UNITED STATES DEPARTMENT OF HOMELAND SECURITY
SCIENCE AND TECHNOLOGY DIRECTORATE
OFFICE OF NATIONAL LABORATORIES
TRANSPORTATION SECURITY LABORATORY

INFORMATION TECHNOLOGY SUPPORT SERVICES

DRAFT STATEMENT OF WORK

1.0 GENERAL

Background

The mission of the United States Department of Homeland Security (DHS) Directorate of Science and Technology (S&T) Office of National Laboratories (ONL) Transportation Security Laboratory (TSL) is to apply our scientific and technical acumen to advance explosives and contraband detection technologies for the Homeland Security Enterprise (HSE). Established in 1992 at the William J. Hughes Technical Center, Atlantic City Airport in New Jersey, the TSL's 20-acre secure campus includes specialized explosive storage and handling areas and a multi-scientific laboratory infrastructure designed for test and evaluation of technology for explosives and contraband detection and blast mitigation.

With its staff of federal employees and contractors including physicists, chemists, engineers, and mathematicians, the TSL is internationally recognized for its unique ability to advance detection technology from conception to deployment through applied research, test and evaluation, assessment, and certification testing.

1.1 Scope

The scope of work for this acquisition includes labor, supplies, equipment, and materials necessary to provide technical support services to the TSL and alternate locations such as the Detection Technology Center (DTC): Approximately 146 Contractor personnel and 60 Federal personnel at TSL with 18 other personnel at alternate locations. This includes enterprise information technology infrastructure and helpdesk support, Network Attached Storage (NAS) configuration and support, Microsoft and Linux Network systems administration, IOS, iPadOS, macOS administration, container-based development environments, management and storage of source code, Share Point development, and software and database development.

These functions provide support to all divisions and areas within the TSL domain. The technical support will be in accordance with the task requirements outlined in this Statement of Work (SOW). Generally, support for alternate locations such as DTC will be conducted remotely however occasional, ad-hoc travel may be necessary.

1.2 Objective

The objective of this project is to provide the TSL with essential support services that are not

inherently governmental and may require a level of effort that is not sufficiently consistent to warrant additional staffing with federal employees. The intent is to maximize the efficient use of TSL assets in support of the Homeland Security mission by ensuring appropriate support resources are in place to effectively manage IT resources, to support known and future software and database development efforts, and to provide laboratory wide IT helpdesk support services including end user account administration and support, network administration of multiple independent and secure networks.

1.3 Applicable Documents

The contractor shall comply with requirements of the following documents, updated as required, to meet the requirements of this contract:

- National Industrial Security Procedures Operation Manual (NISPOM);
- 49 CFR 1520 Protection of Sensitive Security Information;
- DHS IT Security Program Publication DHS MD 4300.Pub;
- TSL Publication Guidelines;
- DHS/S&T/TSL Document Format Templates;
- DHS Instruction 121-01-011;
- HSAR Class Deviation 15-01 Safeguarding of Sensitive Information; and
- DHS S&T Explosives Research and Development Program Security Classification Guide, DHS SCG S&T-006, (current version).

These reference documents can be accessed through an Internet search engine except the DHS SCG S&T-006 and the DD-254. These two documents will be provided after award.

1.4 Reference Documents

The following documents will be reviewed by the contractor in performing the work described in the SOW and will be provided upon award or post-award:

- DD 254;
- TSL Management Directives; and
- TSL Management Instructions.

1.5 Performance Requirements Summary

This contract includes a Performance Requirements Summary (PRS) in section 10.0. The PRS plays an integral role in the administration of the contract. In addition to any applicable inspection clauses or other related terms and conditions contained in the contract, the PRS shall serve as a primary tool for inspection and acceptance of services as facilitated by the Contracting Officer's Representative (COR) and alternate COR. Evaluation of the contractor's overall performance shall be in accordance with the performance standards set forth in the PRS, and will be conducted by the COR/alternate COR. The PRS constitutes a material aspect of the contract and will not be changed or otherwise modified without prior written approval of the Contracting Officer.

