**STATEMENT OF WORK**

**CONNECTIONS II**

**Order Identification Number: [######]**

**Operations, Administration and Management (OA&M)**

**Support for the [Agency] Network Enterprise**

**Issued by:**

**[Agency Logo]**

**[Name of Agency]**

**[Address of Agency]**

**DATE: [DD MM YYYY]**

About this SOW Template

This Statement of Work (SOW) Template has been provided by GSA to help customer Agencies contract for communications and networking solutions at the Local Area Network (LAN), building, campus, and enterprise level on the Connections II contract. The template is designed as a guide for developing a SOW and contains an example statement of work and requirements that can be readily tailored to meet Agency procurement needs.

At a minimum, the SOW must include the description and quantity of supplies and equipment to be delivered and/or supported, the staffing needs to be provided, and support to be performed as well as the evaluation criteria upon which the evaluation will be based.

Context boxes in this template contain informational material or instructions that should be deleted by the Agency when finalizing this document.

* **BLUE context boxes** such as this one contain informational material, no action required.
* **YELLOW context boxes** contain instructions, or suggested requirement language/narratives and possible options the Agency may choose to include or discard when developing the SOW requirements.
* **ORANGE Text** indicates placeholders where Agency provides a numeric value (e.g. n for number of days, or number of pages) or replaces text with its own Agency name, etc.

In most instances, a context box describes what requirements should be captured or included in a section; it may have a brief Q&A to guide the Agency in describing to the offeror the desired solution including products/equipment and staffing or support the agency intends to obtain.

Sections of this SOW template may be deleted if they are not relevant to the SOW, and new sections may be added to meet the agency’s specific needs.

The text “*DRAFT SOW TEMPLATE”* watermark and the references in the page footers should also be removed for the final copy.

REMOVE THIS PAGE WHEN FINAL DRAFT IS GENERATED

**Table of Contents**

[1 Project Description 5](#_Toc410910368)

[1.1 Project Title 5](#_Toc410910369)

[1.2 Purpose 5](#_Toc410910370)

[1.3 Background 5](#_Toc410910371)

[1.3.1 Organization and Mission 5](#_Toc410910372)

[1.4 Objectives 6](#_Toc410910373)

[1.5 Scope 7](#_Toc410910374)

[1.5.1 General Description of Requirements 8](#_Toc410910375)

[1.5.2 Existing Communications and Network Infrastructure 9](#_Toc410910376)

[1.5.3 Anticipated Limitations and Constraints 10](#_Toc410910377)

[1.6 Acquisition Selected 10](#_Toc410910378)

[1.7 Period of Performance 10](#_Toc410910379)

[1.8 Place of Performance/Hours of Operation 11](#_Toc410910380)

[1.9 Fair Opportunity 12](#_Toc410910381)

[1.10 Regulatory Requirements and Compliance Guidelines 12](#_Toc410910382)

[1.10.1.1 Regulatory Requirements 12](#_Toc410910383)

[1.10.1.2 Compliance Guidelines 12](#_Toc410910384)

[2 Statement of Work 12](#_Toc410910385)

[2.1 Task 1: Program Management and General Requirements 14](#_Toc410910386)

[2.1.1 Sub-task 1: General Roles and Responsibilities 15](#_Toc410910387)

[2.1.2 Sub-task 2: Project Management Planning and Implementation 16](#_Toc410910388)

[2.1.3 Sub-task 4: Network Management Information System (MIS) Dashboard 17](#_Toc410910389)

[2.1.4 Sub-task 5: Training 17](#_Toc410910390)

[2.1.5 Sub-task 6: Reporting and Communication Plan 17](#_Toc410910391)

[2.2 Task 2: Network Operations Center (NOC) Support 18](#_Toc410910392)

[2.2.1 Network Support Environment To Be Provided 19](#_Toc410910393)

[2.2.2 Sub-task 1: Day-to-Day Network Management 20](#_Toc410910394)

[2.2.3 Sub-task 2: Change Management 21](#_Toc410910395)

[2.2.4 Sub-task 3: Configuration Management 22](#_Toc410910396)

[2.2.4.1 Configuration Management Roles and Responsibilities 22](#_Toc410910397)

[2.2.4.2 Configuration Management System (CMS) 23](#_Toc410910398)

[2.2.5 Sub-task 4: Incident Management 24](#_Toc410910399)

[2.2.6 Sub-task 5: Outage Notification (Scheduled and Unscheduled) 24](#_Toc410910400)

[2.2.6.1 Scheduled Maintenance and Provisioning Support 26](#_Toc410910401)

[2.2.6.2 Trouble Reporting and Escalation 26](#_Toc410910402)

[2.3 Task 3: Security Operations Center (SOC) Support 27](#_Toc410910403)

[2.3.1 Sub-task 1: Access Control 29](#_Toc410910404)

[2.3.2 Sub-Task 2: Managed Firewall 32](#_Toc410910405)

[2.3.3 Sub-Task 3: Intrusion Detection and Prevention 34](#_Toc410910406)

[2.3.4 Sub-Task 4: Vulnerability Scanning 36](#_Toc410910407)

[2.3.5 Sub-Task 5: Anti-Virus Management 39](#_Toc410910408)

[2.3.6 Sub-Task 6: Incident Response 41](#_Toc410910409)

[2.4 Other Network OA&M Logistical Support 43](#_Toc410910410)

[2.4.1 Sub-task 1: Support for [Agency] Internal Billing Process 43](#_Toc410910411)

[2.4.2 Sub-task 2: Inventory Management Support 44](#_Toc410910412)

[2.4.2.1 Hardware and Software Inventory 44](#_Toc410910413)

[2.4.2.2 Agreements and User Licenses 44](#_Toc410910414)

[2.4.3 Sub-task 3: Support by Service Locations and Site Classification 45](#_Toc410910415)

[2.4.4 Sub-task 4: Support for Site Survey 46](#_Toc410910416)

[3 Staffing and Personnel Requirements 47](#_Toc410910417)

[3.1 Labor Types 47](#_Toc410910418)

[3.2 Personnel Requirements 47](#_Toc410910419)

[3.2.1 Contractor Personnel Security Requirements 48](#_Toc410910420)

[3.2.2 Special Qualifications and Certifications 49](#_Toc410910421)

[4 Travel and Other Direct Costs (ODC) / (Un-priced Items) 49](#_Toc410910422)

[4.1 Travel 49](#_Toc410910423)

[4.2 Other Direct Cost (ODC )/ Un-priced Items 50](#_Toc410910424)

[5 Materials, Equipment and Facilities 50](#_Toc410910425)

[5.1 Equipment Warranty and Inventory, and Supply Chain Risk Management (SCRM) 50](#_Toc410910426)

[5.2 Government-Furnished Property 51](#_Toc410910427)

[5.2.1.1 Government Furnished Equipment (GFE) 51](#_Toc410910428)

[5.2.1.2 Government Furnished Information (GFI) 51](#_Toc410910429)

[5.3 Contractor-Furnished 51](#_Toc410910430)

[5.3.1.1 Contractor Furnished Equipment (CFE) 51](#_Toc410910431)

[5.3.1.2 Contractor Furnished Items (CFI) 52](#_Toc410910432)

[5.4 Facilities 52](#_Toc410910433)

[5.4.1.1 Contractor Facilities 52](#_Toc410910434)

[5.4.1.2 Government Facilities 52](#_Toc410910435)

[5.4.1.3 Incidental Construction 53](#_Toc410910436)

[6 Invoice Requirements 53](#_Toc410910437)

[6.1 Detail Billing Requirements 53](#_Toc410910438)

[6.2 Invoice Address, Data Format and Delivery Method 53](#_Toc410910439)

[6.2.1 Invoice Address 53](#_Toc410910440)

[6.2.2 Invoice Submission 54](#_Toc410910441)

[6.2.3 Billing Cycle and Data Elements 54](#_Toc410910442)

[6.2.4 Electronic Funds Transfer (EFT) 55](#_Toc410910443)

[6.3 Billing for Other Direct Costs (ODCs) or Unpriced Item 55](#_Toc410910444)

[6.3.1 Invoice for Travel Expenses 56](#_Toc410910445)

[7 Electronic and Information Technology Accessibility Standards (Section 508) 57](#_Toc410910446)

[8 Proposal Instructions 57](#_Toc410910447)

[8.1 Solicitation Closing Date and Time 57](#_Toc410910448)

[8.2 Preparation and Delivery Instructions 58](#_Toc410910449)

[8.3 Price Proposal 59](#_Toc410910450)

[8.4 Technical/Management Proposal 60](#_Toc410910451)

[8.5 Appendices 61](#_Toc410910452)

[9 Evaluation Factors and Basis for Award 63](#_Toc410910453)

[9.1 Evaluation Methodology and Basis for Award 63](#_Toc410910454)

[9.2 Evaluation Approach – Trade Off or LPTA 64](#_Toc410910455)

[9.3 Technical Evaluation Criteria 65](#_Toc410910456)

[9.4 Price Evaluation Criteria 70](#_Toc410910457)

[10 Task Order Award 71](#_Toc410910458)

[11 Organizational Conflicts of Interest 71](#_Toc410910459)

[12 Acronyms and Glossary of Terms 72](#_Toc410910460)

[12.1 Acronyms and Definition 72](#_Toc410910461)

[12.2 Glossary of Terms 72](#_Toc410910462)

[13 Attachments 74](#_Toc410910463)

[13.1 Attachment A – Program Management Plan 74](#_Toc410910464)

[13.2 Attachment B – Support Locations 74](#_Toc410910465)

[13.3 Attachment C – Pricing Instructions 74](#_Toc410910466)

[13.4 Attachment D – Pricing Template 74](#_Toc410910467)

[13.1 Attachment E – Equipment Support, Warranty and Inventory 74](#_Toc410910468)

[13.2 Attachment F – Past Performance Worksheet 75](#_Toc410910469)

[13.3 Attachment G – Task Order Deliverables Performance Matrix 75](#_Toc410910470)

[13.4 Attachment H – Current Network Architecture and Service Environment 75](#_Toc410910471)

# Project Description

This is the [Agency] Statement of Work for the following task(s) utilizing the General Services Administration’s Connections II contract:

## Project Title

**Operations, Administration, and Management (OA&M) Support for the [Agency’s] Network Enterprise**

## Purpose

The [Agency] has requirements for more efficient and proactive ways to manage its increasingly large network enterprise, while ensuring the stability, security and speed needed to support mission-critical operations and other business functions.

The purpose of this Statement of Work (SOW) is to acquire support for [Name of Agency’s network systems]. The [Agency] has the need to outsource the operations, administration and management (OA&M) of the Agency’s IP-centric network enterprise and shift the responsibilities to the Connections II offeror, thereby allowing the Agency to focus on its core mission. The OA&M support includes running the day-to-day management and operations of the network enterprise.

## Background

To provide background information relevant to this SOW, this section should include at a minimum the following subsection.

### Organization and Mission

This is where the Agency provides brief description of its organization and mission.

[Add Agency-specific information here]

## Objectives

This section is where the Agency may provide additional justification and benefits of outsourcing the management of network infrastructure support and equipment.

Why OA&M for Networks?

Effectively managing networking and communications equipment (including Voice over Internet Protocol (VoIP) requires tools, resources and expertise that may not be available in-house. Agencies must first determine whether their need to support infrastructure would be best managed in-house or by a support contractor.

The objectives in this SOW can be contained within the full array of operations, administration and management (OA&M) of network infrastructure support and associated equipment offered under the Connections II contract or customized to meet Agency-specific needs.

The objective is for the Agency to leverage industry-leading resources and management capabilities for a secure and reliable network which may include OA&M for complex voice, data, and video communication systems.

The objective of this SOW is to provide network OA&M support, including any associated equipment and equipment support, for the management and monitoring of the [Agency] network enterprise. The offeror assumes responsibility for the operations and maintenance of [Agency] legacy systems and [other Agency data infrastructure, systems, and applications]. To achieve this objective, the offeror must have the required operations, maintenance, and customer support functions in place to meet [Agency] contract requirements.

The network OA&M support will help the Agency achieve cost-effective operations and administration of its own network infrastructure, provide predictable equipment and personnel-related costs, reduce operating and maintenance costs, and minimize expenses and unscheduled outages that can arise from unexpected network incidents and complex managed network problems. The offeror will not be providing telecommunications services between locations, but can assist in coordinating those services.

## Scope

**OA&M for Networks** allows the Agency to leverage industry-leading resources and management capabilities available from the Connections II contract contractors for secure and reliable network operations.

This scope may include multiple tasks to design, develop, acquire, deliver, transition, integrate, configure, test, validate, monitor, document, support, enhance, refresh, upgrade, fit-up and sustain the Agency's network. Depending upon the Agency's business needs and funding, the scope may include support for:

* Network intelligence and insight into the [Agency]’s own network communications systems including assistance with troubleshooting, network planning, network optimization, tracking and control of inventory of telecommunication equipment and assets, service ordering, billing analysis/verification and monitoring of service performance.
* Opportunity for the [Agency] to leverage for new technologies as they become available while having more control over operational costs, allow its own in-house IT staff to focus on core business tasks, maximize technology performance, uptime and availability of its network services.
* A fully managed communications platform such that all hardware, software, and equipment will be managed and maintained by the Connections II offeror.

The **SCOPE** section should briefly describe the scope (products and support) that the agency intends to obtain under this task order.

The scope specifies the volume of coverage or support needed based upon support locations, size and population of users per location, network platforms to be supported, desired quantity of equipment, and payment terms for equipment support such as maintenance and warranty.

The OA&M SOW may cover end-end support for the operations, administration, and management (OA&M) of the Agency’s network enterprise, network security, performance monitoring, and general logistics management requirements. Depending upon the Agency needs, the scope may include all or a combination of the following:

1. Communications scope - includes all metropolitan and wide area networks at all [Agency] physical locations and presence including Internet Protocol (IP) and other networks.
2. Technical scope - includes management of all communications network equipment and all related network connectivity.
3. Agency-specific Logistics support to manage and maintain the Agency’s network enterprise such as:

* Integrated performance monitoring
* Configuration Management
* Fault Management
* Unscheduled and Scheduled Outage notification
* Network traffic analysis and reporting
* Other Agency-specific logistics for network support

If the Agency deletes a set of task(s) that do not apply to its SOW in Section 2.0 Statement of Work, then the Agency must also make the corresponding deletion in Section 9.3, Technical Evaluation Criteria.

Adequate staffing and personnel requirements including telecommunications subject matter experts (SMEs), technical specialists, network engineers, and other labor categories shall be provided to support in managing and maintaining the [Agency’s] network enterprise.

### General Description of Requirements

The Agency's telecommunications service provider is solely responsible for the management, performance, and maintenance of its services up to the demarcation point or network side. The [Agency] requires the offeror to provide in-house support to monitor its network enterprise including network troubleshooting, software distribution and updating, router and domain name management, performance monitoring, and coordination with affiliated networks. In addition, the [Agency] also has a need to be informed of planned and unplanned service outages impacting events so that proper action is taken as required.

The requirements for Network OA&M will shift the tasks and responsibility of managing the [Agency’s] network enterprise to the offeror as the managed service provider (MSP) and thereby enabling the Agency to achieve real-time visibility of its enterprise-wide network resources, network operations security, contract compliance and service performance.

Section 2.0, Statement of Work, provides details of the task requirements, required functional areas and support to be provided by the offeror including, but not limited to, the following support for:

Task 1: Program Management and General Requirements

Task 2: Network Operations Center (NOC) Support

Task 3: Security Operations Center (SOC) Support

Task 4: Integrated Performance Management

.

[Add Agency-specific information here]

### Existing Communications and Network Infrastructure

A diagram can be included as an Attachment H-1, Current Network Topology (an example diagram is provided in Attachment H-1).

