

**DEPARTMENT OF HOMELAND SECURITY (DHS)**  
**CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)**  
**STATEMENT OF WORK (SOW)**  
**FOR**  
**PROOF OF CONCEPT EXECUTION MANAGER**

**1.0 GENERAL**

**1.1 BACKGROUND**

CISA's mission is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. CISA includes the CISA Mission Enabling Offices (MEOs) and six Divisions: the Cybersecurity Division (CSD), the Emergency Communications Division (ECD), the Integrated Operations Division (IOD), Infrastructure Security Division (ISD), the Stakeholder Engagement Division (SED), as well as, the National Risk Management Center (NRMC), which are headquartered with the National Capital Region (NCR).

The Emergency Communications Division is the MEO that oversees the efforts and offerings of Priority Communication Services (PCS) to provide Federal, State, Local, Territorial, and Tribal levels of government and National Security/Emergency Preparedness (NS/EP) authorized users with priority secure, reliable, and resilient communication services under any circumstances causing network congestion or overload through two programs.

In response to communication challenges, CISA supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. The Priority Telecommunications Service (PTS) program provides priority communications over the commercial carrier networks. These priority services provide capabilities required under the authority of 6 USCODE section 571, as well as Executive Order 13618 and Presidential Policy Directives for Continuity of Operations (COOP) and Continuity of Government (COG). However, emerging technology and advancing operational command and control procedures have created a gap in the availability of priority communications. PTS voice in the commercial carrier networks begin to obsolesce when circuit-switched technology in the public switched telephone network (PSTN) transitions to packet-switched IP-based technology. For advanced command and control, PTS currently does not yet provide priority data, video, and information services (DVIS).

The Priority Telecommunications Service (PTS) program is a White House directed acquisition program that leverages the commercially owned Public Switched Telephone Network (PSTN) to provide the NS/EP user community with priority communications under all circumstances, when network congestion or damage renders conventional communications ineffective. PTS enhances the ability for registered users to complete calls during a natural or manmade congestion event using four PTS operational components: Government Emergency Telecommunication Services (GETS), Wireless Priority Service (WPS), Special Routing Arrangement Service (SRAS), and Telecommunication Service Priority (TSP). Each of these programs contributes to assure NS/EP communications as described below.

GETS is a major ECD program for the improvement of NS/EP telecommunications that supports key Government users in the event of major natural or manmade disasters up through early post-nuclear attack. GETS was established to provide users with an end-to-end, switched voice telephone service that can be used for clear voice, encrypted secure voice, facsimile, and low speed data services using the surviving facilities of the Public Switched Network (PSN). End-to-end was defined to be from the originating caller's Local Exchange Carrier (LEC) end office to the destination end office. With PTS the definition of end-to-end will be expanded within the access networks to extend as close as possible to the end user. GETS provides routing alternatives and traffic management features that do not exist for normal PSN calls and is accessible from virtually anywhere in the United States and is capable of using all major LEC facilities, Interexchange Carrier (IXC) facilities, and selected Government networks (e.g., Defense Information System Network, Diplomatic Telecommunications Service, and Federal Telecommunication Service 2001/Network/Enterprise Infrastructure Solutions (EIS) or follow-on services). GETS also provides the capability for international inbound and outbound access. Under the current PTS aided by new NGN PS technologies, the services will take maximum advantage of new Internet Protocol (IP) based networks with far reaching improvements in routing and multi-media exchange.

The WPS program was approved as a result of the September 11, 2001, terrorist attack and provides a priority scheme that is fully compatible with GETS. WPS implements wireless priority capabilities that enhance NS/EP transmission through the wireless elements of the PSN and is compatible with the Federal Communications Commission (FCC) Report and Order, FCC22-36A1. Priority transmission through the Wireless networks provides services equivalent to those provided by GETS in wireline networks. Priority access for WPS (known as Enhanced Overload Performance (EOP)) was implemented in selected networks in addition to priority transport in response to drastically increased radio network congestion.

SRAS is a GETS service for special users that provides for the highest level of non-traceable PTS service during times of severe PSN congestion or disruption as may result from acts of terror or war.

TSP authorizes NS/EP organizations to receive priority restoration and installation of vital voice and data circuits and infrastructure for telecommunications services damaged because of natural or man-made disaster. Organizations designate critical circuits to receive priority restoration in an emergency and TSP provisioning authorizes prompt installation of new circuits.

The NGN PS program oversees the development of priority data, voice, and information (DV&IS) capabilities, in accordance with Presidential Policy Directive (PPD) 40<sup>1</sup> and will leverage and expand relationships, processes, mechanisms, and expertise from the separate NGN PS Phase 1 program to develop and verify priority DV&IS capabilities on advancing networks and technologies for transfer to the Level 3 Priority Telecommunications Services (PTS) acquisition program for operations and sustainment.