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 Information Technology and Helpdesk Support

As an active federal research laboratory, the TSL generates a significant quantity of data and reports. These are designated as Sensitive Security Information (SSI), For Official Use Only (FOUO), Classified, or For Public Release. The TSL is heavily dependent on the data that is developed during testing at on-site and at off-site locations and the subsequent reports which are generated during that testing in order to perform the mission and support the TSL customers. Additionally, the federal and on-site support staff depend on connectivity to the internet and DHS intranet to conduct day-to-day business. To support this work, the contractor shall:

2.1.1 Provide end user helpdesk support for local IT issues to include:

2.1.1.1 In person and remote (e.g., telephone, MS Teams, or other approved access tools) support for government-owned and/or issued IT products including laptops, desktops, monitors, hard drives, mobile phones, etc. The contractor shall also assist and support government-owned laboratory instruments/computers, connections, data backup, and operations (e.g., software installs). Limited support shall also be provided for vendor owned equipment such as support interfacing, data transfers, etc.;

2.1.1.2 In person and remote support, including installation, configuration, troubleshooting, and working with S&T Headquarters (HQ) for all DHS-owned and/or approved issued software requests using manual or remote install/updates, Microsoft Endpoint Configuration Manager or other supported methods;

2.1.1.3 In person and remote support for network connectivity request;

2.1.1.4 Maintain all workstations in Microsoft Endpoint Configuration Management System, install updates, vulnerability management and other associated function;

2.1.1.5 Image workstations for deployment on all networks and monitor images for completeness;

2.1.1.6 Supplement missing software and patches as required. This includes unclassified and classified standalone workstations for use in special case and secure rooms and areas;

2.1.1.7 Build and configure custom Linux and Windows workstations for data collection and analysis;

2.1.1.8 Install, maintain, and gain authorization for installation of Commercial Off The Shelf (COTS) and custom vendor software and update as needed to latest versions;

2.1.1.9 Work with OEM and third party vendors to provide support, updates, resolve issues and fixes to software including connection to networks as required;

2.1.1.10 Work with TSL Federal staff for IT hardware refreshments for End Of Life equipment as needed, generally every 3-4 years;

2.1.1.11 Support all cloud-based software systems and maintenance;

2.1.1.12 Design and provide end user support for automation of Microsoft Office applications to streamline TSL processes and increase efficiency and data management;
2.1.1.13 Recommend software and hardware upgrades for users' existing programs and systems;
2.1.1.14 Suggest innovative solutions to resolve or enhance operations; and
2.1.1.15 Manage group Software Licenses as needed for common software.

2.1.2 Communications and Video Teleconferencing (VTC) equipment maintenance and support activities including:

2.1.2.1 Deploy, configure, maintain, and troubleshoot various communications equipment in use at the TSL. This includes:

a. Government issued cellular phones and devices (i.e. range extenders, wireless access points, etc.);
b. Wired and Wireless Connections, Encryption, Virtual Private Network (VPN), and other hardware devices and software for on and off local network connections;
c. Maintain, update and troubleshoot VTC and presentation systems throughout TSL campus. Main Conference Room(s) and one Secure Conference room have VTC and presentation systems, and four additional conference rooms, which have presentation systems only;
d. Provide audio visual support (e.g., microphones, enable closed captioning, ensure IT-related accessibility needs are met, etc.) for presentations as required;
e. Move and/or setup up IT-related hardware (e.g., phones, PC, etc.) and software for new or existing laboratory staff; and
f. Support and repair land line analog and digital telephones and related equipment (e.g., cellular extenders).

2.1.1.16 Support wireless access zones throughout the TSL campus

2.1.3 Maintenance, utilization, and management of end user helpdesk ticket system (currently in SharePoint) to ensure that all end user requests for assistance are accurately tracked, routed, and responded to or escalated as needed.

2.1.3.1 Optimize, redevelop, and/or improve current IT ticket system to better respond to customer needs and be more informative to the ticket submitter. Include current status, delays, issues, escalation to S&T or other entity with details as needed or at the direction of the Technical Monitor (TM).