**Scope of Infrastructure and Services to be Supported**

The following network components and topology of the Service Environment will be provided as Appendices under this SOW. The appendices will provide a comprehensive description of the scope of the network environment to be supported. The Service Environment Appendices are to be maintained and reviewed by the offeror with the [Agency] and made available to the [Agency] on a quarterly basis.

**Hardware and Software**

1. Network Hardware- A listing and description of all supported network hardware
2. Network Software - A listing and description of the supported network software and utilities
3. Network Circuits - A listing of supported network circuits
4. Network Topology - A listing of other data network topology appendices
5. Network Topology Diagram - A network topology diagram describing the supported network components
6. Site Topology Diagram - A site topology diagram describing the supported site components
7. Network Boundaries Topology - A network boundaries topology diagram describing the supported network boundaries
8. Network Low Level Design - A low level network design document describing the data center architecture, disaster recovery site, remote sites, and the security architecture

See ***Attachment H – Network Diagrams and Figures***.

[Add Agency-specific information here]

### Anticipated Limitations and Constraints

[Add Agency-specific information here]

## Acquisition Selected

The order type for the OA&M for Network OA&M SOW defaults to **Firm Fixed Price.**

The Agency has the option to specify a **Time and Materials** (T&M) type task order.

A **Time-and-Materials** task ordermay be used when it is not possible for the Agency at the time of placing the task order to estimate accurately the extent or duration of the work or to anticipate costs with any reasonable degree of confidence. (Federal Acquisition Regulation (FAR) 16.601(c) Time-and-materials contracts).

A time-and-materials task order provides for acquiring supplies or services on the basis of (1) Direct labor hours at specified fixed hourly rates that include wages, overhead, general and administrative expenses, and profit; and (2) Actual cost for materials (except as provided for in FAR 31.205-26(e) and (f)).

This is a ***Firm Fixed Price*** Task Order against the GSA Connections II Indefinite-Delivery, Indefinite-Quantity (IDIQ) Contract.

The offeror shall adhere to the terms and conditions specified in the Connections II Contract in addition to the support specific requirements in this solicitation. This SOW also contains additional or supplemental requirements to those defined in the Connections II contract.

## Period of Performance

The Tasks agreed upon by [Agency] and the offeror will remain in effect for the life of the Connections II Task Order. The offeror shall provide technical support and shall procure and install [or recommend] the equipment for these Tasks.

The term of the order will be from the date of award through a base period plus [n] option periods. The overall period of performance is specified in the following table.

**Table 1.7-1: Date of Task Order Award**

|  | **Start Date** | **End Date** |
| --- | --- | --- |
| Base Period | <<Performance\_Start\_Date>> | <<Performance\_End\_Date\_BasePeriod>> |
| Option Period 1 | <<Performance\_Start\_Date\_Option\_Period\_1>> | <<Performance\_End\_Date\_Option\_Period\_1>> |
| Option Period 2 | <<Performance\_Start\_Date\_Option\_Period\_2>> | <<Performance\_End\_Date\_Option\_Period\_2>> |
| Option Period 3 | <<Performance\_Start\_Date\_Option\_Period\_3>> | <<Performance\_End\_Date\_Option\_Period\_3>> |
| Option Period [n] | <<Performance\_Start\_Date\_Option\_Period\_4>> | <<Performance\_End\_Date\_Option\_Period\_4>> |

*Note: This table is for illustration purposes only. The Agency has the option to add or remove years as required. The Connections II contract was awarded in October 2011. It ends January 19, 2021. An order placed before January 19, 2021 can last until January 19, 2026.*

## Place of Performance/Hours of Operation

The offeror shall comply with the geographic requirements specified in this solicitation to provide the operations, administration, and management of the [Agency’s] network enterprise.

A description and location address of all Agency facility and office locations requiring OA&M support are provided in Attachment B – Support Locations.

Appendix B contains a column for hours of operation for each site. If all sites have common hours of operation or if hours of operation can otherwise be conveniently summarized (e.g., one set of hours for headquarters location, another of branch locations) then the Agency may choose to put that information here and delete the column in the Appendix. A full listing of all locations in two places, however, should be avoided.

Sizing for each location is expressed in terms of the number of users, as defined in Appendix B.

The offeror shall adhere to the hours of operation described herein. Any work performed after normal business hours will be allowed as necessary upon prior approval and coordination with the **[Agency] Contracting Officer’s Representative (COR)**.

## Fair Opportunity

This SOW will be released for Fair Opportunity under **FAR 16.505**.

## Regulatory Requirements and Compliance Guidelines

This is where the Agency should provide the general description of the compliance requirements, OMB directives, and general policy and guidelines that the offeror must stipulate compliance with, provide acknowledgement of, or must complete to meet the requirements stated herein.

The offeror shall review the following requirements and guidelines:

#### Regulatory Requirements

[Additional Agency-specific information can be inserted here]

#### Compliance Guidelines

[Additional Agency-specific information can be inserted here]

# Statement of Work

**A primer on Network OA&M solutions**

Network OA&M support provided by a Connections II offeror can take away much of the complexity that comes from managing all elements of the Agency’s network enterprise in-house.

The Network OA&M statement of work includes requirements for outsourced network OA&M solutions to help alleviate the business challenges and allow the Agency to focus on its core mission.

**Network OA&M** is a series of tasks, activities, processes and tools provided by the offeror for the lifecycle management and operations, including engineering support, for the following areas and components supporting the Agency’s network enterprise:

1. Operations and administration of converged network for voice, data, and multi-media services
2. Other Agency-specific communications and logistics support

The requirements in this section are suggestive and it is up to the agency to determine the most suitable life-cycle solution to meet its goals and objectives.

**Format and Structure of Network OA&M Requirements**

This section describes the technical requirements for the support services (labor), equipment, and equipment services that the agency intends to obtain.

* For standard or baseline requirements based on the Connections II contract, the Agency may simply identify the total number of staff and support personnel (labor categories), and if known, the quantity and types of equipment and devices needed to meet requirements.
* For complex requirements, the Agency may provide additional information or attach relevant documentation and diagrams (e.g., “As is” logical and physical network diagrams, endpoints/nodes, population or volume of users, technology platform currently in place).
* **Roles and Responsibilities**

Each task provides a brief summary of roles and responsibilities that identify the party that will be responsible for performing the task. The Agency has an inherent role to review, approve and provision the network services, including services that the offeror is required to support and manage. The Agency may acquire or source the underlying telecommunications services from another contract such as Networx. The Connections II offeror has a specific set of complementary roles and responsibilities for each task to meet and satisfy the requirements for delivering and supporting the network enterprise.

* **OA&M and General Requirements**

The OA&M for Network Support SOW Template provides sample boilerplate and general requirements for the offeror to provide technical skills and expertise (labor categories), associated equipment, and equipment service support for the Agency’s network enterprise and interworking systems including tasks required to design, develop, acquire, deliver, transition, integrate, configure, test, validate, monitor, document, support, enhance, refresh, upgrade, fit-up and sustain the Agency’s network.

This Statement of Work is composed of four (4) tasks, each containing sub-tasks and a list of requirements that the offeror is expected to meet.

The offeror shall provide the appropriate labor categories (skills and expertise), associated equipment, and equipment services to support and deliver a network OA&M solution agency-wide including support for network operations center (NOC) and security operations center (SOC) and integrated performance management.

In addition to the support services described for each task, the offeror shall also be responsible for providing the skills and expertise, any associated equipment and tools and other logistic support for the day to day operations and program management of the [Agency]’s network enterprise. The offeror shall propose other labor categories as appropriate to meet the requirements.

**Task and Sub-tasks List**

The list describes the full range of offeror support services, associated equipment, and equipment services required for Network OA&M, including the performance measures to be used to assess the quality and timely delivery of the following tasks:

* Task 1: Program Management and General Requirements
  + Sub-task 1 - General Roles and Responsibilities
  + Sub-task 2 - Project Management Planning and Implementation
  + Sub-task 3 - Day-to-Day Network Management
  + Sub-task 4 - Task Order Management and Online Tracking System
  + Sub-task 5 – Reporting and Other Communications
* Task 2: Network Operations Center (NOC) Support
  + Sub-task 1- Configuration Management
  + Sub-task 2- Fault Management
  + Sub-task 3- Trouble Tickets Handling
  + Sub-task 4- Accounting/Billing Management
  + Sub-task 5- Inventory Management
* Task 3: Security Operations Center (SOC) Support
  + Sub-Task 1 - Access Control
  + Sub-Task 2 - Managed Firewall
  + Sub-Task 3 - Intrusion Detection and Prevention
  + Sub-Task 4 - Vulnerability Scanning and Analysis
  + Sub-Task 5 - Anti-Virus Management
  + Sub-Task 6 - Incident Response
* Task 4: Integrated Performance Management
  + Sub-Task 1 - SLA Performance Reporting and Analysis

Sub-Task 2 - Tracking and Requesting SLA Credits

## Task 1: Program Management and General Requirements

The [Agency] recognizes that Program Management tasks are an essential component for successful contract management and establishment of an ongoing [Agency]-offeror relationship. The offeror shall provide adequate program management capabilities to operate and manage the [Agency’s] network operations center to the level of performance required by the Government. The offeror’s program management approach shall include strong governance over compliance, privacy and data security standards as well as meet the following goals:

* Deliver a program management solution that increases functionality and usability of the [Agency] network enterprise as new features and technologies become available
* Implement measures to reduce network infrastructure cost and risk
* Maintain robust security through regular, timely network software upgrades
* Establish best practices for easier migration to IP technologies such as unified communications

Network OA&M support encompasses program wide functional service areas that set forth the roles and responsibilities required under this task order. The offeror shall meet the Agency requirements for a complete end-to-end lifecycle management that apply to the provision, delivery and management of the [Agency] network enterprise to include support for network infrastructure, equipment, applications and affiliated systems.

### Sub-task 1: General Roles and Responsibilities

The following table identifies general program management roles and responsibilities associated with Task 1. An “X” is placed in the column under the Party that will be responsible for performing the task. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements.

**Table 2.1.1-1 – General Roles and Responsibilities**

| **General Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Provide support services (Labor Types), equipment, and equipment services supporting the processes for the [Agency]’s Network OA&M business needs, technical requirements, and other end user requirements in support of its enterprise telecommunications including networking systems, applications, and equipment. | **X** |  |
| 1. Approve Services and the supporting processes that support [Agency]’s Network OA&M requirements, make sure the offeror meets technical requirements and other end user requirements in support of Agency-wide telecommunications including voice, data, and video network, applications, and systems. |  | **X** |
| 1. Comply with [Agency] policies, guiding principles , standards and regulatory requirements applicable to [Agency] for information, information systems, personnel, physical and technical security | **X** |  |
| 1. Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to [Agency] for all Network OA&M projects and major Service activities | **X** |  |
| 1. Maintain and update a project management plan as changes are made to the project schedule, personnel resources, work load assignments, and other logistics supporting this project. | **X** |  |
| 1. [Add agency-specific roles and responsibilities here] | **X** |  |

### Sub-task 2: Project Management Planning and Implementation

The offeror shall establish and execute [or recommend] a Project Management Plan (PMP) to ensure that all activities from the kick-off meeting to the ongoing lifecycle management of network services are executed properly as planned and on schedule.

* + - 1. The offeror shall establish a Project Management (PM) function to provide management and operations support to the Agency and serve as a single point of contact for the Agency to manage and administer the Network OA&M solution.
      2. The offeror shall provide project management support that includes management and oversight of all activities performed by offeror personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work. The offeror shall identify a Project Manager (PM) by name, to provide management, direction, administration, quality assurance, and leadership for the execution of this task order. The PM will be the primary point of contact for all program activities.
      3. The offeror shall describe in the PMP proposed Labor Types for professional services, technical expertise, and administrative skills that fully meet the requirements in Tasks 1 to 9 to provide life cycle management for the network enterprise. This includes (as applicable): network management and monitoring, network security, performance, billing analysis, equipment inventory management, helpdesk support and equipment repair and maintenance.
      4. The PMP shall delineate the activities required to prepare and support the Network OA&M solution. The PMP shall capture and establish the SOW goals, identify a critical path, and create general timelines to support and implement appropriate operational procedures for the network enterprise. The PMP shall contain at a minimum:
  1. Project management approach for Tasks 1 thru 4.
  2. Project Team Organization (Roles & Responsibilities)
  3. Program Tracking and Communication Plan
  4. Project Schedules & Milestones
     + 1. The PMP shall describe the Connections II offeror’s role to perform, coordinate and act as systems integrator for third-party services including services any commercial vendor provide to the Agency.
       2. The PMP shall serve as a repository documenting the processes and methodology for meeting the requirements of each task described in this Statement of Work.
       3. The PMP shall be updated periodically for any changes to the program plans, activities, schedules, and any other related issues that may potentially impact the delivery and performance of the Network OA&M solution.
       4. An initial draft PMP shall be provided to the Government with the proposal. Upon award the Government will provide comments, which shall be incorporated into the final PMP. The offeror shall provide to the Agency both the draft and final document deliverables in MS Word format, and any required briefings/presentations in MS PowerPoint format.

### Sub-task 4: Network Management Information System (MIS) Dashboard

1. For requirements associated with Tasks 1 thru 4, the offeror shall develop and maintain a web-based online tracking and reporting system or dashboard [or similar reporting capabilities accessible by the Agency online and provided through the offeror’s web portal]. The self-service customer online portal or web-based reporting system shall provide the Agency access to documentation, reports and other information associated with the health and status of network service including but not limited to:

* Dynamic reporting capabilities, scorecards and monthly service level reports
* View and analyze asset inventory
* Track configuration, incident management and trouble tickets
* Manage and view Billing summary on a monthly. quarterly, or yearly basis
* Secure access to network issues, fault management, and status of incidents, and Move, Add, Change, or Disconnect (MACD) orders
* Manage performance reports, including network traffic and usage
* Track status of equipment repairs, warranty and EOL (end-of-life)

### Sub-task 5: Training

The offeror shall be responsible for all education and skills-based training necessary to ensure that all staff assigned to the project are qualified to perform the work. The offeror shall develop in-house orientation and training courses for contractor staff, the work to be performed, and the associated duties, responsibilities, security guidelines, policies, operating procedures, etc. The Agency will review these materials at the request of the offeror.

**Training of Contractor Staff**

1. The offeror shall be responsible for providing trained, experienced staff for performing the work ordered under this task order. The offeror shall make its best efforts to retain staff members who have gained experience on this contract, and to minimize staff turnover.
2. The offeror shall train its staff to ensure all personnel are able to perform their duties under each task order satisfactorily. Except where specifically approved by the COR, training of contractor staff is not separately billable. Specialized training requested by the COR beyond that which would normally be required to perform under the contract is billable.

### Sub-task 6: Reporting and Communication Plan

1. The offeror shall keep the Agency apprised of its activities on a regular basis. The Agency expects the offeror to be in daily or weekly contact via phone, email, or face-to-face with its Agency counterparts. The frequency of these contacts will change depending upon the workload, issues identified, etc.
2. The offeror shall provide a comprehensive calendar year end report, detailing workload, process change or other enhancements.
3. The offeror shall participate in daily operations teleconferences to provide statuses on the [Name of Project] and [Agency] systems. Teleconferences are generally less than an hour in duration. The offeror shall provide an update on its activities and discuss any achievements, problems, or future activities that may impact the workload.
4. The offeror shall provide ad hoc performance, workload, or other reports at the request of the Agency. These requests generally arise from external requests for information or special projects requiring data other than that normally provided to the Agency during the offeror’s normal reporting activities.

## Task 2: Network Operations Center (NOC) Support

**A primer on Network Operations Center (NOC)**

A network operations center (NOC) is a place from which administrators supervise, monitor and maintain a telecommunications network. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and domain name management, performance monitoring, and coordination with affiliated networks.

In most cases, the average or smaller Agency requires NOC support to be performed from the contractor-site. A large Agency may require NOC support at its own government-provided facility or an Agency site location. The Agency must be specific about where the NOC support will be performed, quantity of staffing personnel, and whether labor categories to be proposed will be off-site or on-site.