NGN PS Phase 1 and Phase 2 are Level 2 special interest programs<sup>2</sup>, for which the Government provides oversight. As such, NGN PS provides requirements and verifies development,

---

<sup>1</sup> Presidential Policy Directive (PPD) 40, 2016, for Continuity of Operations (COOP) and Continuity of Government (COG) and includes data, video, and information services.

<sup>2</sup> NGN PS Programs are Level 2 special interest designation by DHS USM Acquisition Decision Memorandum (ADM), June 6, 2018; and DHS Deputy, USM ADM, November 21, 2019.

implementation, and interoperability of evolving Priority Services capabilities within the commercial communications service providers' networks; prior to incorporation into PTS operations. Together, NGN PS and PTS provide continuous NS/EP priority communications under all circumstances when network congestion or damage renders conventional communications ineffective.

The NGN PS Mission Need Statement (MNS)<sup>3</sup> describes the required mission needs, capability gap, and program justification to support the transition from legacy circuit switched PTS onto next generation, IP packet switched public carrier networks to, "...provide communications under all circumstances, including crisis or emergency, attack, recovery, and reconstitution, when network congestion or damage renders conventional communications ineffective."

*"The NGN Priority Services Program goal is to maintain legacy priority voice telecommunications services (GETS, WPS, and SRAS) while the Program Office works to achieve priority voice services in the packet-switched networks. NGN service providers will implement priority service features to meet the original White House recommendations for voice services, including authentication, exemption from network management controls, and enhanced routing for NGN voice priority traffic. The White House recommendations specify providing broadband service in support of NS/EP missions including video and data." — MNS*

PTS and NGN PS Priority Services Programs are managed by the Department of Homeland Security as directed by Executive Order (EO) 13618<sup>4</sup>. The EO establishes policy for the Federal Government to have the ability to communicate at all times during all circumstances to ensure national security, effectively manage emergencies, and improve national resilience. NGN PS supports PPD 40 National Continuity Policy to support Continuity of Operations (COOP) and Continuity of Government (COG).

NGN PS will provide NS/EP communications users with priority service in the converging and next generation commercial networks. These networks will eventually replace the current circuit switched, time division multiplex (TDM) networks with packet switched and packet transport facilities supporting a wide variety of communications services. NGN PS will both replace and supplement current GETS, SRAS and WPS services as the PSN gradually migrates to packet-based technologies. NGN PS will be provided for both the current voice and voice-band data NS/EP requirements and the expanding needs of NS/EP communications users—beyond voice and voice-band data services into areas such as broadband data and video. NGN PS will assure a full range of NS/EP communications requirements are satisfied by the next generation public communications networks.

The PTS and NGN PS Priority Services Programs are designed to achieve cost effective prioritized communications by continuing to leverage the highly survivable, commercially owned public communications network assets. CISA ECD oversees NGN PS phased programs to provide technical requirements and manage the development verification and transition of advanced service capabilities to PTS operations and sustainment. Priority Services capabilities reside within the

---

<sup>3</sup> National Security Emergency Preparedness Next Generation Network Priority Services Program Mission Needs Statement Version 1.1 dated April 22, 2010 (approved)

<sup>4</sup> EO 13618 July 6, 2012, the EO updates and clarifies the Federal Government NS/EP communications responsibilities to address a challenging and dynamic technological environment.



commercial communications service providers' networks and are customized within each service provider's commercial development methodology.

When deployed under PTS operations oversight, NGN PS capabilities will provide the Government with priority communications over advanced, robust, and diverse nationwide communications networks at a fraction of the cost required to build and maintain a government-owned system.

## **1.2 SCOPE**

This Statement of Work (SOW) specifies the tasks and responsibilities required of the Contractor, to develop, propose, execute, oversee, and complete proofs of concept and evaluations of evolving communication technology. In alignment with the Test and Evaluation process and procedures, the contractor shall be responsible for conducting all work using the System Engineering Life Cycle (SELC). The Contractor shall be responsible for developing and providing a transition plan for proofs, and evaluations that are accepted by the Government for program implementation.

## **1.3 OBJECTIVE**

The objective of this SOW is to specify the workout outcomes required to of the Contract to:

