission operations. Services that execute mission operations shall meet the relevant provisions of Section 508, Subparts B, C, and D as identified in paragraph C.6.4 or shall provide equivalent facilitation.

### **C.6.4 Section 508 Provisions Applicable to Technical Requirements**

The relevant provisions of Subpart B, Technical Standards, paragraph 1194.21, Software Applications and Operating Systems, shall apply to the following Networx services:

2. Call Center/Customer Contact Center Services (CCS)
3. Cellular/PCS (CPCS)
4. Collaboration Support Services (CoSS)
5. Converged IP Services (CIPS)
6. IP Telephony Services (IPTeIS)
7. Managed E-Authentication Services (MEAS)
8. Multimode Wireless LAN Service (MWLANS)
9. Paging (PagS)
10. TeleWorking Solutions (TWS)
11. Unified Messaging Services (UMS)
12. Web Conferencing Service (WCS)

The relevant provisions of Subpart B, Technical Standards, paragraph 1194.22, Web-based Intranet and Internet Information and Applications, shall apply to the following Networx services:

11. Call Center/Customer Contact Center Services (CCS)
12. Cellular/PCS (CPCS)
13. Collaboration Support Services (CoSS)
14. Converged IP Services (CIPS)
15. Incident Response Service (INRS)
16. Internet Facsimile Service (IFS)
17. IP Telephony Service (IPTeIS)
18. IP Video Transport Services (IVTS)
19. Managed E-Authentication Services (MEAS)
20. Managed Tiered Security Services (MTSS)
21. Paging Service (PagS)

22. Secure Managed Email Service (SMES)
23. TeleWorking Services (TWS)
24. VOIP Transport Service (VolPTS)
25. Web Conferencing Service (WCS)
26. Unified Messaging Services (UMS)

The relevant provisions of Subpart B, Technical Standards, paragraph 1194.23, Telecommunications Products, shall apply to the following Network services:

27. Call Center/Customer Contact Center Services (CCS)
28. Cellular/PCS (CPCS)
29. Combined Services (CS)
30. Converged IP Services (CIPS)
31. IP Telephony Services (IPTeIS)
32. Land Mobile Radio Service (LMRS)
33. Paging Service (PagS)
34. Voice Services (VS)
35. TeleWorking Services (TWS)
36. Toll Free Service (TFS)
37. Unified Messaging Services (UMS)
38. VOIP Transport Service (VolPTS)

The relevant provisions of Subpart C, Functional Performance Criteria, paragraph 1194.31, shall apply to the services identified in paragraphs C.6.4. above. For these services, the contractor shall provide one of the following two capabilities:

- a. Support for assistive technologies used by disabled individuals.
- b. At least one mode of operation and information retrieval that:
  - g. For blind users, does not require vision.
  - h. For vision impaired users, does not require visual acuity greater than 20/70.
  - i. For deaf users, does not require hearing.
  - j. For hearing impaired users, does not require enhanced auditory capability.
  - k. For users with no speech capability or with impaired speech, does not require user speech.
  - l. For users without fine motor control or simultaneous action capability, does not require fine motor control or simultaneous action and is operable without limited reach and strength.

The relevant provisions of Subpart D, Information, Documentation, and Support, paragraph 1194.41, shall apply to the services identified in paragraphs C.6.4.1 above.

#### **C.6.5 Section 508 Provisions Applicable to Reporting and Training Requirements**

The Government's information reporting requirements are addressed in the Management and Operations section (Sections C.3.2 through C.3.9) and in the

Technical Reporting section (Section C.7) of the Contract. Required information shall be reported via the Internet, email, or telephone. Services providing the required information shall meet the relevant provisions of Section 508, Subparts B, C, and D or shall provide equivalent facilitation.

Training requirements are outlined in Section C.3.7.2. Training shall be delivered via meeting and briefings, classroom, seminars, instructor-led and non-instructor on-line web based, self study, and manuals or desk top guides. For training delivered via meeting and briefings, classroom, and seminars, assistance such as signers and Braille products shall be provided to disabled trainees when requested in advance by the Government. For training delivered via instructor-led and non-instructor on-line web based, the same capabilities provided for Internet reporting shall be provided to disabled trainees. For self study and manuals or desk top guides using audio/video tapes, CD ROM, DVD, the relevant provisions outlined in Section C.6.4 above shall apply.