The Agency can revise the suggested requirements below for the scope of network services to be supported.

Network services and features to be supported may include but are not limited to:

* Wide Area Network (WAN) Services
* Local Area Network (LAN) Services
* Virtual Private Network (VPN) Services
* Quality of Service (QOS)
* Network Security Services

The list of network elements/component provided in in sub-section 2.2.1 is suggested requirements for the network services to be supported. The Agency may revise these requirements to meet their needs

As part of the transition to outsourced Network OA&M support, the offeror shall provide integrated support services, management and operations processes and a shared knowledge base that meet the requirements of the agency-wide Network OA&M solution.

Support to the Agency of network services shall include, but are not limited to, management of user accounts; configuration management; fault management; network operations center (NOC) management; installation support for moves, adds, and changes; and notification of outages. Support services for billing reconciliation, analysis and disputes shall also be performed.

### Network Support Environment to Be Provided

In addition to the NOC-specific roles and responsibilities described in each sub-task, the offeror shall be responsible for supporting the [Agency]’s converged network enterprise including all associated equipment, equipment services and peripheral activities (e.g. network transition, device migration, moves, adds, change disconnects (MACD), etc.).

The offeror shall work with public carriers and other [Agency] circuit providers on behalf of [Agency] to ensure delivery of WAN services.

The offeror responsibilities shall include, but are not limited to, the design/engineering, provisioning, management, administration and troubleshooting of the following networks and assets:

* **Wide Area Network (WAN) Services**

WAN services include the provision, monitoring, and management of voice and data networks that interconnect two or more separate facilities that span a geographic area larger than a campus or metropolitan area. Transmission facilities include, but are not limited to, dedicated Internet connections, Internet-based VPNs, Multi-Protocol Label Switching (MPLS), and dial-up connections.

* **Local Area Network (LAN) Services**

LAN services include the provision, monitoring, and management of networks that are usually confined to a single facility or portion of a facility. LAN components may include wired and wireless LANs supporting all network traffic originating from desktop devices, local file and print servers, application servers, database servers, peripherals, firewalls/routers, other network devices and other user premise devices.

* **Virtual Private Network (VPN) Services**

VPN services include the provision, monitoring, and management of methods for remote users and business partners to securely connect to the Network and Data Center Computing Services over the public Internet. This service includes dedicated site-to-site VPN connectivity on a shared public IP network. It requires industry/Internet-based standards for security to create and preserve privacy, data integrity, and authenticity.

* **Quality of Service**

Quality of service (QOS) is used to differentiate among traffic flows when congestion occurs, providing better performance for some traffic types while degrading the performance of others. QOS is often used for converged networks that must support real-time traffic, such as Voice over Internet Protocol (VoIP), simultaneously with transaction traffic and batch traffic.

* **Network Security Services**

Network Security Services include the provision and support of methods that provide security to physical and logical devices connected to the network. (See Section 2.3 Task 3 - Security Operations Center (SOC) Support for more detailed requirements).

### Sub-task 1: Day-to-Day Network Management

The offeror shall be responsible for day-to-day network management and operations support at the [Agency can specify the location for Network Operations Center (NOC and/or Security Operations Center (SOC) whether government site or offeror site], using offeror-provided network management, security management and monitoring systems. In addition, the offeror will be responsible for the delivery and support of all related customer premise configuration items including but not limited to network routers, Uninterruptible Power Supplies (UPS), firewalls, Intrusion Detection Prevention Systems (IDPS), the DSU/CSU (data service units/channel service units), and out-of-band modems.

The offeror shall provide the capability to provision, monitor, and troubleshoot the network enterprise for a large number of government users agency-wide on a continuous basis.

1. The [Agency] approved formal procedural, reporting and communication processes and structures shall be established to manage the delivery of the network services in an efficient and effective manner.
2. Day-to-day management processes shall be documented and maintained by the offeror, as approved by the [Agency], and modified and updated on an ongoing basis to reflect changes to the business and operational processes.
3. Offeror and the [Agency] will agree upon additional points of contact and a reporting structure covering day-to-day operations and reviews of the offeror’s performance.
4. These reviews shall include technical, financial, and service-level requirements reviews as well as the resolution of any contractual issues that may arise.
5. The reporting schedules shall be documented and maintained by the offeror in an online repository accessible to the [Agency]’s management team.
6. A regular meeting schedule shall be required for the different reporting levels established, with ongoing 24-hour access to all of offeror points of contact when required.

### Sub-task 2: Change Management

**Configuration Management vs. Change Management**

A Configuration Management system is primarily a version control system for the component or elements of a network enterprise. A Configuration Management plan documents how configuration management will be performed. It defines those items that are configurable, those that require formal change control, and the process for controlling changes to such items.

A Change Management System ensures that every change request is received, analyzed and either approved or rejected. If it is approved, all other project constraints will also be analyzed for any possible impact due to this change. Basically, the purpose of the Change Management System is to implement the approved changes into the project with a minimum of disruption.

**A Change Management Plan** is a generic plan that guides the Project Manager in terms of making any kind of change on the project, especially the ones that can impact the baselines (scope, time, cost baselines). A Change Management Plan documents how changes will be monitored and controlled and also defines the process for managing change on the project, whereas, a Configuration Management Plan provides guidance in making changes which are specific to the network component or hardware/software configuration..

The Agency may include additional requirements for the offeror to provide a configuration management plan and/or change management plan applicable to their SOW.

Change Management support services are activities that are performed by the offeror to ensure that standardized methods and procedures are being applied and observed for efficient and prompt handling of all changes, in order to minimize the impact of change upon network service quality and consequently to improve the day-to-day operations of the [Agency] network enterprise.

Change Management shall cover all aspects of managing the introduction and implementation of all changes affecting any network elements and components associated with the Agency] network enterprise and in any of the management processes, tools, and methodologies designed and utilized to support those components.

The [Agency] and/or [Agency] designated contractors shall have the option to create, add, delete, and modify agents, routing options, in-queue messages, and any other applications, components, systems, in “real time” and as deemed necessary by [Agency].

The offeror shall document how changes will be monitored and controlled and also defines the process for managing change on all network projects including, but not limited to, all planned and unplanned activities to the Agency's data network, the Agency defined configuration items (CIs), change requests and incidents and all of these activities must be synchronized and updated in real-time.

### Sub-task 3: Configuration Management

**Configuration Management Services** are the activities associated with providing a logical model of the Agency's enterprise network devices and their relationships in the network architecture and topology by identifying, controlling, maintaining and verifying installed hardware and software as well as maintaining current documentation of the network configuration (i.e. maintenance contracts, SLA documents, etc.).

The goal of configuration management is to account for all network assets and configurations; provide accurate information on configurations; and provide a solid base for Incident, Problem, Change and Release Management. Proper record-keeping and documentation must be maintained to verify configuration records against the infrastructure and to track and correct any exceptions.

The Configuration Management process is closely linked to the Change Management process.

The offeror shall be responsible for the creation and maintenance of the Configuration Management Database (CMDB). The offeror shall obtain approval for any changes to the network when such changes may result in an alteration to a tracked Configuration Item (CI). Such changes shall be documented and updated into the (CMDB).

Proper record-keeping and documentation shall be maintained at all times and the offeror shall account for all network assets and configurations to verify configuration records against the infrastructure and to track and correct any exceptions.

#### Configuration Management Roles and Responsibilities

The following table identifies the roles and responsibilities associated with Configuration Management under Task 2. An “X” is placed in the column under the party that will be responsible for performing the task. The offeror responsibilities are indicated in the column labeled “Offeror”. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements.

**Table 2.2.3.1-1 – Configuration Management Roles and Responsibilities**

| **Configuration Management Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Define Configuration Management requirements and policies |  | **X** |
| 1. Develop, document and maintain in the Standards Process and Procedures Manual Configuration Management procedures that meet requirements and adhere to defined policies | **X** |  |
| 1. Review and approve Configuration Management procedures and processes |  | **X** |
| 1. Identify and document the Configuration Item structure | **X** |  |
| 1. Approve the Configuration Item structure |  | **X** |
| 1. Establish Configuration Management database, in accordance with [Agency] requirements | **X** |  |
| 1. Review and approve Configuration Management database |  | **X** |
| 1. Select and purchase Configuration Management tools (Note: it is also possible that the Agency will require the offeror to provide contractor-provided CM tools] |  | **X** |
| 1. Install and maintain Configuration Management tools | **X** |  |
| 1. Enter/upload configuration data into configuration database | **X** |  |
| 1. Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and Asset Management processes | **X** |  |
| 1. Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing | **X** |  |
| 1. Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back-out of configuration items |  | **X** |
| 1. Develop procedures for establishing configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states | **X** |  |
| 1. Develop procedures for establishing security baselines as reference points for rebuilds, and provide ability to revert to stable configuration states |  | **X** |
| 1. Establish procedures for verifying the accuracy of configuration items, adherence to Configuration Management process and identifying process deficiencies | **X** |  |
| 1. Provide a deficiency report and steps taken to address the issues identified | **X** |  |
| 1. Provide [Agency] Configuration Management reports as required and defined by the [Agency] | **X** |  |
| 1. Audit Configuration Management process and accuracy of configuration data |  | **X** |
| [Additional agency-specific roles and responsibilities for configuration management] |  |  |

#### Configuration Management System (CMS)

The Agency has the option to require the offeror to provide a configuration management tool. If not required or applicable to the Agency’s SOW, then this sub-section can be removed.

Below are suggested requirements for the Configuration Management tool. The Agency may revise the requirements to meet their needs.

Configuration Management is a Version Control System for the product of a project. A Configuration Management plan documents how configuration management will be performed. It defines those items that are configurable, those that require formal change control, and the process for controlling changes to such items.

The offeror shall install and maintain a Configuration Management System (CMS) as required by the Agency. The CMS shall be a repository of all records and information pertaining to the installation, changes, and maintenance of the network enterprise systems. It shall contain a complete inventory, schematics, floor plans, equipment, circuits, etc. associated with each site location.

### Sub-task 4: Incident Management

Incident Management includes the activities associated with restoring normal service operation as quickly as possible and minimizing the adverse impact on business operations of [Agency], thus ensuring that the best possible levels of service quality and availability are maintained. While the Incident Management processes apply to Level 1, Level 2 and Level 3 support groups, Level 1 support, normally at the service desk, is responsible for primary ownership of recording and tracking the incident and is responsible for the close coordination and ongoing monitoring and tracking of, and reporting on, incidents that have been escalated to second-level and third-level support groups to ensure that escalated Incidents are resolved as promptly as possible.

The primary activities of Incident Management process include:

* Incident detection and recording
* Incident classification and initial support
* Incident investigation and diagnosis
* Incident escalation
* Incident resolution and recovery
* Incident closure

The offeror is responsible for escalating incidents and coordinating with all appropriate

Level 2 and Level 3 support groups to ensure knowledge capture and transfer regarding Incident Resolution procedures from the offeror’s Level 1 Service Desk to support the objective of increasing the first call resolution number of Incidents capable of being resolved by Level 1 service technicians.

Requirements that are specific to security incident management are described in Section 2.3 – Task 3 Security Operations Center (SOC) support, 2.3.6 Sub-task 6 – Incident Response.

### Sub-task 5: Outage Notification (Scheduled and Unscheduled)

**Scheduled Maintenance Outage**

The offeror shall promptly notify the [Agency] user community of all scheduled maintenance, deployment, and service order installation dates. A summary report of all installations scheduled for completion including all regular scheduled maintenance shall be communicated to the Agency users on a weekly or monthly basis. A follow-up email notification shall be sent to the user community within 24 hours as a reminder of any upcoming scheduled maintenance specifying the duration, start time, and end time that the network will be inaccessible.

**Unscheduled Outages**

In the event of unscheduled network outages, proactive management of distributed network trunk resources requires real-time notification and the ability to reach out to any trunk circuit in the [Agency]'s network enterprise and perform remote troubleshooting. The offeror shall maintain and keep current a list of Agency personnel to be contacted in the event of an unscheduled outage.  The Agency will provide the offeror with a list of personnel to be contacted in the event of an unscheduled outage at the Kickoff meeting.

The offeror shall promptly notify and provide a clear explanation of the unscheduled outage. The offeror shall communicate by email notification to all [Agency] users impacted with the outage a periodic status, severity and escalation level, and the remedy applied until the outage is restored. The offeror shall initiate, manage, and track trouble tickets of all and any unscheduled outages submitted to the Agency’s carrier or service provider.

**Service Level Agreements**

The offeror must have the ability to validate for the Agency that the carrier or service provider is providing the level of performance required by the Government. Strong governance over compliance, privacy, and security standards is required.

The offeror shall provide the necessary system and tools to track service performance of the network circuits including support services to enforce service level agreements (SLA):

1. Monitor and enforce Service Level Agreements. The offeror shall provide a network system tracking tool that provides comprehensive historical fault data that can be automatically summarized and distributed to provide monthly analysis of the service provider/carrier’s service performance.
2. The tool shall provide real-time health-and-status information for all monitored trunk circuits throughout the enterprise.
3. In the event of a fault indication, the offeror’s system and tools shall provide real-time troubleshooting information indicating whether problems are associated with the customer premise equipment (CPE) or the carrier.
4. The offeror shall immediately open a trouble ticket with the Agency’s service provider to report an unscheduled outage. The offeror shall track all such open trouble tickets until resolved. The offeror must be familiar with the service performance threshold to measure performance and ascertain the SLA is maintained at or above the acceptable quality level as agreed between the Agency and its service provider.
5. Unscheduled outages and the corresponding trouble tickets issued to the service provider must be reported to the Agency within [nn minutes or hours], with status reporting every [mm minutes or hours].

#### Scheduled Maintenance and Provisioning Support

Scheduled maintenance, upgrades, changes, and installs or any other activity affecting telecommunications equipment or software shall be performed after hours or on weekends at the Agency’s discretion. The offeror shall provide/host post stability conference bridges when required by the Agency.

The offeror shall supply to the Agency a scheduled maintenance plan which will include proactive activities to keep the network functioning at peak efficiency. The offeror shall ensure that any and all maintenance activities do not conflict with other scheduled initiatives or application testing/turn-ups.

#### Trouble Reporting and Escalation

[Agency] or the offeror shall have the ability to collect and centrally monitor major failures, alarms, outages and any other error conditions that could potentially threaten the availability of the Network operations.

The offeror shall clearly define each severity alarm type in order to provide the Agency with a clear explanation for assigning severity to alarms. For example, the offeror shall clearly identify what constitutes a Severity 1 alarm, Severity 2 alarm, etc. The offeror’s process for trouble and escalation procedures shall be documented and submitted in writing to the Agency within 30 days of contract award.

The offeror shall provide and clearly define escalation levels for the Agency to utilize in escalating troubles. These levels shall include contact names, numbers and clearly defined procedures for escalating a trouble within the offeror organization.

## Task 3: Security Operations Center (SOC) Support

**Primer on SOC:**

The Security Operations Center (SOC) enforces Agency specific security requirements for incoming/outgoing traffic and operational support systems. The security management operations 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 the Agency enterprise services, information, and operational support systems; and to prevent fraudulent use of network services.