1. Oversee proofs of concept and subcontract with service providers
2. Execute technical feasibility studies and needs analysis to ensure Proof of Concept (PoC) is in line with the program roadmap. Conduct impact analysis on NS/EP priority services' security and potential vulnerabilities with the deployment of the PoC solution, and necessary protection/mitigation measures. Define any new priority, security capabilities and any synergistic deployments with other priority services (e.g., FirstNet, commercial priority service) as a result of the PoC.
3. Ensure tailored SELC process is used throughout the PoC and evaluation; demonstrate the government can operationalize the product/service discussed in the PoC; define what can be conducted in a vendor's or service provider's lab, to determine that the PoC can be operationalized. Validate lab verification of Key Performance Parameters' (KPP). Provide analysis of the effort required to deploy and operate the PoC solution. Define of quantitative KPP values to support a measurable Success/Failure criterion in the PoC proposal. Ensures that any change in the UE, SPs' networks, and/or Operations, Administration, Maintenance, and Provisioning (OAM&P) systems required for the "concept" should be defined and integrated into the PoC proposal. Define impact on existing network components and OAM&P systems. Draft required technical documents which include, but not limited to, network architecture/design, provisioning information, tests cases and results, as they should be available during the course of the effort.
4. Develop a detailed project plan for deliverables
5. Document a transition plan if the PoC is successful, and specify through what vendor or service provider the government can use to deploy the PoC into operations
6. Oversee PoC transition into operations
7. Work with the Test and Evaluation team as necessary (e.g., DOT&E, Independent Test Agent)

## 1.4 APPLICABLE DOCUMENTS

### 1.4.1 Reference Documents

The following documents may be helpful to the Contractor in performing the work described in this document:

Reference	Title	Date	Sections
(a)	NS/EP PS Functional Requirement Specification (FRS) Version 3.0 – and/or current version and Appendix c SRAS FRS	29 September 2017	All
(b)	NGN PS Phase 2 Functional Requirements Document (FRD), includes FRS and/or current version	09 December 2022	All
(c)	NS/EP PoC Process	14 December 2022	All
(c)	GETS/WPS Security Classification Guide (SCG) – DHS SCG CISA-007.1	22 November 2019	All
(d)	SELC Guidebook	May 2019	
(e)	NS/EP Cybersecurity Requirements	20 Marc 2023	All
(f)	NGN PS Test and Evaluation Master Plan (TEMP) v 4	30 September 2020	All

## 2.0 SPECIFIC REQUIREMENTS/TASKS

### 2.1 TASK ONE. Program Management

The Contractor shall provide a Program Manager who shall be responsible for all Contractor work performed under this SOW. The Program Manager shall be a single point of contact for the Contracting Officer and the COR. The name of the Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Program Manager, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Program Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. Additionally, the Contractor shall not replace the Program Manager without prior approval from the Contracting Officer.

As part of the basic contract and for the duration of the contract, the Contractor shall provide the planning, direction, coordination, and control necessary to accomplish all work requirements contained in this contract and as amended by contract modifications. In addition, the Contractor shall conduct program review meetings and produce documentation as defined in the specified in each subtask to keep the Government informed on the status of all tasks.

The Program Manager shall be available to the Government via telephone between the hours of 9:00AM and 5:30PM EST, Monday through Friday.

### **2.1.1 Project Management**

The Contractor shall determine the project organization, how technical and project management will be performed, how personnel and physical resources will be managed, and what mechanisms will be used for cost and schedule control.

The Contractor shall designate a single individual to serve as the program manager, who shall also be identified under the key personnel provision, who is responsible for the cost, schedule, and technical performance of the contract and serve as the central point-of-contact (POC) for both management and technical matters. The program manager shall have the authority to represent and act on behalf of the entire Contractor support team in all matters concerning the project.

The Contractor shall schedule and carry out tasks set forth in this contract and related contract modifications.

The Contractor shall include risk management practices and mechanisms for controlling implementation activities within approved resources and schedules.

The Contractor shall support the required Government oversight meetings, processes and related roles, which will be facilitated for Contractor understanding through the Program Management Office, including:

- Service Provider Council (SPC) and related Working Groups to support understandings for Government requirements and oversight verification processes, across Contractors
- Systems Engineering Lifecycle (SELC), as tailored for PS and technical reviews that are initially conducted with the Contractor
- The Integrated Test and Evaluation (T&E) Strategy as outlined in the NGN PS Test and Evaluation Master Plan (TEMP), Section 3.0 for understanding:
  - Overall T&E and verification processes
  - Key test events
  - Independent Test Agent evaluations in alignment with the NGN PS TEMP

The Contractor shall provide all required coordination and associated reporting for its services and interactions concerning the PTS contractor and other providers that support NS/EP PS. This coordination shall include emphasis on end-to-end service and OAM&P arrangements.

### **2.1.2 Quarterly Program Management Reviews**

The Contractor shall conduct quarterly program reviews (QPR) on a date and at a location within the Washington, District of Columbia (DC) area or virtually as mutually agreed upon between the Government and the Contractor.

The Contractor shall include presentations on NS/EP PS management, planning, and operations, administration, maintenance, and provisioning OAM&P activities in each review.

The Contractor shall record all Government questions, comments, or issues that are raised during these reviews and report the status of outstanding actions in subsequent monthly status reports.

The Contractor shall be prepared to attend or host ad hoc technical interchange meetings (TIM) with the Government to discuss enhancements, plans, or operational impacts of incidents impacting service.

Proofs of Concepts can be proposed by the Contractor or the Government.