2.1.4 Support and administration for Property and Asset Management to include:

2.1.4.1 Assume the role of the IT Property Custodian (PC) under the TSL Accountable Property Officer (APO);

2.1.4.2 Add new IT related assets to inventory and obtain all paperwork regarding acquisition;
2.1.4.3 Place into excess inventory all IT assets that have reached end of life;
2.1.4.4 Track, maintain, and notify users of property pass expirations for all TSL laboratory personnel;
2.1.4.5 Maintain and track inventory changes via TSL Inventory Database as well as the Sunflower Asset Management System (SAMS) database at S&T HQ for IT assets;
2.1.4.6 Maintain and support inventory scanners, hardware, and software products used in the collection of inventory information;
2.1.4.7 Research and assist with the purchase and budgeting of IT hardware and software; and
2.1.4.8 Maintain records for all software and IT related subscriptions and provide notifications well in advance of expiration dates in order to ensure that there is no lapse in service or support. Examples include OriginPro, MATLAB, LS-DYNA, COMSOL, Red Hat Enterprise Linux (RHEL), and others.

2.1.4.8.1 The contractor shall ensure software is kept up to date to address security issues.
2.1.4.8.2 The contractor shall recommend to the government adjustments to the quantity of software licenses to meet end user needs.
2.1.4.8.3 The contractor shall recommend software to enhance the efficiency of the TSL and will perform the necessary market research if requested by the TM.
2.1.4.8.4 Maintain/distribute licensing for vendor software, update software, submit for Software Exception Request (SER) as necessary to gain approval for network access and installation.
2.1.4.8.5 Research, test, and verify proper deployments, functioning of software patches and fixes and remediate as necessary.

2.1.5 Data Storage and Transfer activities including:

2.1.5.1 Configure and maintain Network Attached Storage (NAS) drives for lab data collection;
2.1.5.2 Configure and maintain TSL Network Attached Storage (TSLNAS) for archiving lab data to primary and duplicate Dell Power Scale Petabyte storage solutions;
2.1.5.3 Assist laboratory staff in uploading and organizing data on TSL storage devices, approved third party IT resources, and/ or Government-owned IT equipment/instruments to the TSLNAS or other location as required to meet laboratory needs;
2.1.5.4 Migrate data to and from various IT equipment and perform system backups, as required, to maintain data integrity;
2.1.5.5 Recover and restore files from backups as required;
2.1.5.6 Maintain archives of all user and laboratory data;
2.1.5.7 Configure and maintain closed loop networks to interconnect laboratory

equipment for data storage and backup;

2.1.5.8 Perform data recovery from failed equipment, both encrypted and non-encrypted;

2.1.5.9 Deploy research and recommend refreshment desktops and laptop systems for End Of Life, failed, and replacement systems; and

2.1.5.10 Perform and/or assist with data transfer of DHS data and work products to approved DHS partners via DHS-approved means such as the use of NAS drives, hard drives, cloud-based transfer, etc.

2.1.6 Security Updates and System Patching duties including:

2.1.6.1 Identify and update Government-owned or issued devices and/or workstations that have critical vulnerabilities and or security issues

2.1.6.2 Advise users on security procedures and verify conformity

2.1.6.3 Maintain and update hardware to meet security policy dictated by S&T HQ

2.1.7 Provide hardware life-cycle support/end of life replacement to include hardware installations and upgrades such as graphics cards, memory chips, external devices, and other small hardware items and peripherals.

2.1.8 Provide support for printers/multi-function printers such as changing toner, installing drivers for users, maintaining network connection, and maintaining printer supplies. The TSL has ~ 20 network printers/multifunction printers located through the TSL campus and several small desktop printers in cubes for printing more restricted documents.

2.1.9 Provide maintenance of TSL local IT Systems & equipment and support connectivity and troubleshooting functions related to TSL Headquarters mandates.

2.1.10 Create/establish and update as needed both SciTech and Labnet user accounts at the TSL for all TSL federal and contractor personnel.