Information security can be broadly categorized as (a) *access control* for protection from unauthorized access and modification of corporate database and (b) *cybersecurity* for protection of corporate database from cyber criminals (aka hackers). The SOC related activities are access control and cybersecurity; and, cybersecurity is further subdivided into managed firewall, intrusion detection and prevention, vulnerability scanning, anti-virus management, and incident response in accordance with Agency security policy; and, in particular the following related activities:

1. Sub-Task 1: Access Control
   1. Access control is the act of ensuring that an authenticated user accesses only what they are authorized to and no more. It includes authentication, authorization, access approval, and audit.
2. Sub-Task 2: Firewall
   1. Firewall inspects traffic according to a set of defined security policies, blocking all traffic not meeting the Agency’s criteria, such as white list and black list.
3. Sub-Task 3: Intrusion Detection and Prevention
   1. Detects signs of intrusion that may jeopardize the confidentiality, integrity, availability, and control of Agency networks. It provides intrusion sensors that analyze packet activity for indications of network attack, misuse, and anomalies, and then generates alerts and records suspicious events. The prvention consists of dropping or rerouting malicious packets.
4. Sub-Task 4: Vulnerability Scanning
   1. Searches (scans) for security holes, flaws, and exploits on Agency systems, networks, and applications for vulnerabilities by comparing scanned information against the vulnerability database. The vulneribity database is updated as new threats are discovered.
5. Sub-Task 5: Anti-Virus Management
   1. Detection and removal of system viruses. The system/tool scans executable files, boot blocks, and incoming traffic for malicious code.
6. Sub-Task 6: Incident Response
   1. Incident Response is composed of both proactive and reactive activities, as follows:
      1. Proactive activities are designed to prevent incidents. They include onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training.

**Primer on SOC: (Cont.)**

1. Reactive activities 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.

The offeror shall support and administer the Agency’s Security Operations Center (SOC). The Security Operations Center (SOC) enforces [Agency] specific security requirements for incoming/outgoing traffic and operational support systems. The security management operations 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 the [Agency] enterprise services, information, and operational support systems; and to prevent fraudulent use of network services.

The SOC-related activities are access control and cybersecurity; and, cybersecurity is further subdivided into managed firewall, intrusion detection and prevention, vulnerability scanning, anti-virus management, and incident response in accordance with [Agency] security policy

The support services (Labor Types) and associated equipment to be provided shall include planning and assessment, training, integration and testing; implementation and migration; documentation; and Operations and Maintenance of the [Agency] Security Operations Center (SOC).

### Sub-task 1: Access Control

**Primer on Access Control:**

Access Control ensures that an authenticated user can only access what they are authorized to and no more. A subject's access to an object depends on whether its identity credentials appear on the access control lists (ACL) associated with the object.

Access Control includes authorization, authentication, access approval, and audit. A more narrow definition of access control would cover only the access approval, whereby the system makes a decision to grant or reject an access request from an already authenticated subject, based on what the subject is authorized to access. Authentication methods include user-id and password, physical security device (such as RSA token and associated PIN for two-factor identification), and biometric identification (such as voice verification, a retinal scan, palm identification, and thumbprints). Access approval grants access during operations, by associating users with the resources that they are allowed to access, based on the authorization policy. Accountability and audit analyzes logs of users’ access to system resources.

Access approval to system resources (objects) in the Access Control 0

1. Mandatory Access Control
   1. Allows access based on least privileges, for example, security clearance of users and classification of data (as confidential, secret or top secret) are used as security labels to define the level of trust.
2. Discretionary Access Control
   1. Allows access to specific resources based on permissions, for example, a system administrator may create a hierarchy of files to be accessed based on certain permissions.
3. Role-Based Access Control
   1. Allows access based on the job title/function, for example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators. Can also be coupled with separation-of-duties to eliminate conflict-of-interest.
4. Rule-Based Access Control
   1. Allows access based on rule, for example, allows use of labs only during a certain time of the day.
5. Responsibility-Based Access control
   1. Allows access based on the responsibilities assigned to an actor or a business role

Access Control Implementation based on Agency Security Policy

1. Populate Access Control List for authentication
   1. Identification and Authentication by
      1. User-id and password
      2. Physical security *device*, such as PIV card or RSA token and associated PIN for two-factor identification
      3. Biometric identification, such as voice verification, retinal scan, palm identification, and thumbprints

**Primer on Access Control (Cont):**

* 1. Enforcement
     1. Perform Identification and Authentication for access control
     2. Deny access – for unsuccessful login attempts
     3. Lock session – for unsuccessful database access attempts
     4. Generate alarms – for logging, reporting, and handling of unsuccessful attempts
     5. Ensure password management with strong passwords and periodic passwords changes

1. Populate Access Control List for access approvals (relationship between subjects and objects)
   1. For Agency systems and resources
      1. Virtual Private Network (VPN) - on-net, remote access, guest access
      2. Wireless LAN
      3. Mobile Devices
      4. Email
      5. Corporate database– normal operation and during changes with lockout or least functionality
      6. Premises entry points – buildings and rooms
   2. Access Approvals for authenticated users by control classifications
      1. Mandatory Access Control - based on least privileges
      2. Discretionary Access Control - based on permissions
      3. Role-Based Access Control - based on job title/function
      4. Rule-Based Access Control - based on rule
      5. Responsibility-Based Access control - based on responsibilities
   3. Enforcement
      1. Perform Access Approvals to Agency systems for already authenticated users
      2. Generate system usage logs for audits and accounting
2. Audit and Accounting of security events
   1. Perform access monitoring, analysis, and reporting as needed
3. Security awareness training
   1. Security training – yearly and ad-hoc

The following table identifies the roles and responsibilities associated with Access Control under Task 3. An “X” is placed in the column under the Party that will be responsible for performing the task. The offeror responsibilities are indicated in the column labeled “Offeror”. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements.

**Table 2.3.1-1 – Access Control Roles and Responsibilities**

| **Access Control Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Develop Access Control implementation based on the [Agency] Security Policy | **X** |  |
| 1. Populate Access Control List for authentication 2. Identification and Authentication by    1. User-id and password    2. Physical security device, such as PIV card or RSA token and associated PIN for two-factor identification    3. Biometric identification, such as voice verification, retinal scan, palm identification, and thumbprints 3. Enforcement    1. Perform Identification and Authentication for access control    2. Deny access – for unsuccessful login attempts    3. Lock session – for unsuccessful database access attempts    4. Generate alarms – for logging, reporting, and handling of unsuccessful attempts    5. Ensure password management with strong passwords and periodic passwords changes | **X** |  |
| 1. Populate Access Control List for access approvals (relationship between subjects and objects) 2. For Agency systems and resources    1. Virtual Private Network (VPN) - on-net, remote access, guest access    2. Wireless LAN    3. Mobile Devices    4. Email    5. Corporate database – normal operation and during changes with lockout or least functionality    6. Premises entries – buildings and rooms 3. Access Approvals for authenticated users by control classifications    1. Mandatory Access Control - based on least privileges    2. Discretionary Access Control - based on permissions    3. Role-Based Access Control - based on job title/function    4. Rule-Based Access Control - based on rule    5. Responsibility-Based Access control - based on responsibilities 4. Enforcement    1. Perform Access Approvals to Agency systems for already authenticated users    2. Generate system usage logs for audits and accounting | **X** |  |
| 1. Audit and Accounting of security events 2. Perform access monitoring, analysis, and reporting as needed | **X** |  |
| 1. Security awareness training 2. Security training – yearly and ad-hoc | **X** |  |
| 1. Provide any required information for performing tasks |  | **X** |
| 1. Provide feedback and/or approve successful performance of tasks. |  | **X** |

### Sub-Task 2: Managed Firewall

**Primer on Managed Firewall:**

A Firewall inspects traffic according to a set of defined security policies, blocking all traffic not meeting the Agency’s criteria, such as white list and black list.

The Firewall (hardware and software) is configured to provide the following:

1. Implements firewall security policies according to the Agency’s needs
2. Detects suspicious activity and policy violations
3. Employs various protection techniques including but not limited to:
   1. Stateful Packet Inspection by which the firewall goes beyond just examining a packet’s source and destination, but also verifies its legitimacy.
   2. Network Address Translation (NAT) and Port Address Translation (PAT) to disguise internal IP addresses, shielding systems from the outside world, especially from malicious activity
4. Guards the Agency’s networks from attacks, including but not limited to:
   1. Denial of Service (DOS) assaults which flood the network with false requests, overwhelming servers and eventually causing them to crash
   2. 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
   3. 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
   4. SYN Flood attacks which clog connections and prevent legitimate session requests from being established
   5. Tear Drop attacks in which packet fragments are deliberately designed to disrupt proper packet reassembly at the receiving end
5. Blocks hostile Java applets, JavaScript, and ActiveX controls to guard against potentially unsafe code, cookies, and web bugs, as required
6. Firewall Load Balancing
   1. Distributes traffic across multiple firewalls, in order to minimize potential downtime caused by any single point of failure.

**2.3.2 Sub-task 2: Managed Firewall Roles and Responsibilities**

The following table identifies the roles and responsibilities associated with Managed Firewall under Task 3. An “X” is placed in the column under the Party that will be responsible for performing the task. The offeror responsibilities are indicated in the column labeled “Offeror”. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements.

**Table 2.3.2-1 – Managed Firewall Roles and Responsibilities**

| **Managed Firewall Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Implement firewall security policies according to the [Agency] needs | **X** |  |
| 1. Detect suspicious activity and policy violations | **X** |  |
| 1. Employ various protection techniques including but not limited to: 2. Stateful Packet Inspection by which the firewall goes beyond just examining a packet’s source and destination, but also verifies its legitimacy. 3. Network Address Translation (NAT) and Port Address Translation (PAT) to disguise internal IP addresses, shielding systems from the outside world, especially from malicious activity | **X** |  |
| 1. Guard the Agency’s networks from attacks, including but not limited to: 2. Denial of Service (DOS) assaults which flood the network with false requests, overwhelming servers and eventually causing them to crash 3. 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 4. 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 5. SYN Flood attacks which clog connections and prevent legitimate session requests from being established 6. Tear Drop attacks in which packet fragments are deliberately designed to disrupt proper packet reassembly at the receiving end | **X** |  |
| 1. Block hostile Java applets, JavaScript, and ActiveX controls to guard against potentially unsafe code, cookies, and web bugs, as required | **X** |  |
| 1. Firewall Load Balancing - Distribute traffic across multiple firewalls, in order to minimize potential downtime caused by any single point of failure. | **X** |  |
| 1. Provide any required information for performing tasks |  | **X** |
| 1. Provide feedback and/or approve successful performance of tasks. |  | **X** |

### Sub-Task 3: Intrusion Detection and Prevention

**Primer on Intrusion Detection and Prevention:**

Detects signs of intrusion that may jeopardize the confidentiality, integrity, availability, and control of Agency networks. It provides intrusion sensors that analyze packet activity for indications of network attack, misuse, and anomalies, and then generates alerts and records suspicious events. The prevention consists of dropping or rerouting malicious packets.

1. Provides intrusion detection software and hardware components to include sensors, tap, and switches, as applicable
2. Monitors Agency servers for security breaches and misuse while enforcing best industry practices, and Agency security policies
3. Detects precursor activities such as unauthorized network probes, sweeps, and scans that may indicate a potential attack
4. Performs anomaly detection in order to identify typical traffic trends and unusual behaviors that may indicate a potential attack
5. Performs signature-based detection and analyzes system activity for known attacks such as, but not limited to:
   1. Buffer Overflows
   2. Brute Force
   3. Denial of Service (DOS)
   4. Reconnaissance Efforts
6. Monitors 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
7. Automatically updates the signature sets in use as new signatures become available, including Agency-defined signatures in the signature database for increased security
8. Analyzes suspicious security alerts to determine the significance of an event and 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
9. Provides the Agency with access to severe alert information, which shall contain but not be limited to the following:
   1. Incident Description
   2. Incident Target
   3. Incident Origin
   4. Potential Incident Impacts
   5. Incident Remedies
   6. Incident Prevention Measures

**2.3.3 Sub-task 3: Intrusion Detection and Prevention Roles and Responsibilities**

The following table identifies the roles and responsibilities associated with Intrusion Detection and Prevention under Task 3. An “X” is placed in the column under the Party that will be responsible for performing the task. The offeror responsibilities are indicated in the column labeled “Offeror”. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements.

**Table 2.3.3-1 – Intrusion Detection and Prevention Roles and Responsibilities**

| **Intrusion Detection and Prevention Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Provide intrusion detection software and hardware components to include sensors, tap, and switches, as applicable | **X** |  |
| 1. Monitor [Agency] servers for security breaches and misuse while enforcing best industry practices, and [Agency] security policies | **X** |  |
| 1. Detect precursor activities such as unauthorized network probes, sweeps, and scans that may indicate a potential attack | **X** |  |
| 1. Perform anomaly detection in order to identify a typical traffic trends and unusual behaviors that may indicate a potential attack | **X** |  |
| 1. Perform signature-based detection and analyze system activity for known attacks such as, but not limited to: 2. Buffer Overflows 3. Brute Force 4. Denial of Service (DOS) 5. Reconnaissance Efforts | **X** |  |
| 1. 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 | **X** |  |
| 1. Automatically update the signature sets in use as new signatures become available, including [Agency] -defined signatures in the signature database for increased security | **X** |  |
| 1. Analyze suspicious security alerts to determine the significance of an event and 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 | **X** |  |
| 1. Provide the [Agency] with access to severe alert information, which shall contain but not be limited to the following: 2. Incident Description 3. Incident Target 4. Incident Origin 5. Potential Incident Impacts 6. Incident Remedies 7. Incident Prevention Measures | **X** |  |
| 1. Provide any required information for performing tasks |  | **X** |
| 1. Provide feedback and/or approve successful performance of tasks. |  | **X** |

### Sub-Task 4: Vulnerability Scanning

**Primer on Vulnerability Scanning:**

Searches for security holes, flaws, and exploits on Agency systems, networks and applications. The system performs external scans by remotely probing the Agency network for vulnerabilities that generally come from the outside; and internal scans which detect flaws originating from the inside. The system tests for vulnerabilities by comparing scanned information to data contained in the vulnerability database, which is updated as new threats are discovered.

1. Provides the Agency with non-destructive and non-intrusive vulnerability scans that will not crash the systems being analyzed, or disrupt Agency operations. The scans will not provoke a debilitating denial of service condition on the Agency system being probed.
2. Ensures that the scanning engine can be updated with new vulnerability information to maintain effectiveness.
3. Periodically probes networks, including operating systems and application software, for potential openings, security holes, and improper configuration.
4. Probes Agency systems for vulnerabilities in, but not limited to, the following areas as applicable:
   1. Backdoors
   2. Bind
   3. Browser
   4. Brute Force Attacks
   5. Common Graphic Interface - Binary (CGI-Bin)
   6. Daemons
   7. Distributed Component Object Model (DCOM)
   8. Databases
   9. Domain Name Service (DNS)
   10. eCommerce Applications
   11. Email
   12. Firewalls
   13. File Sharing
   14. File Transfer Protocol (FTP)
   15. General Remote Services
   16. Hardware and Network Appliances
   17. Hubs
   18. Information/Directory Services
   19. Instant Messaging
   20. Lightweight Directory Access Protocol (LDAP)
   21. Mail Applications
   22. Multimedia Internet Mail Extension (MIME)
   23. Network
   24. Network Sniffers
   25. Netbios
   26. Network File System (NFS)

**Primer on Vulnerability Scanning (Cont.):**

* 1. Network Information System (NIS)
  2. Port Scans
  3. Protocol Spoofing
  4. Router-Switch
  5. Remote Procedure Call (RPC)
  6. Shares
  7. Simple Mail Transfer Protocol (SMTP)
  8. Simple Network Management Protocol (SNMP)
  9. Server Message Block (SMB)
  10. Transmission Control Protocol/Internet Protocol (TCP/IP)
  11. Trojan Horses
  12. Web Scans
  13. Web Servers
  14. Wireless Access Points
  15. X-Windows

1. Notifies the Agency of vulnerabilities discovered via email, fax, or telephone, as directed by the Agency.
2. Proposes appropriate countermeasures, fixes, patches, and workarounds for identified vulnerabilities to the Agency

**2.3.4 Sub-task 4: Vulnerability Scanning Roles and Responsibilities**

The following table identifies the roles and responsibilities associated with Vulnerability Scanning under Task 3. An “X” is placed in the column under the Party that will be responsible for performing the task. The offeror responsibilities are indicated in the column labeled “Offeror”. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements.