### **2.1.3 Annual Program Management Reviews**

The Contractor shall conduct annual program reviews (APR) on a date and at a location within the Washington, DC area or virtually as mutually agreed upon between the Government and the Contractor.

The Contractor shall include presentations on NS/EP PS management, planning, and operations, administration, maintenance, and provisioning OAM&P activities in each review.

The Contractor shall record all Government questions, comments, or issues that are raised during these reviews and report the status of outstanding actions in subsequent monthly status reports.

The Contractor shall be prepared to attend or host ad hoc TIM with the Government to discuss enhancements, plans, or operational impacts of incidents impacting service.

Proofs of Concepts can be proposed by the Contractor or the Government.

## **2.2 TASK TWO Proof of Concept Management**

**2.2.1** The Contractor shall follow the PoC process for every PoC authorized by the Government. The Contractor shall obtain Government approval at each of the decision points below:

- (a) Request for Needs Analysis
- (b) Needs Analysis
- (c) Work Statement
- (d) Proposal Development
- (e) Prototype Development and Evaluation
- (f) Reports and Prototype

Refer to Ref. (c) NS/EP Priority Services PoC Process Brief for details of the Proof of Concept Process.



#### **2.2.1.1 PoC Progress Reports**

The Contractor shall provide a PoC progress report monthly and as requested by the Government to the COR and T&E Manager via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

#### **2.2.1.2 PoC Technical Exchange Meeting Minutes**

The Project Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place *at the Contractor's facility* or virtually as mutually agreed upon between the Government and the Contractor.

#### **2.2.2 Systems Engineering Life Cycle (SELC) Requirement Details**

The Government uses a service acquisition contract strategy based on the requirements identified in the FRS and FRD in Attachment (a) and (b), which includes industry standards. The Contractor may propose using additional industry standards, as well as the standards-like Government Industry Requirements documents as the basis for its approach to meet the requirements of the FRS; however, such an approach shall be evaluated by the Government and may be used if found to be acceptable. Any vendor development initiated by the Contractor and paid for by the Government shall include Right to Use language, where feasible, allowing other carriers, who are also approved by the Government to provide NS/EP PS, to use the resulting development in their own networks at no additional vendor development cost to Government.

The Contractor may propose tailoring the NGN PS SELC process to better match their own internal SELC processes, such proposed tailoring shall be evaluated by the Government and may be used if found to be acceptable. Regardless, the Contractor shall provide the technical reviews and testing deliverables to the Government as outlined below. Successively developed proofs, , and evaluations may result in multiple design and test reviews. Contractor documentation for design and test reviews and Government witness testing shall be the main deliverables used to verify and validate that requirements are being met. All issues concerning the subject of a review shall be resolved prior to conducting that formal technical review. The Contractor shall support direct on-site attendance at testing events of at least 6 individuals total (Government representatives and support Contractors) to serve as Government witnesses. The Contractor may propose, pending Government approval, alternate approaches such as virtual participation in test events, where direct participation by 6 representatives is not possible.

Subtask Requirements Management: The Contractor shall provide and maintain a Requirements Traceability and Verification Matrix (RTVM) that details how the NGN PS requirements are being verified and validated at mutually agreed upon milestones. This RTVM shall include the Contractor's planned requirements for all functions, capabilities, and performance to be implemented for a proof, , and evaluation. The Contractor shall define interoperability and regression testing requirements that ensure the implemented capabilities are compatible with existing priority service capabilities. The Contractor shall incorporate these interoperability and regression testing requirements into the RTVM. This RTVM shall be the basis of the design, implementation, and testing for the remainder of the Contractor's proofs, , and evaluations.



Using the high-level information provided in its proposal as a basis, the Contractor shall provide a report that thoroughly identifies and describes the risks addressed by proposed priority capabilities in addition to providing a level of performance improvement and/or risk mitigation expected due to deployment of each capability proposed. The report shall also investigate the potential benefit to NS/EP priority communications of advanced features such as a dedicated Establishment Cause for WPS User Equipment (EUs) and alternative capabilities.

**SELC Technical Reviews:** The Contractor shall provide a preliminary schedule at the kickoff meeting to be scheduled 45 days after award for conducting technical reviews and update the schedule throughout the duration of this effort. The Contractor may substitute commercial practices and processes for elements of the DHS SELC process if the Contractor can demonstrate significant savings in terms of cost and time, and/or enhanced performance to the Government. The Contractor shall provide documentation to be approved by the Government that verifies and validate each milestone (Preliminary Design Review (PDR), Critical Design Review (CDR), Initial Readiness Review (IRR), and Production Readiness Review (PRR)) provided under this tasking.

The Contractor shall conduct SELC reviews at a location within the Washington, DC area or virtually as mutually agreed upon by the Government and the Contractor.

The Contractor shall include presentations on SELC in each review.

The Contractor shall record all Government questions, comments, or issues that are raised during these reviews and report the status of outstanding actions in subsequent monthly status reports.