### **C.7 Technical Reports**

The contractor shall provide the following reports to the subscribing Agency & GSA COR as required for each service identified below. Instructions on report delivery, applicable contract section, media, format, frequency, and data elements are also included. The contractor shall provide these reports in a media and with the frequency as appropriate to the Agency. Each report shall contain standard information including but not limited to the following:

1. Contractor Name
2. Contract Number
3. Title of Report
4. Date of Report
5. Period covered by the Report
6. Name of subscribing Agency
7. Service(s) included in the Report

Management and Operations Reports are defined in Section C.3.

### **C.7.1 Frame Relay Service (FRS)**

#### **C.7.1.1 FRS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.3.1
3. Media — Electronically
4. Format — Contractor commercial format
5. Frequency
6. First report — 5 business days after the first complete calendar month
7. Updated — Monthly
8. Data Elements to be contractor proposed and to include but not limited to

1. Network statistics
2. Exception analysis
3. Network availability and latency
4. Error rates
5. Utilization

## **C.7.2 Asynchronous Transfer Mode Service (ATMS)**

### **C.7.2.1 ATMS Performance Reports**

- i. Deliver to — Subscribing Agency & GSA COR
- ii. Section — C.2.3.2
- iii. Media — Electronically
- iv. Format — Contractor commercial format
- v. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — Monthly
    - vi. Data Elements to be contractor proposed and to include but not limited to
      - a. Network statistics
      - b. Exception analysis
      - c. Network availability and latency
      - d. Error rates
      - e. Utilization

## **C.7.3 Dark Fiber Services (DFS)**

### **C.7.3.1 DFS Acceptance Reports**

- i. Deliver to — Subscribing Agency & GSA COR
- ii. Section — C.2.5.3
- iii. Media — Electronically
- iv. Format — contractor commercial format
- v. Frequency — Acceptance criteria for each fiber measured at delivery, and as requested by the subscribing Agency
- vi. Data Elements to be contractor proposed and to include but not limited to
  - a. Attenuation coefficient SMF
    - i. 1550 nm
    - ii. 1310 nm
  - b. Attenuation coefficient MMF
    1. 850 nm (50/125  $\mu\text{m}$ )
    2. 1300 nm (50/125  $\mu\text{m}$ )
      - c. Polarization Mode Dispersion (PMD)
        1. Long distance networks

2. Metro networks
  - d. Chromatic dispersion at 1550 nm
  - e. Reflectance events (all events)
  - f. TTR
  - g. Connectors
    - a. Return loss
    - b. Insertion loss
  - h. Optical Time Domain Reflectometer (OTDR) traces

#### **C.7.4 Premises-Based IP VPN Services (PBIP-VPNS)**

##### **C.7.4.1 PBIP-VPNS Performance Reports**

- a. Deliver to—Subscribing Agency & GSA COR
- b. Section—C.2.7.2
- c. Media—Electronically
- d. Format—contractor commercial format
- e. Frequency
  - a. First — 5 business days after the first complete calendar month
  - b. Updated — Monthly

1. Data Elements to be contractor proposed and to include but not limited to
  - a. Network statistics
  - b. Exception analysis
  - c. Network availability and latency
  - d. Error rates
  - e. Utilization

#### **C.7.5 Network-Based IP VPN Services (NBIP-VPNS)**

##### **C.7.5.1 NBIP-VPNS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.7.3
3. Media — Electronically
4. Format — contractor commercial format
5. Frequency
  - i First report — 5 business days after the first complete calendar month
  - ii Updated — Monthly
6. Data Elements to be contractor proposed and to include but not limited to
  - i Network statistics
  - ii Exception analysis
  - iii Network availability and latency
  - iv Error rates
  - v Utilization

#### **C.7.6 Managed Tiered Security Services (MTSS)**

**C.7.6.1.1 MTSS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.7.4
3. Media — Electronically
4. Format — contractor commercial format
5. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — Monthly
6. Data Elements to be contractor proposed and to include but not limited to
  1. Availability
    - i. Firewall
    - ii. NSA approved multilevel security solution (as applicable)
    - iii. Type 1 Encryption (as applicable)
    - iv. Web portal
  2. Configuration/Rule change
  3. Event notification
  4. Help desk statistics
  5. Security incident reporting