**Table 2.3.4-1 – Vulnerability Scanning Roles and Responsibilities**

| **Vulnerability Scanning Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Provide the Agency with non-destructive and non-intrusive vulnerability scanning capability 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. | **X** |  |
| 1. Ensure that the scanning engine can be updated with new vulnerabilities information in order to maintain effectiveness | **X** |  |
| 1. Scanning engine will periodically probe networks, including operating systems and application software, for potential openings, security holes, and improper configuration | **X** |  |
| 1. Probe Agency systems for vulnerabilities in, but not limited to, the following areas as applicable: 2. Backdoors 3. Bind 4. Browser 5. Brute Force Attacks 6. Common Graphic Interface - Binary (CGI-Bin) 7. Daemons 8. Distributed Component Object Model (DCOM) 9. Databases 10. Domain Name Service (DNS) 11. eCommerce Applications 12. Email 13. Firewalls 14. File Sharing 15. File Transfer Protocol (FTP) 16. General Remote Services 17. Hardware and Network Appliances 18. Hubs 19. Information/Directory Services 20. Instant Messaging 21. Lightweight Directory Access Protocol (LDAP) 22. Mail Applications 23. Multimedia Internet Mail Extension (MIME) 24. Network 25. Network Sniffers 26. Netbios 27. Network File System (NFS) 28. Network Information System (NIS) 29. Port Scans 30. Protocol Spoofing 31. Router-Switch 32. Remote Procedure Call (RPC) 33. Shares 34. Simple Mail Transfer Protocol (SMTP) 35. Simple Network Management Protocol (SNMP) 36. Server Message Block (SMB) 37. Transmission Control Protocol/Internet Protocol (TCP/IP) 38. Trojan Horses 39. Web Scans 40. Web Servers 41. Wireless Access Points 42. X-Windows | **X** |  |
| 1. Notify the Agency of vulnerabilities discovered via email, fax, or telephone, as directed by the [Agency] | **X** |  |
| 1. Propose appropriate countermeasures, fixes, patches, and workarounds for identified vulnerabilities to the [Agency] | **X** |  |
| 1. Provide any required information for performing tasks |  | **X** |
| 1. Provide feedback and/or approve successful performance of tasks. |  | **X** |

### 

### Sub-Task 5: Anti-Virus Management

**Primer on Anti-Virus Management:**

Provides the most current anti-virus software and tools for detection and removal of system viruses. The system will scan executable files, boot blocks, and incoming traffic for malicious code. The system will monitor traffic for malicious content, and will complement the anti-virus software already implemented on Agency desktops.

1. Provides design and implementation (software and hardware components) to determine the appropriate anti-virus solution suited to Agency needs in order to support
   1. Scanning of web and email traffic for worms, viruses, and malicious content in
      1. Incoming and outgoing FTP, HTTP, POP, and SMTP traffic for possible infection, including HTTPS traffic for the server-based application.
   2. Scanning of all files and software housed on a specific server, including the operating system
2. The system will perform data integrity checks and, at a minimum, will protect against the following:
   1. Known viruses
   2. Behaviors and patterns that may indicate the presence of viruses
   3. Malicious mobile code
   4. Different strains of polymorphic viruses
   5. Viruses in compressed files, as required by the Agency
   6. Viruses in different languages (e.g., JAVA, ActiveX, Visual Basic)
   7. Trojan horses and worms
   8. Macro viruses
3. The system will respond to infections and violations of the Agency networking environment and provide the following:
   1. Alerts
      1. Systems/Network Administrator notification via email, fax, or telephone, as directed by the Agency’s notification procedures
      2. Sender and recipient notification, in case of email-borne virus
   2. Isolation of infected file for cleaning, deletion, or post alert analysis and interpretation.
   3. Control of user access and environment for the malicious file
4. Provides access to logs:
   1. Infections detected
   2. Malicious emails
   3. Rule violations
   4. Traffic/mail statistics

**2.3.5 Sub-task 5: Anti-Virus Management Roles and Responsibilities**

The following table identifies the roles and responsibilities associated with Anti-Virus Management under Task 3. An “X” is placed in the column under the Party that will be responsible for performing the task. The offeror responsibilities are indicated in the column labeled “Offeror”. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements.

**Table 2.3.5-1 – Anti-Virus Management Roles and Responsibilities**

| **Anti-Virus Management Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Provide design and implementation (software and hardware components) to determine the appropriate anti-virus solution suited to [Agency] needs in order to support 2. Scanning of web and email traffic for worms, viruses, and malicious content in    1. Incoming and outgoing FTP, HTTP, POP, and SMTP traffic for possible infection, including HTTPS traffic for the server-based application. 3. Scanning of all files and software housed on a specific server, including the operating system | **X** |  |
| 1. Perform data integrity checks and, at a minimum, shall protect against the following: 2. Known viruses 3. Behaviors and patterns that may indicate the presence of viruses 4. Malicious mobile code 5. Different strains of polymorphic viruses 6. Viruses in compressed files, as required by the Agency 7. Viruses in different languages (e.g., JAVA, ActiveX, Visual Basic) 8. Trojan horses and worms 9. Macro viruses | **X** |  |
| 1. Respond to infections and violations of the [Agency] networking environment and provide the following: 2. Alerts    1. Systems/Network Administrator notification via email, fax, or telephone, as directed by the [Agency]’s notification procedures    2. Sender and recipient notification, in case of email-borne virus 3. Isolation of infected file for cleaning, deletion, or post alert analysis and interpretation. 4. Control of user access and environment for the malicious file | **X** |  |
| 1. Provide access to logs: 2. Infections detected 3. Malicious emails 4. Rule violations 5. Traffic/mail statistics | **X** |  |
| 1. Provide any required information for performing tasks |  | **X** |
| 1. Provide feedback and/or approve successful performance of tasks. |  | **X** |

### 

### Sub-Task 6: Incident Response

**Primer on Incident Response:**

Incident Response is composed of both proactive and reactive activities, as follows:

1. Proactive activities are conducted to prevent incidents. They include onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training.
2. Reactive activities 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.

Incident Response provides an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks. In addition, Incident Response provides forensics analysis that can assist in apprehending and prosecuting offenders.

1. Reviews the Agency’s security infrastructure to develop the appropriate strategic plans in collaboration with the Agency. These plans will detail
   1. Incident response process,
   2. Identify internal resources,
   3. Assign duties to team members,
   4. Describe policies,
   5. define severity levels,
   6. List escalation chains, and
   7. Specify emergency/recovery procedures.
2. Provides support for
   1. Effective incident response support on a 24x7 basis
   2. Provide incident analysis and assessment in order to determine the scope and impact of incidents
   3. Coordinate with the Agency to handle potential security incidents according to the appropriate response procedures
   4. Provide countermeasures to contain the security incident, limit its spread, and protect internal systems
   5. Recommend the fixes necessary to eliminate identified vulnerabilities, and the appropriate procedures to guard against future attacks
   6. Assist the Agency in containing the damage and restoring affected systems to their normal operational state
   7. Assist the Agency in testing restored systems in order to ensure that identified vulnerabilities have been corrected
   8. Provide dedicated cybersecurity SME support until resolution of the problem
   9. Provide post-incident investigative and forensics analysis. This includes
      1. Isolating the impacted area,
      2. Capturing and collecting data,
      3. Categorizing malicious or illegal events,
      4. Performing reconstruction analyses.
      5. 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.
      6. Trace the offenders and assist in prosecuting attackers, as required
   10. Provide security awareness training to Agency personnel as required.
       1. This includes mock attack drills, emerging threats and vulnerabilities workshops, and new incident response tools and processes demonstrations

**2.3.6 Sub-task 6: Incident Response Roles and Responsibilities**

The following table identifies the roles and responsibilities associated with Incident Response under Task 3. An “X” is placed in the column under the Party that will be responsible for performing the task. The offeror responsibilities are indicated in the column labeled “Offeror”. For the roles and responsibilities indicated in the column labeled “Offeror”, the offeror shall perform, provide support, and meet the requirements. “Agency” role and responsibility includes providing information, if required, for performing the task and providing feed-back and/or approving the successful performance of the requirement.

**Table 2.3.6-1 – Incident Response Roles and Responsibilities**

| **Incident Response Roles and Responsibilities** | **Offeror** | **Agency** |
| --- | --- | --- |
| 1. Review the [Agency]’s security infrastructure and develop the appropriate strategic plans in collaboration with the [Agency]. These plans shall detail 2. Incident response process, 3. Identify internal resources, 4. Assign duties to team members, 5. Describe policies, 6. define severity levels, 7. List escalation chains, and 8. Specify emergency/recovery procedures | **X** |  |
| 1. Provide support for 2. Effective incident response support on a 24x7 basis 3. Provide incident analysis and assessment in order to determine the scope and impact of incidents 4. Coordinate with the [Agency] to handle potential security incidents according to the appropriate response procedures 5. Provide countermeasures to contain the security incident, limit its spread, and protect internal systems 6. Recommend the fixes necessary to eliminate identified vulnerabilities, and the appropriate procedures to guard against future attacks 7. Assist the [Agency] in containing the damage and restoring affected systems to their normal operational state 8. Assist the [Agency] in testing restored systems in order to ensure that identified vulnerabilities have been corrected 9. Provide dedicated cybersecurity SME support until resolution of the problem 10. Provide post-incident investigative and forensics analysis. This includes     1. Isolating the impacted area,     2. Capturing and collecting data,     3. Categorizing malicious or illegal events,     4. Performing reconstruction analyses     5. 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.     6. Trace the offenders and assist in prosecuting attackers, as required 11. Provide security awareness training to [Agency] personnel as required.     1. This includes mock attack drills, emerging threats and vulnerabilities workshops, and new incident response tools and processes demonstrations | **X** |  |
| 1. Provide any required information for performing tasks |  | **X** |
| 1. Provide feedback and/or approve successful performance of tasks. |  | **X** |

## Other Network OA&M Logistical Support

### Sub-task 1: Support for [Agency] Internal Billing Process

Some Agencies may have a need for the offeror to support in analyzing and sorting through complex monthly billing files, performing invoice verification, and validating completed orders against the charges on the invoice. The task may include analyzing inventory (active services vs. disconnects) and tracking notices or status of in-flight orders (e.g. service order confirmation notices).

The suggested requirements below can be revised or modified to meet Agency-specific requirements to support billing, invoice verification, and inventory validation.

The Agency will be utilizing the [Centralized or Direct] billing method for its network services. The offeror shall provide experienced personnel with billing expertise and the necessary tools and equipment to support and administer internal billing processes including the management and maintenance of the [Agency]’s internal billing system.

1. The offeror shall provide support for billing analysis, invoice verification, billing disputes and other billing management and logistic functions associated with data and network assets of the [Agency]’s network enterprise that are administered under this Task Order.
2. The offeror shall review billing data to ensure the charges are correct, perform inventory analysis (e.g. active services vs. disconnects), and track acknowledgements and notices for status of in-flight orders (e.g. service order confirmation notices for new, changed or cancelled orders, etc.).
3. The offeror shall help and assist the Agency in resolving billing disputes with the [Agency]’s service provider, including performing billing data queries for analysis, identifying billing discrepancy, submitting billing disputes, and tracking issues until resolution.

### Sub-task 2: Inventory Management Support

The offeror shall track all networking and peripheral equipment supporting the network. The offeror’s tracking report shall describe where equipment is installed or stored at all times as a part of its inventory management responsibilities. This shall include the creation and ongoing maintenance of an inventory database that is readily accessible to the offeror’s authorized users and [Agency] personnel as needed. The offeror shall provide electronic access to [Agency] inventory data so that the inventory can be reviewed at any time by the Agency.

The offeror shall maintain an inventory of all equipment including but not limited to end-of-life (EOL) status, warranty, manufacturer, model number, and other information to keep track of networking equipment and assets that are actively billed and charged to the Agency.

A sample template is provided in ***Attachment E – Equipment Support, Warranty and Inventory***.

#### Hardware and Software Inventory

The network service environment described in the appendices is to be maintained by the offeror. The offeror shall regularly provide a status report on the state and condition of hardware and software components, including risk mitigation for equipment approaching EOL (End of Life). The report shall be made available to the [Agency] on a [quarterly or semi-annual] basis.

The following Attachments specify the Agency-specific hardware, software applications and other relevant materials containing details of the Agency’s Voice Network environment.

1. A listing and description of all hardware to be supported is provided in ***Attachment H.1- Network Hardware.***
2. A listing and description of the software and utilities to be supported is provided in ***Attachment H.2 – Network Software.***
3. A listing and description of the Network circuits to be supported is provided in ***Attachment H.3 – Network Circuits Database.***
4. A listing and description of the data sets and applications to be supported are provided in ***Attachment H.4 - Applications and Data Sets.***

#### Agreements and User Licenses

The offeror shall maintain a list of Network-related agreements and licenses. The offeror shall review and identify redundant and overlapping licensing and provide a summary report including recommendations of actions the Agency should undertake to minimize the cost of maintaining any redundant licenses and overlaps. A list is provided in ***Appendix K – Network Software Licenses.***

### 

### Sub-task 3: Support by Service Locations and Site Classification

**Site Classification**

The cost and complexity of managing the Agency’s data network enterprise is directly proportional to the size and classification of site locations that will be supported.

A site represents a physical location (i.e. one physical address). The site locations identified in this SOW are classified based on:

* The criticality of the site (i.e. Routine or Critical); and
* The total population or number of Agency customer agencies at a site (i.e. Single or Multi-Tenant).

**Routine Site**

A typical routine site will be configured with a single network access, single edge router, a single plain old telephone service (POTS) line and a modem for out-of-band management, and an UPS to meet the site availability requirement. A routine site with less than or equal to twenty (20) users, considered a small office, may be a viable candidate for site-to-site VPN configuration.

1. Optional Site-to-Site VPN - a small office may be configured with a secure private communications link over the public network infrastructure (I.e. Managed IP VPN Broadband service). Each Small Office must have the capability to establish connectivity to a primary and alternate Hub in the event of an outage. Each site will be sized in accordance to customer agency bandwidth requirements.
2. Routine Enhanced Site (with Optional Backup Communication) – Network based VPN service will also be considered as a viable Backup Communication for routine sites requesting alternate access in the event of network access outage.

**Critical Site**

A typical critical site will be configured with dual network access using diverse physical circuits and paths to the building; two edge router devices with load sharing; a POTS line and a modem for out-of-band management and an UPS to meet the site availability requirement. The routers will be configured to meet failover requirements.

* The customer may require diverse physical paths for circuits at critical sites with separate entry points to the building or a single path.
* The offeror shall ensure each site is connected to the network using highly survivable technology. This connectivity shall provide, at a minimum, two distinct paths to the Customer

**Single Tenant Site**

Physical Locations (i.e. buildings) having one customer agency on premises are deemed single tenant sites. A single tenant site will be configured to provide network access to a single customer agency Local Area Network (LAN). Each site will be sized in accordance to the customer agency bandwidth requirements. Customer facilities may already be equipped with UPS devices.

**Site Classification (Cont)**

**Multi-Tenant Site**

A multi-tenant site will be configured to provide logical separation between agencies and provide shared network access to multiple agency Local Area Networks. Each site will be sized in accordance to the aggregate customer agency bandwidth requirements. Each agency will be guaranteed a minimum bandwidth with the capability to utilize excess bandwidth not used by other agencies.

The Agency may add customized requirements in this section to meet their needs for network management at a single or multiple sites.

[Agency] Facilities to be supported

As development phases of various [Agency] network systems and applications are installed and completed, contractor personnel maybe be deployed to support geographically dispersed [Agency] office locations in the U.S. The offeror shall provide adequate staffing resources to support the implementation activities based upon site classification (e.g. size and service level). A listing of [Agency] office locations is provided in Appendix B - Support Locations.

As a Managed Service Provider (MSP) of the [Agency], the offeror shall deliver Network OA&M solutions at designated Agency locations utilizing the Agency’s existing and new infrastructures, as well as provide personnel, applications and tools.