The Contractor shall be prepared to attend or host ad hoc technical interchange meetings with the Government to discuss enhancements, plans, or operational impacts of incidents impacting service.

At a minimum, the following technical reviews shall be conducted:

1. The Contractor shall conduct a PDR for the Government for the limited capability (LC), initial operating capability (IOC), and full operating capability (FOC) feature development and associated implementation efforts. The PDR allows the Government to evaluate the Contractor's proposed solution, agree on the system requirements, assess whether the Contractor has addressed the functional requirements, review preliminary solution design documentation (objective: 75%), and determine if the solution can be implemented within the cost and schedule constraints.
2. The Contractor shall conduct a CDR for the Government for the LC/IOC/FOC feature development and associated implementation efforts. The CDR allows the Government to determine if the design is complete (objective: 95%) and accurate in its documentation specification and can produce the results defined in the baseline requirements. The Contractor shall have resolved all action items from a PDR prior to the CDR.
3. The Contractor shall conduct an IRR for the Government prior to each testing event in order to review test plans, assess test objectives, test methods and procedures, scope of tests, determine if required test resources (people, facilities, test articles, test instrumentation) have

been properly identified and coordinated to support the test, and otherwise determine the Contractor's readiness for the testing event (e.g., review pertinent documentation, logistics, results from dry runs, etc.). Subsequent submission shall be the FINAL version of the Test Plan incorporating Government comments on the draft Test Plan.

4. The Contractor shall conduct a PRR for the Government after development and testing is complete and prior to placing the new capabilities in operation.

Testing: The Contractor shall propose their testing approach and shall establish a schedule for and conduct testing of the specified capabilities for each proof of concept, , and evaluation as mutually agreed to between the Government and the Contractor. The Contractor shall conduct an Operational Readiness Test (ORT) that verifies a proof, , and evaluation can be added or deleted, user priority levels modified successfully, and that accurate OM and test results are being reported to verify against KPP that are being reported.

1. The Contractor shall provide a Captive Office Test (COT) verifying functional requirements defined in the RTVM, as well as performance and stress testing of the features to verify they are capable of meeting the KPPs in a simulated all-hazards laboratory environment.
2. The Contractor shall provide a NSAT in a limited production environment to verify correct operation in a live network.
3. The Contractor shall conduct testing IAW the Government-approved test plans. The Contractor shall allow the Government to witness all testing and have access to test results and all relevant test data. The Government may waive the requirement for Government-witnessed testing for specific testing events based on technical discussions with the Contractor, but this does not relieve the Contractor of the requirement to furnish test results and all relevant test data.
4. The Contractor shall define interoperability and regression testing requirements drawn from Attachment (a) and (b) to ensure that the capabilities architecture/solution is backward-compatible with legacy services with no service degradation. The Contractor shall incorporate these interoperability and regression testing requirements into the RTVM, as well as the test plans for COT and NSAT.
5. The Contractor shall conduct all testing IAW the RTVM. The Government will use the RTVM in its acceptance of the Contractor's work.

### **2.3 - TASK THREE Transition Plan From Proof of Concept to Operations (Optional)**

The Contractor at the discretion of the Government will develop a transition plan to transition the Proof of Concept to Operational status.

### **2.4 - TASK FOUR Other Direct Costs (ODCs)**

The purchase of other direct costs such as equipment, materials, or service access fees may be required to complete proofs of concepts. The Contractor shall be responsible for obtaining Government approval (electronic mail is acceptable) prior to expending any funds for ODCs and are not to exceed the cost agreed upon at contract award.

## 2.5 - TASK FIVE Travel

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

## 3.0 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

**3.1** The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

**3.2** The Government will have 10 business days to review deliverables and make comments. The Contractor shall have 3 business days to make corrections and redeliver.

**3.3** All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

## 4.0 DELIVERABLES

The Contractor shall consider items in **BOLD** as having mandatory due dates. Items in *italics* are deliverables or events that must be reviewed and/or approved by the Government prior to proceeding to next deliverable or event in this SOW.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	6.8	<b>Post Award Conference</b>	Within 10 working days of contract award	N/A
2	2.2	<i>Request for Needs Analysis</i>	As Required	COR, Contracting Officer
3	2.2.1	<i>Needs Analysis</i>	As Required	COR, Contracting Officer
4	2.2.1	<i>Work Statement</i>	As Required	COR, Contracting Officer