2.1.11 Education of staff members through training and individual support for software and hardware applications.

2.2 Network and Hardware Support and Administration

2.2.1 Maintain Networks

2.2.1.1 Ensure, maintain, and optimize the health and availability of all networks that TSL is dependent on, including:

2.2.1.1.1 LAN A, LAN B, LAN C, SciTech, Labnet, Wireless, Closed Loop, Lab Equipment, Cloud Based, Building Management, Security (including access points and camera systems), PIV, Homeland Secure Data Network (HSDN), Homeland Security Information Network (HSIN), internal land

line telephone network, cellular extenders, electronic mail, high performance clusters, and Printer and Print Servers

2.2.1.2 Promptly identify and resolve network issues as they occur
2.2.1.3 Work with S&T HQ to deploy fixes and rectify issues.
2.2.1.4 Work with external agents as needed in order to maintain infrastructure integrity
2.2.1.5 Escalate all identified issues as appropriate
2.2.1.6 Upgrade and maintain network infrastructure when required.
2.2.1.7 Configuration and management of networking technologies (OSI network layers, TCP/IP).
2.2.1.8 Administration, performance tuning, and system monitoring
2.2.1.9 Verify stability, interoperability, portability, security, or scalability of system architecture.

2.2.2 TSL Laboratory Asset support including:
2.2.2.1 Assist in the installation and maintenance of IT-related resources for laboratory equipment/instruments
2.2.2.2 Connect laboratory equipment/instruments to current IT infrastructure or other equipment as required
2.2.2.3 Install custom software and assist vendor with updates
2.2.2.4 Direct connections of Vendor Equipment, emulators, and test equipment to TSL NAS, NAS and other devices for data storage. Backup NAS and other equipment, recover data, etc. as need to requested by the TM
2.2.2.5 Configure and interface TSLNAS with vendors test imaging and scanning systems

2.2.3 Secure Rooms
2.2.3.1 Copy and move data between secure workstations
2.2.3.2 Maintain logs
2.2.3.3 Oversee destruction of digital media and documents in accordance with ISO/National Institute of Standards and Technology (NIST) regulations
2.2.3.4 Serve and act as the backup for ISSO (Information System Security Officer) duties as required.
2.2.3.5 Assist the government with investigation, cleanup, and remediation of data in the event of a classified spill or other unauthorized disclosure event.

2.2.4 User Account Management activities including:
2.2.4.1 Maintain and update users accounts in Active Directory (AD)
2.2.4.2 Grant users network access and assign permissions and network memberships
2.2.4.3 Update user, machine, mobile phone, and other certificates to allow network access
2.2.4.4 User PIV Card maintenance
2.2.4.5 Issue and track Property Passes for users to remove DHS owned equipment from the TSL
2.2.4.6 Maintain security paperwork for users' property upon their exit and verify its return
2.2.4.7 User migration between networks and updates to email and servers as required or

requested by the TM

2.2.5 Write, update and maintain standard operating procedures (SOP) that details the steps required to regain Local Area Network access in the event of network failure. The SOP should be sufficiently detailed so that if the individual mainly responsible for network administrator functions or their designee is not available, that any minimally qualified technician may restore network services. The SOP shall be treated as Security Sensitive Information and distribution shall be controlled and restricted. In addition, write update and maintain SOPs for installation, repair, troubleshooting and other aspects of normal operations for software and hardware.

2.2.6 Review current network configuration and implementation at TSL main location and satellite locations. Recommend upgrades and suggest improvements to enhance current IT infrastructure. Implement noted upgrades and improvements as directed by the government and in conjunction with S&T Engineering teams.

2.3 Software/Database Development and Administration; Special Projects

The contractor shall serve as TSL's agent for cataloging, storing, retrieving and generating a variety of information, documentation, and briefings. The contractor shall be responsible for developing, administering, and maintaining a wide variety of custom software, request systems, and database products by gathering user requirements and then analyze, design, and develop software to meet those requirements. The contractor shall be able to design and develop solutions to complex applications problems, system administration issues, or network concerns and perform systems management and integration functions. Additionally, the contractor shall be responsible for the installation, configuration, and troubleshooting of Linux-based systems and high-performance computational clusters.

The contractor shall deploy and manage Sharepoint server on premise and/or Office 365 Enterprise, taking advantage of latest features and capabilities, modernize site pages, web parts and authorization.

The contractor shall analyze and design databases within an application area, working individually or coordinating database development as part of a team including systems analysts, engineers, and other programmers.