A description and address of all [Agency] facility and office locations requiring Network OA&M services is provided in ***Attachment B – Support Locations***.

**Hours of Operations**

The Contractor Service Desk shall handle all changes on behalf of the Agency. The Agency hours of operation are from [7:00 a.m. to 7:00 p.m. EST, Monday-Friday], and on-call after-hours and weekends. The Contractor Service Desk shall handle all incidents on behalf of the Agency and coordinate all activities within their NOC, SOC, and third-party suppliers. The Contractor Service Desk hours of operation are 24 hours, seven days a week, including all federal holidays.

### Sub-task 4: Support for Site Survey

Upon task order award, the offeror shall perform site surveys. Prior to conducting any site surveys, the offeror must prepare and submit for Government approval a standardized “site survey checklist” that provides a comprehensive list of the information that the offeror intends to collect during site surveys.

At a minimum, site survey checklists must identify site preparation work, space requirements and any other related issues, and any specific assistance that will be required from the Government prior to implementing new systems and upgrades to existing systems, and deploying support services personnel at designated locations.

As ordered by the Government, the offeror must coordinate and conduct site surveys at domestic Government facilities to collect the information identified on the Government-approved checklist. During the site survey, the offeror must address any preliminary data gathering (e.g., existing numbering plans, equipment locations, space and workstations for key offeror personnel, etc.) and coordination activities necessary to ensure the successful completion of the planned implementation activities.

The offeror shall document the outcome of the site surveys in a Site Survey Report. A consolidated Site Survey report must be delivered to document the results of all site surveys conducted at campus locations.

# Staffing and Personnel Requirements

This is where the Agency provides staffing requirements and labor types needed in support of the operation, administration, and management of the Agency’s network enterprise.

The requirement under this solicitation seeks the support and expertise from Connections II contractors to provide adequate staffing to meet the requirements for the operations, administration, and management of the Agency’s network enterprise for the life of the task order.

## Labor Types

The offeror shall provide Labor Types for both professional and technical expertise that fully meet the requirements of all tasks in support of the solutions specified in this SOW, including full life cycle management as applicable, and the analysis, planning, design, specification, implementation, integration and management of required services and equipment.

## Personnel Requirements

The offeror has ultimate responsibility for managing the tasks, for achieving the performance results in each of the task areas, and for determining the appropriate staffing pattern in support of its technical approach.

* + - 1. The offeror shall provide experienced personnel to perform the required services. The Government and the offeror understand and agree that the services to be delivered are non-personal services.
      2. Offeror personnel shall conform to standards of conduct and codes of ethics, which are consistent with those applicable to Government employees. Offeror personnel shall obtain authorization to have access to Agency support sites and Government facilities, and shall obtain Common Access Cards (CAC) for computer access.
      3. All offeror employees must be fluent in spoken and written English.
      4. Background Checks: All contractor employees must submit a Questionnaire for National Security Positions (SF-86) to the [Agency] Personnel Security Manager. A favorable SF-86 is required before gaining access to a U.S. Government LAN. The offeror, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the order.
      5. The contracting officer may require the offeror to remove from the job site any offeror employee who is identified as a potential threat to the health, safety, security, general well-being or operational mission of the installation and its population.
      6. In order to ensure a smooth and orderly startup of work, it is essential that the key personnel specified in the offeror's proposal be available on the effective date of the order. If these personnel are not made available at that time, the offeror must notify the contracting officer and show cause. If the offeror does not show cause, the offeror may be subject to default action.
      7. The offeror-supplied personnel are employees of the offeror and under the administrative control and supervision of the offeror. The offeror, through its personnel, shall perform the tasks prescribed herein. The offeror must select, supervise, and exercise control and direction over its employees (including subcontractors) under this order. The Government shall not exercise any supervision or control over the offeror in its performance of contractual services under this order. The offeror is accountable to the Government for the actions of its personnel.

A description of qualifications, skills, and education level for the proposed staffing and personnel requirements is provided in section J.1 of the Connections II contract. The offeror shall propose additional skills and labor categories as needed to meet the requirements.

### Contractor Personnel Security Requirements

1. The Government may require security clearances for performance of this contract. The offeror must obtain these clearances before beginning work on the contract (Agency will not allow contractor employees without clearance in any of its facilities). The offeror must obtain these clearances by using the eQIP system. If satisfactory security arrangements cannot be made with the offeror, the required services must be obtained from other sources.
2. The level of classified access required will be indicated on a **DD-254** or other appropriate form incorporated into each request requiring access to classified information. Contractors are required to have background investigations for suitability if they occupy positions of trust (e.g., systems administration) even if they do NOT have access to classified information.
3. Necessary facility and/or staff clearances must be in place prior to start of work on the contract
4. Offerors are responsible for the security, integrity and appropriate authorized use of their systems interfacing with the Government and or used for the transaction of any and all Government business. The Government, through the Government's Contracting Officer, may require the use or modification of security and/or secure communications technologies related to Government systems access and use.
5. The Government, at its discretion, may suspend or terminate the access and/or use of any or all Government access and systems for conducting business with any/or all contractors when a security or other electronic access, use or misuse issue gives cause for such action. The suspension or termination may last until such time as the Government determines that the situation has been corrected or no longer exists.

A description of qualifications, skills, and education level for the proposed staffing and personnel requirements is provided in **Attachment C – Labor Types** for a List of Technical and Professional support services.

### Special Qualifications and Certifications

The offeror shall ensure that its employees have all required professional certifications and licenses (current and valid) for each applicable task and labor type category before commencement of work.

The offeror’s personnel shall meet the minimum qualifications and certifications and education level as summarized and identified in section J.1 of the Connections II contract**.**

[Agency may add Agency-specific requirements here]

# Travel and Other Direct Costs (ODC) / (Un-priced Items)

## Travel

The offeror shall comply with the Travel and Per Diem requirements as described in Section G.5.1.2 of the Connections II contract including conditions and limitations applying to travel associated with work performed under this SOW.

**Local Vicinity**: If travel within the local vicinity is required, travel reimbursements for local travel are not authorized; neither is the use of a Government vehicle.

**Distance Travel**: If travel outside the local vicinity is required, costs incurred by offeror personnel for travel, including costs of lodging, other subsistence, and incidental expenses, shall be considered reasonable and allowable only to the extent that they do not exceed the rates and amounts set by the Federal Travel Regulations. See **FAR 31.205-46(a) (2)(i)**.

As part of the Price Proposal, the offeror shall provide any anticipated travel costs, to include origination, destination, and the number of trips, number of persons, and a breakdown of lodging, meals, transportation and related costs.

Prior written approval by the [Agency] contracting officer is required for all travel directly and identifiably funded by the [Agency] under this order. The offeror shall therefore present to the contracting officer an itinerary for each planned trip, showing the name of the traveler, purpose of the trip, origin/destination (and intervening stops), and dates of travel, as far in advance of the proposed travel as possible, but in no event less than three weeks before travel is planned to commence.

For cost effectiveness, economy class travel must be used on all official travel funded under this Task Order. Business class travel should only be used under exceptional circumstances, and in compliance with the Federal Travel Regulations (**FAR 31.205-46**).

## Other Direct Cost (ODC)/ Un-priced Items

Other direct costs proposed (e.g. travel, per diem, etc.), which are considered necessary for the completion of the work, shall provide sufficient information to establish the basis for the estimate of such cost.

The offeror shall provide a breakdown for un-priced items and/or Other Direct Costs (ODCs) in the Price Proposal. The breakdown shall identify any “open market” items. ***Attachment E – Equipment Support, Warranty and Inventory*** is provided for the offeror to store and track equipment records by the task order number. The [Agency] may also task the offeror to store additional information in this file.

# Materials, Equipment and Facilities

The offeror shall meet and comply with the baseline general requirements for the management, maintenance, and handling of equipment and equipment services as described in **Section C.2.1 General Requirements** of the Connections II contract.

## Equipment Warranty and Inventory, and Supply Chain Risk Management (SCRM)

Agency-specific requirements for equipment and facilities may be provided for each individual task. In addition, the offeror shall:

* Comply with **Section C.2.1.9: Warranty Service** of the Connections II contract to provide, at no additional cost to the Government, a minimum one-year system warranty, or the warranty provided by the Original Equipment Manufacturer (OEM) whichever is longer, for all hardware and software purchased under this order.
* Comply with **Section C.3.6: Inventory Management** of the Connections II contract to establish and maintain an Inventory File of equipment, equipment warranty, and maintenance services purchased under each of the Tasks. Each record of this file shall include the OEM’s name and contact number, the maintenance offeror’s name and local repair number, the date of acceptance, the date maintenance was performed (if available), a description of the maintenance action (if available), and the date that the warranty ends.
* Comply with **Section C.3.3 Supply Chain Risk Management (SCRM)** of the Connections II contract to create a trackable and traceable supply chain, utilizing qualified equipment vendors and suppliers, verifying genuine ICT (Info and Communication Technology) products to ensure such products are not counterfeit or illegally modified. The offeror shall also employ proper labeling of remanufactured or repaired products and verify valid licenses are documented for these products.

***Attachment E – Equipment Support, Warranty and Inventory*** is provided for the offeror to store and track equipment records by the task order number. The [Agency] may also task the offeror to store additional information in this file.

## Government-Furnished Property

Government Furnished Property (GFP), which includes Government Furnished Material (GFM), Government Furnished Information (GFI), and Government Furnished Equipment (GFE), may be provided and shall be identified in the individual task order. The offeror shall be responsible for conducting all necessary examinations, inspections, maintenance, and tests upon receipt.

#### Government Furnished Equipment (GFE)

Upon the award and placement of each task order, Government Furnished Equipment (GFE) may be made available by the [Agency] for use by the offeror to support the tasks. The offeror shall use GFE to provide support services as mutually agreed upon by the offeror and Agency. The offeror shall evaluate all equipment as the Agency directs.

[Agency may add Agency-specific requirements here]

#### Government Furnished Information (GFI)

Site floor plans, specifications, and references will be provided by the COTR. Site drawings, cable run sheets and complete technical documentation generated by the offeror, as well as documentation that was provided to the offeror by the COR or technical Point of Contact, shall be delivered NLT thirty (30) work days to [Agency]’s POC following the completion of the project.

[Agency may add Agency-specific requirements here]

## Contractor-Furnished

#### Contractor Furnished Equipment (CFE)

All material and equipment identified on the network design package to accomplish this task will be furnished by the offeror. The offeror will purchase, ship, move, store, inventory, and handle installation material that is identified as CFE. Excess materials and prescribed spares shall be turned over to the COR at the completion of the project. Material turned over at the completion of the project shall be thoroughly documented including description, part numbers, and quantities.

[Agency may add Agency-specific requirements here]

#### Contractor Furnished Items (CFI)

The offeror shall identify in its proposal any items to be furnished during the performance of this task order.

The offeror shall provide all equipment and labor necessary to deploy the Network OA&M solution into operational status and ready to provide telecom service to end users. The offeror shall provide documentation for design, detailed design drawings, softswitch and gateway configuration(s), network topology, training materials including web-based training, support hotline telephone number and e-mail/website, and completion of task letter signed off on by Agency COTR.

## Facilities

This section may be removed if the requirements under this sub-section do not apply to this SOW.

#### Contractor Facilities

Except for those items and services specifically stated above in Section 5.3.1.2 as Government-Furnished, the offeror shall furnish everything needed to perform this Contract according to all its terms and conditions as stated in specific sections of this SOW. Such property includes, but is not limited to, facilities, equipment, material, supplies, repair parts, vehicles, data processing equipment, safety clothing, identification system camera and badges, and timekeeping system and facilities.

[Agency may add Agency-specific requirements here]

#### Government Facilities

To the extent it is available and is technically adequate, government facilities shall be used within the Government buildings and is support locations identified by the Agency in ***Appendix C – Support Locations***.

Where offeror equipment is required at the site, the Government will provide space, power, heating, ventilation and air conditioning (HVAC). To the extent that uninterrupted AC power is available and required, it shall be provided to the offeror by the Government. Government furnished equipment (GFE) may be used to satisfy this requirement if it is available.

[Agency may add Agency-specific requirements here]

#### Incidental Construction

Requirements for incidental and non-severable construction may be removed if it does not apply to this SOW.

Agency may add incidental and non-severable construction requirements here specific to their needs to support the solution.

[Agency may add Agency-specific requirements here]

# Invoice Requirements

The offeror shall meet and comply with the Billing and Invoice requirements as described in **Sections C.3.4 Billing, G.5.1 General Billing Requirements, and G.6 Payment of Bills** of the Connections II contract. The baseline requirements for Connections II contract for Invoicing and Billing including the handling of Associated Government Fee, approval for payment of supplies/services, resolution of billing disputes, and the option for Agency to pay by electronic funds transfer shall apply.

## Detail Billing Requirements

The offeror shall comply with the detailed billing requirements defined in **Section C.3.4** and the general billing requirements in **Section G.5** of the Connections II contract when submitting a proper bill for each order.

## Invoice Address, Data Format and Delivery Method

The offeror shall be capable of directly billing each customer at the address given by the Agency in the order and shall also have the capability to centrally bill designated customers through GSA. The baseline requirements for direct and centralized billing as defined **Section C.3.4** of the Connections II contract shall apply.

### Invoice Address

The offeror shall send invoices directly to the address (electronic mail or postal/physical address) designated by the Agency’s authorized Ordering Entity. This address will be determined at the time the order is placed.

**Remove this context box when finalizing the SOW**

Agency has two options how to receive invoice whether by electronic (email method) or to require hard copies. Or both. Suggested Requirements:

The offeror shall provide the signed original invoice via email:

[Agency provide an email here]

The offeror shall also provide via postal/physical address an additional copy of the invoice to the Contracting Officer and COR or provide [n] copies of the signed original to:

Name of Agency Department

POC Name/Position and Title

Email

Mailing Address

Street, City, Zip

Inquiries regarding payment of invoices should be directed to [Agency provide an email here]

### Invoice Submission

The offeror shall comply with the detail billing requirements defined in Section C.3.4 and the general billing requirements in Section G.5 of the Connections II contract when submitting a proper bill for each order.

A proper invoice must include the following items:

1. Contractor name and address

2. Contractor representative

3. Contract number

4. Order number(s)

5. Accounting Control Transaction (ACT) number (assigned by the OCO on the order)

6. Period of performance (month services performed for work request orders, month

deliverable completed for fixed price orders)

7. Bill number

8. Customer’s name and address

9. For Fixed Price Orders, products delivered and accepted, listed by deliverable number;

for Time and Materials orders, labor charges accepted during the period of performance

10. Travel and per diem charges

11. Total billed amount

12. Prompt payment discount offered (if applicable)

### Billing Cycle and Data Elements

The offeror shall invoice on a monthly basis.  The invoice shall include the period of performance covered by the invoice. The labor categories with total labor hours incurred for the period and other direct costs shall be reported on the invoice and shall be calculated for the current billing month. A Year-to-date total from project inception to date shall also be provided.  If subcontracting is proposed, one consolidated invoice from the prime contractor shall be submitted in accordance with other terms and conditions of the RFQ.

**Remove this context box when finalizing the SOW**

Agency has option to specify the format and agency-specific data elements for invoice content.

Suggested Requirements:

The offeror shall provide the invoice data in spreadsheet form with the following detailed information.  The listing shall include separate columns and totals for the current invoice period and the project to date. The following data elements shall be provided on the Invoice, at a minimum:

1. Labor Type (Contractor Employee)
2. CONNECTIONS II labor category
3. Monthly and total cumulative hours worked
4. Burdened hourly labor rate
5. Cost incurred not billed

### Electronic Funds Transfer (EFT)

**Remove this context box when finalizing the SOW**

Agency has option to specify the method of delivery for invoice and payments.

Insert additional agency-specific requirements here.

Below is a standard ‘boilerplate” requirements for EFT.