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
5	2.2.1	<i>Proposal Development</i>	As Required	COR, Contracting Officer
6	2.2.1	<i>Prototype Development and Evaluation</i>	As Required	COR, Contracting Officer
7	2.2.	<i>Reports and Prototype</i>	As Required	COR, Contracting Officer
8	2.3	<i>Transition Plan from PoC to Operations</i>	As Required	COR, Contracting Officer
9	6.10	<b>Program Plan</b>	45 calendar days after contract award	COR, Contracting Officer
10	6.11	<b>Program Progress Report</b>	By the 10 <sup>th</sup> of each month for the life of the contract	COR, Contracting Officer
11	6.11	<b>Program Status Report</b>	45 calendar days after contract award	COR, Contracting Officer
12	2.1.2 2.1.3	<i>Program Review Agenda (QPR and APR)</i>	DRAFT version shall be submitted 3 working days prior to conference; Final version shall be submitted 1 working day prior	COR and T&E Manager
13	2.1.2 2.1.3	<i>Program Review Minutes (QPR and APR)</i>	DRAFT version shall be submitted 3 working days after conference; Final version shall be submitted 10 working days following receipt of Government's comments	COR and T&E Manager
14	2.2.1.2	<i>PoC Technical Exchange Minutes</i>	DRAFT version shall be submitted within 3 working days after meeting; FINAL version shall be submitted within 10 working days after meeting	COR and T&E Manager



ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
15	2.2.2	<i>Test Plan</i>	DRAFT version shall be submitted 60 days before test/demonstration; Final version shall incorporate Government's comments on draft.	COR and T&E Manager
16	2.2.2	<i>Test Plan Report</i>	30 working days after completion of testing	COR and T&E Manager
17	6.11	<i>Monthly Performance Report</i>	Monthly and as required by the Government	COR, Contracting Officer
18	2.2.1.2	<i>PoC Progress Report</i>	Monthly and as request by the Government	COR and T&E Manager
19	2.2.2	<i>Network Service Architecture Document</i>	As required	COR and T&E Manager
20	2.2.2	<i>Program Planning Review</i>  <i>(All Required Documentation 10 Days before the review)</i>	As required	COR and T&E Manager
21	2.2.2	<i>Preliminary Design Review</i>  <i>(All Required Documentation 10 Days before the review)</i>	As required	COR and T&E Manager
22	2.2.2	<i>Critical Design Review</i>  <i>(All Required Documentation 10 Days before the review)</i>	As required	COR and T&E Manager
23	2.2.2	<i>Integration Readiness Review</i>  <i>(All Required Documentation 10 Days before the review)</i>	As required	COR and T&E Manager

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
24	2.2.2	<i>Production Readiness Review</i>  <i>(All Required Documentation 10 Days before the review)</i>	As required	COR and T&E Manager

## 5.0 CONTRACTOR PERSONNEL

### 5.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

### 5.2 Employee Identification

#### 5.2.1 Key Personnel

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as *Key* for this requirement. Note: The Government may designate additional Contractor personnel as *Key* at the time of award.

IT Project Manager (SME) is designated as *Key* for this requirement and must have the following qualifications:

Masters degree in IT or Project Management  
Minimum of 15 years IT/Telecom experience  
Minimum of 5 years Project Management experience

The Project Manager shall be available to the COR via telephone between the hours of 9:00 a.m. and 5:00 p.m. ET, Monday through Friday.

**5.2.2.** Contractor *Key* personnel shall not be assigned by the Contractor to more than one *key* position for this requirement.

**5.2.3** Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

**5.2.4** Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

### **5.3 Employee Conduct**

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

### **5.4 Removing Employees for Misconduct or Security Reasons**

The Government may, at its sole discretion (via the Contracting Officer\*), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

## **6.0 OTHER APPLICABLE CONDITIONS**

### **6.1 SECURITY**

Contractor access to CISA Sensitive Information, systems, networks and reoccurring access to CISA facilities is not required under this SOW; therefore, contractor employees will not require DHS Fitness Determination to perform work.

Sensitive Information is defined in the DHS Instruction Handbook, 121-01-007, "The Department of Homeland Security, Personnel Security, Suitability and Fitness Program" as "Any information, the loss, misuse, disclosure, unauthorized access to, or modification of, which could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy. This definition includes one of the following categories of information:

- A. Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 21 1-224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual; or
- B. Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520; or

C. Sensitive but Unclassified Information (SBU) -For Official Use Only -, which consists of any other information which:

- (1 ) If provided by the government to the contractor, is marked in such a way to place a reasonable person on notice of its sensitive nature;
- (2) Is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements.”

Contractor will not require access to classified information under this SOW. The maximum level of classification is Fitness Only.

### **6.3 PERIOD OF PERFORMANCE**

The period of performance for this contract is a one-year base period with four one-year option periods as follows:

Base Period	June 15, 2023 through June 14, 2024
Option Period One	June 15, 2024 through June 14, 2025
Option Period Two	June 15, 2025 through June 14, 2026
Option Period Three	June 15, 2026 through June 14, 2027
Option Period Four	June 15, 2027 through June 14, 2028

### **6.4 PLACE OF PERFORMANCE**

The primary place of performance will be the Contractor’s facilities with occasional visits to the Department of Homeland Security facilities in the Washington Metro Area.