Additionally, the contractor shall ensure that all projects are properly planned, scoped, and that anticipated timeframes and/or milestone schedules are provided to the government and agreed upon prior to commencing work. Consideration shall be given to ensuring that proper resources are attributed to each project and that priorities are established and managed when multiple projects are being conducted.

Duties shall include:

2.3.1 Support, Troubleshoot and maintain System/software life-cycle to include development and maintenance of systems, applications and tools including software

enhancements, databases, database maintenance, test and evaluation systems, Training systems maintenance, automation and backup, and keep and maintain information systems security.

2.3.2 Design strategies for enterprise database systems and set standards for operations, programming, and security. Design and construct large databases of various types. Integrate new systems with existing warehouse structure and refine system performance and functionality. Examine and identify database structural necessities by evaluating operations, applications, and programming. Assess database implementation procedures to ensure they comply with internal and external regulations. Prepare accurate database design and architecture reports for management and stakeholders. Oversee the migration of data from legacy systems to new solutions.

2.3.3 Data management functions and the maintenance of software resources including the removal of outdated/duplicate/unnecessary files to ensure optimum performance and reliability. The contractor shall conduct the creation of models and diagrams showing programmers the software code needed for an application and ensure that programs continue to function normally through software maintenance and testing. Proper detailed documentation is required as a reference for future maintenance and upgrades.

2.3.4 Maintain software tools and utility development to include providing unique capability (i.e. VBA for macros) working with off the shelf applications such as Adobe, Excel, Access, PowerPoint, Teams and other Microsoft and DHS applications. Databases, briefings, spreadsheets and documents shall be developed from these applications to provide information and information management tools. This includes the Local Area Network (LAN) and web administration, application training, electronic and paper file management, and Documentation of TSL IT department system and procedures.

2.3.5 Infrastructure support for Machine learning and Artificial Intelligence support for projects, including Docker, Kubernetes, RedHat, and associated technologies. Linux support with GPU and systems. Responsibilities include:

2.3.5.1 Linux administration and desktop support.
2.3.5.2 Ability to package and ship programs and code via a container platform (e.g. Docker).
2.3.5.3 Configure and maintain infrastructure to ensure packaged containers can interface with current IT infrastructure (e.g. TSL NAS, GPUs).
2.3.5.4 Configure and maintain tools to deploy, scale, and manage containers.
2.3.5.5 Develop and maintain a repository for tracking and storing source code such as GitLab, GitHub and similar repositories.
2.3.5.6 Creation of scripts (e.g. using Perl, Ruby, Python) and setting up software for automation.

2.3.6 Infrastructure support for high performance computing projects. Responsibilities include:

2.3.6.1 Administration of the cluster(s) and desktop support.
2.3.6.2 Ensuring optimal system performance, reliability and scalability.
2.3.6.3 Creation of scripts and setting up software for automation, such as the automated scheduling of computational jobs.
2.3.6.4 Configure and maintain infrastructure to ensure computational packages can be utilized to their optimal capabilities by laboratory users.
2.3.6.5 Assist as needed to ensure TSL laboratory staff can access computational resources from other government agencies (e.g., DoD) or government approved cloud-based sources as required or directed by the TM.

2.3.7 Several special, short-term projects will be underway or will be launched by the TSL during the course of the contract that the contractor shall be responsible for advising, planning, implementing, maintaining, developing and/or refining Examples of these projects include the Project Deliverables Tracking System, the Procurement Request Database, the Contracts Database, and X-ray CT augmentation tool (XCAT). Other projects of this nature will be required as well.

2.3.7.1 Project Deliverables Tracking System. The contractor shall conduct a review of the current systems in place and make recommendations as to whether to optimize the existing framework to maintain and update, as needed, the current SharePoint system for managing the workflow and tracking of document-based deliverables or to develop a new system for the same purpose. The Project Deliverables Tracking System enables TSL federal or contractor staff to upload an item for review, enable the Business Operations support staff to assign or manage workflows, and enable the deliverable to be assigned for technical report processing. The Tracking System provides the ability to obtain reports on overall processing time for deliverables by POC, functional group, or document type to enable optimization of TSL processes.
2.3.7.2 Procurement Request database. The contractor shall conduct a review of the current systems in place and make recommendations as to whether to utilize the existing framework to maintain and update, as needed, the current system for managing the workflow and tracking of procurement requests or if a new system should be developed. The Procurement Request database is the system that has been developed for the purpose of tracking PR activity originating from the TSL. It also houses a document repository for all related acquisition documents. The government would look to replace the current system or expand upon the functionality of the existing system.
2.3.7.3 Contracts Database. The contractor shall perform an assessment of all contract related systems, repositories, and documents that are utilized by the TSL during the lifecycle of a contract. The results of the assessment shall be used to provide recommendations regarding the development of a