The offeror shall cooperate with the government to allow payment of bills via Electronic Funds Transfer (EFT) to the extent feasible in accordance with **Section G.6.3 Use of Electronic Funds Transfer** of the Connections II contract.

## Billing for Other Direct Costs (ODCs) or Unpriced Item

The offeror may invoice monthly on the basis of cost incurred for ODC or unpriced item.  The invoice shall include the period of performance covered by the invoice and the item number and title.

**Remove this context box when finalizing the SOW**

Agency has option to specify the format and agency-specific data elements for ODC and unpriced items.

Suggested Requirements:

The offeror shall provide the following detailed information for each invoice submitted, as applicable.  Spreadsheet submissions, in MS Excel format, are required.

1. ODCs or unpriced items purchased
2. Date delivery accepted by the Government
3. ODC or unpriced item number
4. Project to date totals
5. Cost incurred not billed
6. Remaining balance of each item

### Invoice for Travel Expenses

The offeror may invoice monthly on the basis of cost incurred for cost of travel comparable with the Joint Travel Regulations/Federal Travel Regulation (JTR/FTR).  Long distance travel is defined as travel over 50 miles.  The invoice shall include the period of performance covered by the invoice, and the CLIN number and title.  Separate worksheets, in MS Excel format, shall be submitted for travel.

**Remove this context box when finalizing the SOW**

Agency has option to specify the format and agency-specific data elements for submitting Travel charges. Suggested Requirements:

The offeror shall provide the following detailed information for each invoice submitted for travel expenses. The Total Cost for Travel shall identify all current travel on the project and their total CLIN/Task costs billed.  The listing shall include separate columns and totals for the current invoice period and the project to date:

1. Travel Authorization Request identifier, approver name, and approval date
2. Current invoice period
3. Names of persons traveling
4. Number of travel days
5. Dates of travel
6. Number of days per diem charged
7. Per diem rate used
8. Total per diem charged
9. Transportation costs (rental car, air fare, etc.)

**Remove this context box when finalizing the SOW (Cont.)**

1. Total charges
2. Explanation of variances exceeding 10% of the approved versus actual costs
3. Indirect Handling Rate.

[Agency may add Agency-specific billing and invoice payment processing requirements here]

# Electronic and Information Technology Accessibility Standards (Section 508)

All Electronic and Information Technology (EIT) procured through this task order must meet the applicable accessibility standards at 36 CFR 1194, unless an Agency exception to this requirement exists. The Section 508 Standards Summary is viewable at: <https://www.section508.gov/index.cfm?fuseAction=stdsSum#technical>

The offeror shall indicate for each line item in the schedule whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the proposal must indicate where full details of compliance can be found (e.g., the offeror's website or other exact location).

# Proposal Instructions

Connections II offerors are expected to review, understand, and comply with all aspects of this Statement of Work. All proposals received by the closing date and time will be evaluated in accordance with the Evaluation Criteria in **Section 9.0: Evaluation Factors and Basis for Award**.

Questions and clarifications concerning this solicitation shall be submitted in writing via email to: [name and email address], no later than [Q&A Closing Date (MM/DD/YYYY)].

## Solicitation Closing Date and Time

All proposals received by the deadline will be reviewed for responsiveness to the specifications outlined in these guidelines and the proposal format. Proposals which are submitted late or are incomplete run the risk of not being considered in the review process.

The proposals should be prepared according to the structural format set forth below. Proposals must be received at the place designated and by the due date specified herein, and must be considered valid for a period of [120] calendar days from the solicitation closing date.

PROPOSALS MUST BE RECEIVED ON OR BEFORE [3:00 PM EDT] ON <<RFP\_Closing\_Date>>.

Any proposal received by the [Agency] after the due date and time will not be considered.

## Preparation and Delivery Instructions

The Proposal shall be delivered to:

Provide the following:

POC Name/Title

Email

Phone

Additional instructions how proposals are to be submitted or delivered

The offeror’s proposal shall consist of individually titled separate volumes. Proposals shall be submitted in three separate volumes as shown below:

| **VOLUME** | **VOLUME TITLE** | **FORMAT** | **PAGE LIMITATIONS** |
| --- | --- | --- | --- |
| **Vol. I** | **PRICE PROPOSAL** | **EXCEL** | **No page limit** |
| **Vol. II** | **TECHNICAL/MANAGEMENT PROPOSAL**   * **Technical approach** * **Management approach** | **PDF** | **[n] maximum number of pages** |
| **Vol. III** | **APPENDICES**   * **Project Management Plan (PMP)** * **Past Performance** * **Proposed Personnel** | **PDF** | **[n] maximum number of pages** |

The table above is an example that may be tailored based on Agency requirements.

The following requirements apply to volumes 2 and 3. Volume 1 (Price) must comply with the instructions found within the attached MS Excel workbook.

1. **FORMAT.** All materials shall be in typeface Times New Roman 11 point (or Arial 11 point), on 8-1/2 x 11” formatted pages with one inch margins all around. Tables and illustrations may use reduced font style but not less than 8-point. All material submitted may be single-spaced. **Each page must provide identification of the submitting offeror in the heading or footer.**
2. **MATERIALS SUBMITTED.** The offeror is advised that all submissions and related material become the property of the U.S. Government and will not be returned. The technical and price proposals, if accepted by the Government, will form binding parts of the task orders that results from this solicitation. Therefore, care must be taken to properly address the requirements set forth in this solicitation.
3. **PROPRIETARY DATA.** Each and every page of the offeror’s proposals must be reviewed and marked as to proprietary data content by the offeror in strict compliance with **FAR 52.215-1**. Also see **FAR 3.104-4**. A single blanket statement at the front of the proposal is not acceptable. Failure to mark every page will subject your proposal to public release through Freedom of Information Act (FOIA) requests.

## Price Proposal

The offeror shall submit its Price Proposal in the form of an MS Excel Workbook included as ***Attachment D – Pricing Template***. The Price Model is used to facilitate the delivery of prices in the required format. In populating all Excel worksheets, the offeror shall present the data (e.g., item number, unit prices, quantities, and summarized prices) in a manner where all computations can be traced to the maximum extent possible. The offeror may add rows, columns, or worksheets to accommodate the required pricing information.

The offeror must assemble a project team with the required knowledge and experience as described in **section 3**. Pricing for each type of labor shall be proposed in all 4 price types. Proposed Labor Types for each Task shall include the Labor Type description, work location type, business day type, clearance status, and minimum educational qualifications and years of work experience. The Proposed Labor Types for each Task shall be provided in ***Attachment D – Pricing Template.***

For each Labor Types proposed, the offeror shall provide fully loaded hourly labor pricing based on the following price types:

1. Hourly Onsite (on government premises), Normal Business Day
2. Hourly Offsite (on contractor premises), Normal Business Day
3. Hourly Top Secret - TS/SCI, Onsite, Normal Business Day
4. Hourly Top Secret - TS/SCI, Offsite, Normal Business Day

The technical support services required at the government-site are described and identified in ***Attachment B – Support Locations.*** Work locations are defined as Government or offeror sites:

* + - 1. **Government site**: The offeror shall provide technical support and equipment when required to the locations identified in ***Attachment B – Support Locations***.
      2. **Offeror site:** The offeror shall provide network and security operations support and monitoring when required, and this work may be performed at the offeror’s NOC and SOC, respectively.

Failure by the offeror to use the prescribed pricing template may result in non-compliance. The Price Proposal must be submitted under separate cover from the Technical Proposal. While there is no page limit for the Price Proposal, the offeror must provide the necessary detail and supporting information to address the solicitation requirements and to allow a complete analysis of each line item price.

## Technical/Management Proposal

The **Volume II Technical/Management Proposal** shall include the technical approach and management approach as described below. Technical/Management Proposals are limited to [n] pages in length and shall be written in English. Each page must be numbered consecutively. Pages that exceed the page number limitation will not be evaluated.

Any page in the Technical/Management Proposal that contains a table, chart, graph, etc., not otherwise specifically excluded below, is included within the above page limitation for the Technical Proposal. Not included in the page limitation are the following:

* Cover/title page
* Table of contents

The offeror must organize its response in the Technical/Management Proposal to contain the following.

**Executive Summary** (5-page size limit)

The Executive Summary shall summarize the key elements of the offeror’s strategy, approach, methodologies, personnel and implementation plan. The Executive Summary must not exceed 5 pages in length.

**Technical Approach**

The Technical Approach must demonstrate a clear understanding of the requirements and include a description of the overall approach and strategy (i.e., implementation plan, testing methodology and risk mitigation strategy) being proposed. The Technical Approach shall include a detailed description of the offeror’s technical solution for each task including the associated equipment, equipment services, labor, and installation, and addressing each paragraph and subparagraph of Section 2.0: Statement of Work. If the offeror simply restates the requirements in Section 2.0 of this solicitation, the offeror’s proposal will be removed from consideration for award.

The Technical Approach shall be organized by the technical evaluation criteria for “Factor 1 – Technical Approach” listed in **Section 9.3** and shall meet and comply with all requirements in this SOW. Marketing literature is not acceptable. The offeror must stipulate that it has read, understands and will meet the Government’s requirements.

**Management Approach**

The offeror’s Management Approach shall provide a summary of the draft Project Management Plan (see instructions for Appendices) and the rationale behind the selected organization and staff chosen. The plan shall also demonstrate that the offeror has the corporate capabilities to execute the submitted PMP.

* **Organizational Structure and Chart**

The proposal shall include the offeror’s approach to organizational structure, quality management, staffing and effective utilization and distribution of the workforce, including subcontractors, in meeting requirements, cost constraints, and schedules. While the [Agency’s] organizational chart is provided for informational purposes, offerors shall submit the organizational structure for their workforce that they believe is most efficient and effective to perform the work. Offerors should not simply reflect the Government’s organizational structure as their own.

The offeror shall describe the proposed organizational structure, including policies, procedures, and techniques for effectively and efficiently managing work, including subcontractors. Include an organizational chart that identifies where this contract fits within the corporate structure. Offerors shall provide a contract resource profile which reflects labor categories, number of positions, and hours grouped by the proposed Work Breakdown Structure (WBS) down to the fourth level. This information shall be included in the draft management plan and will be evaluated.

* **Staffing Approach**

The staffing approach shall describe how the offeror intends to staff this effort and how the approach will ensure the offeror meets contract requirements. Consolidations, improvements, and other changes shall be explained in detail with a clear, convincing rationale. The staffing approach shall include a comprehensive hiring approach which presents the approximate rate of incumbent capture, those to be transferred from within the offeror‘s own organization, and those from other sources.

* **Position Qualifications**

Offerors shall provide position qualifications for each specific labor category. Offerors shall provide the minimum requirements in the position qualifications, to include:

* 1. duties and responsibilities
  2. licensing and/or certifications
  3. education
  4. experience

Organizational structure, staffing approach, and personnel’s position qualifications shall be included in the draft management plan and will be evaluated.

## Appendices

**Project Management Plan (no size limit)**

The offeror shall submit a draft Project Management Plan (PMP) based on its proposed technical approach using ***Attachment A - PMP Template***. The offeror’s PMP will be evaluated as part of Technical/Management. The PMP shall be submitted as an Attachment with no size limit.

The offeror shall identify in the Project Management Plan, by name and by roles and responsibilities, the proposed key personnel (i.e., the key management and technical personnel who will work under this order). The core project team should be composed of qualified professionals with strong technical backgrounds and experience in designing large, complex network configurations.

**Past Performance**

Offerors shall submit the following information as part of their proposal:

1. The offeror shall describe its past performance directly related to contracts it has held within the last [5 years] that are similar in scope, magnitude and complexity. Offerors shall provide a minimum of three (3) relevant examples. There is no maximum number of examples that can be provided.
2. The offeror shall provide relevant past performance documentation and references for services comparable to those described in the SOW. Past performance listed may include those entered into by the Federal Government, state and local government agencies, and commercial customers.
3. The offerors shall notify each of their private-sector (commercial) references that they may be contacted by the [Agency] and authorize them to provide the past performance information requested. References other than those identified by the offeror may be contacted by the Government, and the information received from them may be used in the evaluation of the offeror’s past performance.

The offeror shall provide with the proposal a summary of the required past performance information. The offeror shall provide the information using the worksheet provided in **Attachment F – Past Performance Worksheet**.

**Proposed Personnel**

The offeror shall describe the skills, qualities and capacities of its proposed Project Manager and other key personnel to meet both the minimal qualifications described in **Section 2.0** as well as their ability to meet the technical and implementation challenges of the proposed implementation approach.

The offeror shall include the resumes for all the proposed key personnel candidates and other long-term technical experts, up to a total number of [n]. Key personnel resumes may not exceed [n] pages in length and shall be in chronological order starting with most recent experience.

Each resume shall be accompanied by a signed letter of commitment from each candidate indicating his/her: (a) availability to work in the stated position, in terms of months; after award; and (b) intention to support and work for a stated term of the service. The offeror's proposed personnel shall also submit a minimum of three (3) references of professional contacts within the last three years. The offeror should provide a current phone, fax address, and email address for each reference contact.

If the Agency has additional proposal instructions above and beyond the instructions stated in this SOW, they may be provided in this section. An Agency is not required to use any of the instructions contained herein.

# Evaluation Factors and Basis for Award

The Government will evaluateeach of the offeror’s proposals to determine if the support services offerings satisfy the specific requirements under each task. The evaluations will be based on the evaluation factors defined in this section.

## Evaluation Methodology and Basis for Award

**SUGGESTED EVALUATION LANGUAGE**

**(Agency may remove or modify the narratives below)**

1. The Government may award a contract based on the initial proposal without discussions or negotiations with offerors, in accordance with **FAR 52.215-1**. Therefore, it is important that each proposal be fully compliant, without exception to any requirement, clause or provision. Offerors should submit initial proposals which respond most favorably to the SOW’s requirements.
2. The Government intends to evaluate offerors proposals in accordance with **Section 9.0** of this SOW and make a contract award to the responsible offeror whose proposal represents the best value to the U.S. Government.
3. The Technical Proposal will be evaluated by a technical evaluation committee using the technical criteria shown below.
4. Price has not been assigned a numerical weight. Offerors are reminded that the Government is not obligated to award a negotiated contract on the basis of lowest proposed price, or to the offeror with the highest technical evaluation score. Agencies must state the following when using tradeoff process: ‘The solicitation shall state whether all evaluation factors other than cost or price, when combined, are significantly more important than, approximately equal to, or significantly less important than cost or price.’
5. As technical scores converge, price may become a deciding factor in the award. Therefore, after the final evaluation of proposals, the contracting officer will make the award to the offeror whose proposal offers the best value to the Government considering both technical and price factors.

## Evaluation Approach – Trade Off or LPTA

**SUGGESTED EVALUATION LANGUAGE**

**IF TRADE OFF APPROACH**

**IS SELECTED BY THE AGENCY**

**(Agency may remove or modify the narratives below)**

The Government anticipates awarding a task order to the offeror whose quote represents the best value, price and other factors considered.

The Government anticipates awarding a task order to the offeror whose quote represents the best value, price and other factors considered.

1. The Government intends to evaluate proposals and may award a contract without discussions. However, the Government reserves the right to conduct discussions if determined by the contracting officer to be necessary. Therefore, each initial offer should contain the offeror’s best proposal from both a price and a technical standpoint.
2. Proposals received in response to this solicitation will be evaluated by the [Agency] pursuant to the Federal Acquisition Regulations (FAR) and in accordance with **FAR 52.215-1**, and as set forth in **Section 8.0: Proposal Instructions**, one award will be made by the contracting officer to the responsible offeror whose proposal, conforming to the solicitation, is determined most advantageous to the Government, all technical and price factors considered.
3. The formula set forth herein will be used by the contracting officer as a guide in determining which proposals will be most advantageous to the Government.

Note: The Agency is required to select either Trade off or LPTA Approach. Once a method has been selected, delete all information in this SOW relevant to the method that was NOT selected.