**C.7.7 Layer 2 VPN Services (L2VPNS)****C.7.7.1 L2VPNS Performance Reports**

- Deliver to — Subscribing Agency & GSA COR
- Section — C.2.7.12
- Media — Electronically
- Format — contractor commercial format
- Frequency
  - First report — 5 business days after the first complete calendar month
  - Updated — Monthly
- Data Elements to be contractor proposed and to include but not limited to
  - Network statistics
    - i. Availability
    - ii. Latency
    - iii. TTR
    - iv. Packet jitter
    - v. Data delivery rate
  - b. Exception analysis
  - c. Utilization

**C.7.8 Incident Response Services (INRS)**

**C.7.8.1.1 INRS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.10.5
3. Media — Electronically
4. Format — contractor commercial format
5. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — At incident
6. Data Elements to be contractor proposed and to include but not limited to
  4. Response Time
    - i. On-site
    - ii. Telephone

**C.7.9 Call Center/Customer Contact Center Services (CCS)**

**C.7.9.1 CCS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.11.2
3. Media — Electronically
4. Format — Contractor commercial format
5. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — Monthly
6. Data Elements to be contractor proposed

**C.7.10 Storage Services (SS)**

**C.7.10.1 SS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Contract section — C.2.11.10
3. Media — Electronically
4. Format — Contractor commercial format
5. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — Monthly
6. Data Elements to be contractor proposed

**C.7.11 TeleWorking Solutions (TWS)**



**C.7.11.1.1 TWS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.12.1
3. Media — Electronically
4. Format — Contractor commercial format
5. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — Monthly
6. Data Elements to be contractor proposed

**C.7.12 Cellular/Personal Communications Service (CPCS)****C.7.12.1 CPCS Performance Reports**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.14.1
3. Media — Electronically
4. Format — Contractor commercial format
5. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — Monthly
6. Data Elements to be contractor proposed and to include but not limited to
  - a. Availability
  - b. TTR

**C.7.13 Multimode/Wireless LAN Service (MWLANS)****C.7.13.1.1 MWLANS Performance Reports**

- a. Deliver to — Subscribing Agency & GSA COR
- b. Contract section — C.2.14.3
- c. Media — Electronically
- d. Format — Contractor commercial format
- e. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — Monthly
- f. Data Elements to be contractor proposed and to include but not limited to
  - a. Availability
  - b. TTR

**C.7.14 Unified Messaging Service (UMS)****C.7.14.1 UMS Performance Report**

1. Deliver to — Subscribing Agency & GSA COR
2. Section — C.2.11.11
3. Media — Electronically
4. Format — Contractor commercial format
5. Frequency

- a. First report — 5 business days after the first complete calendar month
- b. Updated — Monthly

6. Data Elements to be contractor proposed

**C.7.15 Land Mobile Radio Service (LMR)**

**C.7.15.1.1 LMR Performance Report**

- 25. Deliver to — Subscribing Agency & GSA COR
- 26. Section — C.2.14.6
- 27. Media — Electronically
- 28. Format — Contractor commercial format
- 29. Frequency
  - a. First report — 5 business days after the first complete calendar month
  - b. Updated — As requested by the subscribing Agency
- 30. Data Elements to be contractor proposed

**C.7.16 National Security and Emergency Preparedness (NS/EP) Functional Requirements Implementation Plan (FRIP)**

**C.7.16.1 Part A—NS/EP FRIP**

- 2. Deliver to — Networkx Program Management Office (PMO)
- 3. Section — C.5.2.2
- 4. Media — Electronically
- 5. Format — Mutually agreed with Networkx PMO
- 6. Frequency
  - b. First plan — Upon contract award
  - c. Updated — Annually, and as requested by the Networkx PMO
- 7. Data Elements to be contractor proposed and to include but not limited to
  - b. Technical systems
  - c. Administration
  - d. Management
  - e. Operations

**C.7.16.2 Part B—NS/EP FRIP**

- e. Deliver to — Networkx PMO
- f. Section — C.5.2.7
- g. Media — Electronically
- h. Format — Mutually agreed with Networkx PMO
- i. Frequency
  - o First plan — Upon contract award
  - o Updated — Annually, and as requested by the Networkx PMO
- j. Data Elements to be contractor proposed and to include but not limited to
  - iii. Technical systems
  - iv. Administration
  - v. Management
  - vi. Operations