customized contract management platform for use by TSL employees or the use of comparable COTS programs if appropriate. The intent of the platform is to provide a centralized, network agnostic system (accessible for SciTech and LANA users) for use by authorized TSL employees for managing contracts and related documentation. The platform shall be able to capture and display information related to all phases of the contract management lifecycle, including:

2.3.7.3.1 Contract inception information including funding information, TSL PR number, STPR number, contract documentation (SOW, IGCE, etc.), contact information, description of effort, stakeholders, etc.

2.3.7.3.2 Contract management information including awarded amount, CO contact information, invoicing information with amounts and copies of the documents, PRISM number(s), modification number(s) and descriptions with copies of the documents, deliverables, contract travel, contract personnel information, etc.

2.3.7.3.3 Contract closeout information including fields to capture V&V and de-obligation information and documents, CPARS related information, etc.

2.3.7.4 XCAT – XCAT is a Python-based software application developed by the TSL. It enables the design, manipulation, and insertion of threat objects into previously scanned luggage. The properties of the threat object (e.g., computed tomography number, Z-effective, density) are retrieved from a library and digitally placed in the desired location within the luggage. The image is then reconstructed by back calculating the corresponding sinogram, followed by forward projection of the correct images based on the explosive detection technologies (EDTs) settings and material properties, ensuring accurate capture of the X-ray scattering characteristics. The contractor will be responsible for the continued development of the software, which includes fixing bugs; optimizing the image generation process through parallelization and GPU configuration; coding and installing the software onto networked computers; improving the graphical user interface; enhancing the software based on requested changes from the test and evaluation teams; and collaborating with physicists to incorporate new system parameters based on the configuration of additional EDTs. This work will require the contractor to perform the above requirements in addition to the following:

2.3.7.4.1 Create and improve software applications, ensuring the ability to expand existing systems to meet evolving requirements.

2.3.7.4.2 Focus on developing robust software that can handle errors gracefully and continue functioning effectively.

2.3.7.4.3 Design and implement scalable solutions that can handle increased demand and automate processes to improve efficiency.

2.3.7.4.4 Establish and support multiple platform versions of software packages to ensure compatibility across various systems.

2.3.7.4.5 Develop, improve, and deploy Diffusion models and other AI/ML algorithms to generate synthetic images.

2.3.7.4.6 Design and assess tools for evaluating the quality and accuracy of synthetic images.

2.3.7.4.7 Apply knowledge of gaming development and virtual environments (e.g., Blender) for creating and manipulating 3D models and synthetic visuals.

2.3.7.4.8 Conduct tests to ensure the accuracy, functionality, and performance of the software and synthetic image generation systems.

2.3.7.4.9 Write and maintain detailed test plans for software validation and performance assessment.

2.3.7.4.10 Analyze user feedback and performance data to identify areas for improvement in software and image generation models.

2.3.7.4.11 Implement refinements and updates to applications based on feedback and test results to improve user experience and performance.

2.3.7.4.12 Collaborate with other teams to integrate AI models, gaming development, and virtual environment tools into the overall system.

2.3.7.4.13 Continuously monitor and optimize the performance of AI models and synthetic image generation systems.

2.3.7.4.14 Perform software or computer engineering analyses and interface with security-related systems to assess the potential for further development, integration, and usefulness in the intended environment.

2.3.7.5 When possible and advantageous, the platform shall interface with existing systems in use within DHS S&T (S&T PR Tracker, STATS, etc.) for the purposes of pulling relevant data (PR numbers, contract numbers, financial information, etc.)