### **6.5 CONTRACTOR TELECOMMUTING – REMOTE PERSONAL RESIDENCE WORK LOCATIONS.**

Telecommuting for federal government contractors will be considered on a situational basis to the extent practicable to meet DHS mission needs. Telecommuting allows contractor personnel to perform their contractual requirements outside of CISA office locations, typically at a contractor’s personal residence or a corporate telecommuting office location. Telecommuting for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. The goal of telecommuting for contractor personnel is to enhance the delivery of services that support the DHS mission. Telecommuting is permitted under the task order in accordance with the requirements below.

Additionally, the provision to permit contractor telecommuting may be revoked at the Task Order level at any time if the Government makes such determination. The telecommuting provision does not change any task order requirements; all other terms and conditions of the task order remain in full force and effect.



## **6.6 CONTRACTOR LABOR RATES CHARGED WHILE TELECOMMUTING**

The contractor shall charge the same applicable fixed hourly rate as for a Government site for those contractor personnel when they telecommute at their designated telecommuting location.

## **6.7 HOURS OF OPERATION**

Contractor employees shall generally perform all work between the hours of 9:00 AM and 5:30 PM EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

## **6.8 TRAVEL**

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

## **6.9 POST AWARD CONFERENCE**

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than ten (10) business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held virtually.

## **6.10 PROGRAM PLAN**

The Contractor shall provide a draft Program Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Program Plan to the COR not later than twenty (20) business days after the Post Award Conference.

## **6.11 PROGRAM PROGRESS REPORTS**

The Program Manager shall provide a monthly progress report to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

## **6.12 PROGRESS MEETINGS**

The Program Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at the Contractor's facility or virtually as mutually agreed upon between the Government and the Contractor.

### **6.13 GENERAL REPORT REQUIREMENTS**

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications).

### **6.14 INTELLECTUAL PROPERTY**

Not Applicable

### **6.15 PROTECTION OF INFORMATION**

The Government will provide all necessary information, data and documents to the Contractor for work required under this contract.

The Government will provide copies of the references cited in SOW 1.4 at the Post Award Conference.

The Contractor shall use Government furnished information, data, and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

### **REFERENCES:**

DHS Management Directive 140-01, *“Information Technology System Security Program, Sensitive Systems”*

- DHS 4300A Policy Directive (Version 13.3, February 13, 2023).
- DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018 for NSS Collateral (Unclass, Secret or Top Secret Collateral).
- DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, Version 2.1, March 24, 2017 for TS SCI/C-LAN.

## 6.23 SECTION 508 COMPLIANCE

### 1.0 Section 508 Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at <https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5>. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

### 1.1 Section 508 Requirements for Technology Services

1. When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.
2. When modifying, installing, configuring or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.
3. When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at <https://www.dhs.gov/compliance-test-processes>.

4. When developing or modifying hardware components of ICT, including closed systems (for example – kiosks), the Contractor shall demonstrate conformance to the applicable Section 508 standards (including the Chapter 4 hardware requirements). Where the requirements in Chapters 4 do not address one or more functions of ICT, the Contractor shall demonstrate conformance to the Functional Performance Criteria specified in Chapter 3. The Contractor shall use a test process capable of validating conformance to all applicable Section 508 standards for hardware functionality delivered pursuant to this contract.
5. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

## 1.2 Section 508 Deliverables

1. **Section 508 Test Plans:** When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.
2. **Section 508 Test Results:** When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.
3. **Section 508 Accessibility Conformance Reports:** For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at <https://www.itic.org/policy/accessibility/vpat>. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.
4. **Other Section 508 Documentation:** The following documentation shall be provided upon request for ICT items offered through this contract:
  - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
  - Documentation on how to configure and install the ICT Item to support accessibility.



- Documentation of core functions that cannot be accessed by persons with disabilities.
- Documentation of remediation plans to address non-conformance to the Section 508 standards

## 7.0 GOVERNMENT TERMS & DEFINITIONS

Acronym	Definition
APO	Accountable Property Officer
APR	Annual Program Review
ATO	Authority to Operate
CDR	Critical Design Review
CISA	Cybersecurity and Infrastructure Security Agency
CLIN	Contract Line Item Number
COG	Continuity of Government
COOP	Continuity of Operations
COR	Contract Officer Representative
COT	Captive Office Test
DC	District of Columbia
DHS	Department of Homeland Security
DOT&E	Director Of Operational Test & Evaluation
DUNS	Data Universal Numbering System
DV&IS	Data, Voice, and Information Services
EA	Enterprise Architecture
ECD	Emergency Communications Division
EDMO	Enterprise Data Management Office
EIS	Enterprise Infrastructure Solutions
EIT	Electronic and Information Technology
EO	Executive Order
EOD	Entry on Duty
EoL	End of Life
EOP	Enhanced Overload Performance
EoS	End of Support
EPEAT	Electronic Product Environmental Assessment Tool
ESOC	Enterprise Security Operations Center
FCC	Federal Communications Commission
FOC	Full Operational Capability
FRD	Functional Requirements Document
FRS	Functional Requirements Specifications
GETS	Government Emergency Telecommunication Services
IAW	In Accordance With
ICT	Information and Communications Technology
IOC	Initial Operating Capability

