

**PROFESSIONAL SERVICES  
SECURITY PROGRAM ASSESSMENT (NIST 800-53)  
STATEMENT OF WORK  
TO VERIZON PROFESSIONAL SERVICES SERVICE ATTACHMENT**

This Statement of Work (SOW) is entered into between the entities identified as, respectively, Verizon and Customer in the related Service Order Form (SOF).

1. **PROJECT DESCRIPTION.** Verizon will provide Customer with a Security Program Assessment (SPA) using NIST 800-53 standards. Customer may also order a Roadmap option which provides guidance on implementing Verizon’s recommendations.
2. **SCOPE OF WORK.** Verizon’s SPA service will be provided an assessment of Customer’s security requirements in the functional areas listed in the NIST 800-53 standard as provided below (Security Requirements):

NIST 800-53		
<ul style="list-style-type: none"> <li>• Media Protection</li> <li>• Awareness and Training</li> <li>• Audit and Accountability</li> <li>• Security Assessment and Authorization</li> <li>• Risk Assessment</li> <li>• Contingency Planning</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• System and Services Acquisition</li> <li>• Identification and Authentication</li> <li>• System and Communications Protection</li> <li>• System and Information Integrity</li> <li>• Physical and Environmental Protection</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Response</li> <li>• Maintenance</li> <li>• Program Management</li> <li>• Access Control</li> <li>• Planning</li> <li>• Personnel Security</li> </ul>

- 2.1 **Package Sizes.** SPA is available in Small, Medium, and Large sizes (Customer selected size detailed on the SOF). Small package is for companies with less than 1,000 employees, one local headquarter (HQ) location and one primary local business unit. Medium package is for companies with less than 10,000 employees, one local HQ location and up to three primary local business. Large package is for companies with greater than 10,000, and no more than 50,000 employees, one local HQ location and up to ten primary business units (international locations will be delivered remote only). Packages will be delivered locally which means in the same country as the contracting country, except where specifically stated.
- 2.2 **Project Initiation.** Verizon will schedule and conduct a kick-off meeting to initiate the Project, to review the SPA size ordered, and confirm if the Order includes Roadmap option. Verizon and Customer will identify documentation and responsible individuals with knowledge of Customer’s security program. Verizon will review Customer documentation, and will work with Customer to plan interviews.
- 2.3 **Data Collection.** Verizon will review Customer provided documentation, interview identified individuals and collect information regarding Customer’s security program. Verizon will work with Customer to collect documentation and interview individuals with knowledge of Customer’s security program.
- 2.4 **Data Analysis.** Verizon will analyze the collected information and determine Customer’s security program maturity, performance, and scope relative to Customer’s Security Requirements. Verizon will develop compliance and maturity scores from this analysis. Verizon will develop and rank order conclusions and recommendations designed to help Customer avoid or reduce risks, and/or achieve greater alignment with Customer’s Security Requirements.
- 2.5 **Roadmap.** If ordered pursuant to a SOF, Verizon will provide a detailed roadmap for implementing Verizon’s recommendations in the report. Verizon will meet with Customer to determine which recommendations from the report will be included in the Roadmap and then develops project definitions,

timing, costs and staffing projections for each recommendation that is to be included in the Roadmap.

- 2.6 **Security Assessment Program Report.** Verizon will develop a draft report and deliver it to the Customer via secure means. Customer will review the report and make comments, and Verizon will finalize and submit a final report to Customer. The final report will include the findings and recommendations (SPA Report). The SPA Report will include the following sections:
- **Executive Summary:** Highlights Customer's current practice and maturity relative to Customer's Security Requirement, and provides a summary of recommendations for improving Customer's information security program.
  - **Controls Assessment:** Provides Verizon's assessment of Customer's information security program compared to Customer's Security Requirement. This includes analysis of the alignment and maturity of information security practices with each of the required information security controls.
  - **Recommendations:** Provides recommendations for improvements to Customer's information security program that address identified weaknesses. Verizon provides a suggested priority order for implementing the recommendations to mature the program and reduce the risk to Customer.
  - **Roadmap:** If purchased, provides a roadmap of Verizon's recommendations that includes project definitions, timing, costs and staffing projections for each project that is to be included in the Roadmap.
- 2.7 **Project Management.** Verizon will designate a project manager who will act as the central point of contact throughout the Project. The project manager is also responsible for managing the change control process.
3. **DELIVERABLES.** Deliverables are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the Agreement's confidentiality terms. Deliverables include the SPA Report.

**FINANCIAL TERMS.** Customer will pay the Charge as detailed in the SOF. Travel and expenses, if any, will be billed as provided in the PSSA, this SOW, and the SOF.