## Technical Evaluation Criteria

**SUGGESTED EVALUATION LANGUAGE**

**IF LOWEST PRICE TECHNICALLY ACCEPTABLE (LPTA) APPROACH**

**IS SELECTED BY THE AGENCY**

**(Agency may remove or modify the narratives below)**

Award will be made to the offeror whose proposal represents the lowest price technically acceptable as defined in **FAR 15.101-1**. The offeror’s proposal will be evaluated with regard to its ability to meet the tasks set forth in the SOW. To result in an award, the offeror’s proposal must demonstrate the ability to satisfy all technical requirements as set forth in the attached Statement of Work, and must conform to all required terms and conditions.

Lowest price technically-acceptable source selection process.

* + 1. The lowest price technically-acceptable source selection process is appropriate when best value is expected to result from selection of the technically-acceptable proposal with the lowest evaluated price.
    2. When using the lowest price technically-acceptable process, the following apply:
       1. The evaluation factors and significant sub-factors that establish the requirements of acceptability shall be set forth in the solicitation.
       2. Solicitations shall specify that the award will be made on the basis of the lowest-evaluated price of proposals meeting or exceeding the acceptability standards for non-price factors.
       3. If the contracting officer documents the file pursuant to FAR 15.304(c)(3)(iii), past performance need not be an evaluation factor in lowest price technically-acceptable source selections.
       4. If the contracting officer elects to consider past performance as an evaluation factor, it shall be evaluated in accordance with FAR 15.305. However, the comparative assessment in 15.305(a)(2)(i) does not apply.
       5. If the contracting officer determines that the past performance of a small business is not acceptable, the matter shall be referred to the Small Business Administration for a Certificate of Competency determination, in accordance with the procedures contained in subpart and U.S.C. 637(b)(7).
    3. Proposals are evaluated for acceptability but not ranked using non-price factors.

The Government will review the responses to this solicitation to ensure that offerors have addressed the requirements for Tasks 1-4 and are sufficient in detail and clarity to allow the Government to determine whether the proposed support services, equipment, and equipment services are acceptable, or if the Government desires to enable the Agency contracting officer to identify items for discussions.

The Government will evaluate the offeror’s proposal based upon the following four factors: technical approach, project management, proposed personnel, and past performance*.* Within these factors, the Government will evaluate the sub-factors identified below. To achieve an acceptable rating, the offeror’s Technical Proposal must achieve a pass rating on all sub-factors.

The Agency is required to develop a source selection / technical evaluation plan to describe how each of these factors will be rated. Depending on the approach used, the Source Selection Plan/Technical Evaluation Plan (SSP/TEP) may select an adjectival rating system, a points system, or any other approved system.

The Government will evaluate offerors Technical Proposals as described below:

| **TECHNICAL EVALUATION CRITERIA** |
| --- |
| **Factor 1: Technical and Management Approach** |
| Sub-factor 1: Task 1 – Program Management and General Requirements |
| Sub-factor 2: Task 2 – Network Operations Center (NOC) Support |
| Sub-factor 3: Task 3 – Security Operations Center (SOC) Support |
| Sub-factor 4: Sub-Task 1 – Support Services for Billing and Invoice Verification |
| Sub-factor 5: Sub-Task 2 – Support Services for Inventory Management |
| Sub-factor 6: Sub-Task 3 – Support Services for [specific site location/site classifications] |
| Sub-factor 7: Sub-Task 4 – Support services for Site Audit and/or Site Survey |
| **Factor 2: Staffing Approach and Proposed Personnel Qualifications/Certifications** |
| Sub-factor 8: Staffing Approach |
| Sub-factor 9: Qualification of Program Lead / Project Manager |
| Sub-factor 10: Position Qualifications of Key Personnel |
| **Factor 3: Past Performance** |
| Sub-factor 11: Past Performance History/Track Record |

**SUGGESTED EVALUATION LANGUAGE**

**FOR TECHNICAL EVALUATION OF TECHNICAL CRITERIA**

**PLEASE NOTE: The standard for evaluation is usually reserved for the SSP/TEP, however an agency may choose to disclose this information in the RFQ/RFP**

**(Agency may remove or modify the narratives below)**

The following evaluation criteria will serve as the standard against which all proposals will be evaluated and will serve to identify the significant discussion items that offerors should address in their proposals. The factors and sub-factors are presented below. Sub-factors are listed in descending order of importance, showing the evaluation weighting for each.

1. **Factor 1: Technical Approach and Project Management**

The extent to which the proposal demonstrates a clear understanding of the statement of work and the degree to which the proposed implementation approach is technically and managerially sound and likely to meet the objectives of the Network OA&M solution as described in this solicitation. The technical approach must be realistic, directly relevant to the achievement of results and must seek to maximize results within budget resources.

The Agency will evaluate the proposed best practices and innovations for reasonableness, realism, and the effectiveness of quantified efficiencies. The Agency will evaluate any assumptions and underlying rationale associated with those assumptions for reasonableness.

* Sub-factor 1: Task 1 – Program Management and General Requirements

**Program Management** - The Agency will evaluate for adequacy, effectiveness, realism, and relevancy, the offeror‘s proposed responsibilities (such as workflow, staffing) and authorities for program management of this contract. This evaluation will consider the offeror‘s proposed approach to resolving internal conflicts over resources with other company organizations, degree of autonomy of the Program Executive, and lines of communication among Agency, offeror, and subcontractor.

**Organizational Structure and Chart** - The Agency will evaluate the realism, effectiveness, and efficiency of the offeror‘s proposed organizational structure, including policies, procedures, and techniques for managing the proposed work to include subcontractors. This evaluation will include the offeror‘s approach to quality management of the required services through surveillance, organizational structure, staffing and utilization and distribution of the workforce in meeting contract requirements, cost constraints, and schedules.

**SUGGESTED EVALUATION LANGUAGE**

**FOR TECHNICAL EVALUATION OF TECHNICAL CRITERIA**

**(Cont.)**

* Sub-factor 2 to 7: Overall Operational and Technical Approach - Support Services, Administration, and Management of Data Network Enterprise

The Agency will evaluate the overall operational and technical approach for Tasks 1 to 4 to determine the offeror understands the requirements for accuracy, effectiveness, efficiency, realism, relevancy, and comprehensiveness.

The Agency will evaluate the proposed best practices and innovations for reasonableness, realism, and the effectiveness of quantified efficiencies. The Agency will evaluate any assumptions and underlying rationale associated with those assumptions for reasonableness.

The Agency will evaluate the approach to achieving compliance for accuracy and effectiveness. The Agency will evaluate for effectiveness, efficiency, timeliness, and realism of the offeror‘s approach to support multiple, simultaneous efforts that may have competing requirements for technical expertise, timelines and delivery schedules that will be supported.

The Agency will also evaluate for effectiveness how the offeror will implement delivery schedule management, identifying and managing risk, quality assurance, and obtaining user feedback for performance improvement.

The Agency will evaluate the overall operational and technical approach for each of the Tasks identified below to determine the offeror understands of the requirements for accuracy, effectiveness, efficiency, realism, and comprehensiveness.

* Sub-factor 2: Task 2 – Network Operations Center (NOC) Support
* Sub-factor 3: Task 3 – Security Operations Center (SOC) Support
* Sub-factor 4: Sub-Task 1 – Support Services for Billing and Invoice Verification
* Sub-factor 5: Sub-Task 2 – Support Services for Inventory Management
* Sub-factor 6: Sub-Task 3 – Support Services for [specific site location/site classifications]
* Sub-factor 7: Sub-Task 4 – Support services for Site Audit and/or Site Survey

1. **Factor 2: Staffing Approach and Qualifications/Certifications of Proposed Personnel**

* Sub-Factor 8: Staffing Approach - The staffing approach shall describe how the offeror intends to staff this effort and how the approach will ensure the offeror meets contract requirements. Consolidations, improvements, and other changes shall be explained in detail with a clear, convincing rationale.

**SUGGESTED EVALUATION LANGUAGE**

**FOR TECHNICAL EVALUATION OF TECHNICAL CRITERIA**

**(Cont.)**

The staffing approach shall include a comprehensive hiring approach which presents the approximate rate of incumbent capture, those to be transferred from within the offeror‘s own organization, and those from other sources. The offeror shall discuss their staffing approach and strategies if their primary staffing strategy is not completely successful.

Offerors should describe their ability to staff from existing resources and from outside sources to satisfy fluctuating requirements.

* Sub-Factor 9: Qualification of Program Lead / Project Manager – The proposed Program Lead/Project Manager shall demonstrate the qualifications and ability to successfully lead this project, including the ability to work constructively at multiple levels of organizations, including senior levels of Government and business. The Resume of Project Manager will be evaluated against these criteria.
* Sub-Factor 10: Position Qualifications of Key Personnel - Offerors shall provide position qualifications for each specific labor category. Offerors shall provide the minimum requirements in the position qualifications, to include:

1. duties and responsibilities
2. licensing and/or certifications
3. education
4. experience

This information shall be included in the draft management plan and will be evaluated. The members of the proposed project team, including subject-matter experts (SMEs), shall demonstrate the experience and ability to successfully meet the project milestones, targets, and goals.The Resumes of Key Personnel will be evaluated against these criteria.

**SUGGESTED EVALUATION LANGUAGE**

**FOR TECHNICAL EVALUATION OF TECHNICAL CRITERIA**

**(Cont.)**

1. **Past Performance**

* **Sub-Factor 11: Past Performance** information will be used for both the responsibility determination and best value decision. The offeror and major subcontractor(s) past performance will be evaluated. A major subcontractor (if applicable) is defined as a subcontractor named in the proposal whose total price exceeds 15% of the offer’s bottom line total price, including fixed fee.
* The submitted performance worksheet will be evaluated against these criteria. Likewise, the contracting officer will also utilize existing database of offeror performance information (i.e. Past Performance Information Retrieval System (PPIRS)) and solicit additional information from the references provided in this SOW and from other sources if and when the contracting officer finds the existing databases to be insufficient for evaluating an offeror’s performance. The [Agency] may use performance information obtained from other than the sources identified by the offeror/subcontractor.

## Price Evaluation Criteria

**SUGGESTED EVALUATION LANGUAGE**

**FOR PRICE EVALUATION CRITERIA**

**(Agency may remove or modify the narratives below)**

1. No points are assigned to the price proposal evaluation. While the technical evaluation criteria are significantly more important than price, price remains important.
2. Price will primarily be evaluated for realism, allow-ability, and reasonableness.
3. This evaluation will consist of a review of the price portion of an offeror’s proposal to determine if the overall price proposed is realistic for the work to be performed, if the price reflects an accurate understanding of the requirements, and if the price is consistent with the Technical Proposal.
4. Evaluation of the price proposal will consider but not be limited to the following:

* Price reasonableness, price realism and completeness of the price proposal and supporting documentation
* Overall price control/price savings evidenced in the proposal (avoidance of prices that exceed reasonable requirements)
* The amount of the proposed fee, if any

**SUGGESTED EVALUATION LANGUAGE**

**FOR PRICE EVALUATION CRITERIA (Cont)**

1. Price realism is an assessment of the accuracy with which proposed prices represent the most probable cost of performance, within each offeror’s technical and management approach. A price realism evaluation shall be performed as part of the evaluation process as follows:

* Verify the offeror’s understanding of the requirements
* Assess the degree to which the price proposal accurately reflects the technical approach
* Assess the degree to which the prices included in the Price Proposals accurately represent the work effort included in the respective Technical Proposals

1. The results of the price realism analysis will be used as part of the Agency’s best value/tradeoff analysis.
2. Although technical evaluation criteria are significantly more important than price, the closer the technical evaluation scores of the various proposals are to one another, the more important price considerations will become. The evaluation of proposed prices may therefore become a determining factor in the award as technical scores converge.

# Task Order Award

The Task Order Award will be made to the responsible offeror whose proposal is in the best interest of the [Agency], given the outcome of the [Agency]’s evaluation of each offeror’s technical excellence, management and business risk factors, and proposed price. In selecting the Task Order Award, the [Agency] will consider the quality offered for the evaluated price. The relative quality of offers will be based upon the [Agency]’s assessment of the tradeoffs between the technical excellence offered in the offeror’s proposal and whether it provides added value, added capability, and/or reduced management and business risk.

# Organizational Conflicts of Interest

The guidelines and procedures of **FAR Subpart 9.5** will be used in identifying and resolving any issues of organizational conflicts of interest at the task order level. (*Refer to* ***Section H.8 Organizational Conflicts of Interest*** *of the Connections II contract*).

In the event that a task order requires activity that would create or has created an actual or potential conflict of interest, the offeror shall:

* Notify the task order contracting officer (CO) of the actual or potential conflict, and not commence or continue work on any task order that involves a potential or actual conflict of interest until specifically notified by the task order CO to proceed.
* Identify the conflict and recommend to the task order CO an alternate tasking approach which would avoid the conflict.

If the task order CO determines that it is in the best interest of the Government to issue or continue the task order, notwithstanding a conflict of interest, a request for waiver shall be submitted in accordance with **FAR 9.503**.  In the event that the offeror was aware of facts required to be disclosed or the existence of an actual or potential organizational conflict of interest and did not disclose, when known, such facts or such conflict of interest to the task order CO, the Government may terminate this contract for default.

In the event that a task order issued under this contract requires the offeror to gain access to proprietary information of other companies, the offeror shall be required to execute agreements with those companies to protect the information from unauthorized use and to refrain from using it for any purpose other than for which it was furnished.

# Acronyms and Glossary of Terms

## Acronyms and Definition

| **Acronym** | **Definition** |
| --- | --- |
| SLR | Service Level Requirements |
| FAR | Federal Acquisition Regulation |
| JTR/FTR | Joint Travel Regulations/Federal Travel Regulation |
| PBX | Private Branch Exchanges |
| QoS | Quality of Service |
| SOW | Statement of Work |
| SSP | Source Selection Plan |
| SCRM | Supply Chain Risk Management |
| TDM | Time Division Multiplexers |
| TEP | Technical Evaluation Plan |
| VoIP | Voice over Internet Protocol |

## Glossary of Terms

| **Glossary of Terms** | **Description** |
| --- | --- |
| **Internet Protocol Private Branch eXchange (IP PBX)** | A telephone switch that natively supports voice over IP (VoIP). An IP PBX uses VoIP-based protocols to communicate with IP-based hosts such as VoIP telephones over a packet-switched network. Some IP PBXs can also support the use of traditional analog and digital phones. |
| **Private Branch eXchange (PBX)** | A private telephone network in an organization. Individual telephone numbers or extension numbers are supported, and calls are automatically routed to them. Users can call each other using extensions, even across distributed locations. |
| **Supply Chain Risk Management (SCRM)** | SCRM is "the implementation of strategies to manage both every day and exceptional risks along the supply chain based on continuous risk assessment with the objective of reducing vulnerability and ensuring continuity. SCRM attempts to reduce supply chain vulnerability via a coordinated holistic approach, involving all supply chain stakeholders, which identifies and analyses the risk of failure points within the supply chain. |

# Attachments

## Attachment A – Program Management Plan



## Attachment B – Support Locations

****

## Attachment C – Pricing Instructions

****

## Attachment D – Pricing Template



## Attachment E – Equipment Support, Warranty and Inventory



## Attachment F – Past Performance Worksheet



## Attachment G – Task Order Deliverables Performance Matrix



## Attachment H – Current Network Architecture and Service Environment



In addition to the current network architecture diagram, the Agency may insert here any relevant information to describe the agency’s service environment, data and network asset information:

* A listing and description of all hardware to be supported is provided in Attachment H.1- Network Hardware.
* A listing and description of the software and utilities to be supported is provided in Attachment H.2 – Network Software.
* A listing and description of the Network circuits to be supported is provided in Attachment H.3 – Network Circuits Database.
* A listing and description of the data sets and applications to be supported are provided in Attachment H.4 - Applications and Data Sets.