Acronym	Definition
IOD	Integrated Operations Division
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IRR	Integration Readiness Review
IT	Information Technology
IXC	Interexchange Carrier
KPP	Key Performance Parameters
LEC	Local Exchange Carrier
MEO	Mission Enabling Offices
MD	Management Directive
MNS	Mission Need Statement
MoP	Method of Procedures
N/A	Not Applicable
NCR	National Capital Region
NDA	Non-Disclosure Agreement
NDAA	National Defense Authorization Act
NGN	Next Generation Network
NGN PS	Next Generation Network Priority Service
NIST	National Institute of Standards and Technology
NRMC	National Risk Management Center
NS/EP	National Security and Emergency Preparedness
NSA	Network Service Architecture
NSAT	Network Services Acceptance Test
OAM&P	Operations, Administration, Maintenance, and Provisioning
OCSO	Office of the Chief Security Officer
OEM	Original Equipment Manufacturer
OIG	Office of Inspector General
OM	Operation Measurements
OMB	Office of Management and Budget
ORR	Operational Readiness Review
ORT	Operational Readiness Test
OSS	Operations Support Services
OTRR	Operational Test Readiness Review
PCII	Protected Critical Infrastructure Information)
PCS	Priority Communication Services
PDR	Preliminary Design Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMO	Program Management Office
PoC	Proof of Concept
POC	Point of Contact
PPD	Presidential Policy Directive
PRR	Production Readiness Review

Acronym	Definition
PS	Priority Service
PSD	Personnel Security Division
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
PTS	Priority Telecommunication Services
SOW	Statement of Work
QPR	Quarterly Program Review
RSVP	Remote Service Verification Process
RTVM	Requirements Traceability and Verification Matrix
SA	Security Authorization
SaaS	Software as a Service
SBU	Sensitive but Unclassified Information
SCG	Security Classification Guide
SDD	System/Software Design
SED	Stakeholder Engagement Division
SELC	System Engineering Life Cycle
SF	Standard Form
SME	Subject Matter Expert
SOC	Security Operations Center
SORN	System of Records Notice
SP	Service Provider
SPC	Service Provider Council
SRAS	Special Routing Arrangement Service
SSI	Sensitive Security Information
SSN	Social Security Number
SSP	System Security Plans
TBD	To Be Determined
TDM	Time Division Multiplex
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TEM	Technical Exchange Meetings
TIM	Technical Interchange Meetings
TRM	Technical Reference Model
TSP	Telecommunication Service Priority
UE	User Equipment
URL	Uniform Resource Locators
USGv6	U.S. Government Version 6
WPS	Wireless Priority Service

## 8.0 GOVERNMENT FURNISHED RESOURCES

The Government will not furnish any resources to the Contractor in support of this contract.

## **9.0 CONTRACTOR FURNISHED PROPERTY**

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in SOW 1.4.1.

### **9.1 Property Inventory**

No property is associated with this contract.

### **9.2 Notification of Property Receipt**

No property is associated with this contract.

### **9.3 Monthly Asset Management Report**

No property is associated with this contract.

### **9.4 Invoice/Receipts**

No property is associated with this contract.

## **10.0 INVOICES AND PAYMENT PROVISIONS**

Invoices shall be prepared per Section VII, Contract Clauses; Paragraph A. entitled "FAR CLAUSES INCORPORATED BY REFERENCE," FAR Clause 52.232-25 Prompt Payment, and FAR Clause 52.232-7, Payments under Time and Materials and Labor-Hours. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

- 1) Cover sheet identifying DHS;
- 2) Task Order Number;
- 3) Modification Number, if any;
- 4) UEI Number;
- 5) Month services provided
- 6) CLIN and Accounting Classifications
- 7) Contract Line Item Number (CLIN) and description for each billed item.
- 8) Any additional backup information as required by this contract.
- 9) ATTN: CISA/ECD

The contractor shall submit invoices monthly. The Contractor shall submit the invoice electronically to the address below:

E-mail: TBD

Simultaneously the Contractor shall provide an electronic copy of the invoice to the following individuals at the addresses below:





**Attachment 1 - SOW**  
**70RCSJ23Q00000045**

The contractor shall submit invoices to the email addresses above. Additionally, the contractor shall prepare and submit a sufficient and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for payment. The contractor shall attach back up information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or electronic acceptance by the COR and date of acceptance shall be included as part of the backup documentation.

If the invoice is submitted without all required back up documentation, the invoice shall be rejected. The Government reserves the right to have all invoices and backup documentation reviewed by the Contracting Officer prior to payment approval.