2.3.7.6 Optimize, redevelop, and/or improve current IT ticket system to better respond to customer needs and be more informative to the ticket submitter. Include current status, delays, issues, escalation to S&T or other entity with details as needed or at the direction of the Technical Monitor (TM).

2.3.7.7 Maintain and update current TSL SharePoint site and applicable user request systems to ensure they meet end-user requirements and retain software/hardware compatibility with TSL IT infrastructure.

2.3.8 The contractor will support other relevant and within scope activities as identified by the COR/alternate COR throughout the life of the contract.

3.0 CONTRACTOR PERSONNEL

3.1 Qualified Personnel

The Contractor shall provide experienced and qualified personnel with all the skills necessary to perform the work identified. All Contractor personnel must have a security clearance at the SECRET level as well as DHS Suitability in order to perform work under this contract. Required experience levels, training, qualifications, licenses, security clearances, DHS Suitability, or certifications must be obtained prior to commencement of work at Contractor expense.

3.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

3.3 Labor Categories and Key Personnel

The Contractor shall provide resumes of all key personnel designated in this SOW. The contractor shall notify the CO, COR, and alternate COR prior to making any change in the individuals identified in the proposal and/or assigned to this contract. Before replacing any individual designated as *Key* by the Government, the contractor shall notify the Contracting Officer, COR and alternate COR 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 table lists contractor personnel that are designated as Key for this requirement. Note: The Government may designate additional contractor personnel as *Key* at the time of award.

TABLE 1

Labor Category	FTE
Project Manager Level II	0.1
Cloud SME Level III	1.0

Systems Engineer Level III	1.0
Applications Developer Level III	1.0
Systems/Data Architect Level III	1.0
TOTAL KEY FTEs	**4.1**

The following table lists contractor personnel that are non-Key for this requirement. General position descriptions for the required labor categories can be found in Attachment III – Labor Category Descriptions.

TABLE 2

Labor Category	FTE
Systems Engineer Level III	1.0
O&M System Engineer Level II	1.0
Applications Developer Level II	2.0
TOTAL NON-KEY FTEs	**4.0**

3.4 Employee Identification

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.

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.

3.5 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.

3.6 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion, 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.

3.7 Non-Disclosure Agreements

All contractor personnel are required to sign non-disclosure agreement (DHS Form 11000-6) upon starting work and as deemed necessary under this contract to protect proprietary and/or source selection information.

4.0 OTHER APPLICABLE CONDITIONS

4.1 Security

The contractor will have access to DHS information systems. Contractor access to classified information may be required under this SOW. The maximum level of classification is Secret. The details will be specified in a DD Form 254.

FAR clause 52.204-2 Security Requirements Clause (prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of information released by the U.S. Government Executive Branch Departments and Agencies to their contractors; the proscribed Federal guidance is the National Industrial Security Program Manual [NISPOM]).

DHS has and will exercise full control over granting, denying, withholding, or terminating unescorted Government facilities and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the contractor to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment contractor fitness (suitability) authorization will follow as a result thereof. The granting of a favorable EOD decision or a full contractor fitness (suitability) authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order. No employee of the contractor shall be allowed unescorted access to a Government facility, access to any sensitive information or access to DHS IT Systems without a favorable EOD decision or contractor fitness (suitability) determination by the DHS Office of Security.

Contract employees assigned to the task order not needing access to sensitive DHS information, DHS systems or access to DHS facilities will not be subject to security contractor fitness

(suitability) screening. Contract employees waiting for an EOD decision may not begin work on the contract/task order.

DHS has determined the contractor and/or subcontractor employee access to CUI or government facilities does have to be limited to U.S. citizens and lawful permanent residents. Contractor will require recurring access to government facilities. Limited access to Government buildings is allowable prior to the EOD decision if the contractor is escorted by a government employee. This limited access is to allow contractors to attend briefings, nonrecurring meetings, and begin transition work. Classified information is Government information which requires protection in accordance with Executive Order 13526, National Security Information (NSI) as amended and supplemental directives. If the contractor has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. If the contractor is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

Contractor will be required to access controlled unclassified information (CUI) in the form of Sensitive Security Information (SSI) under this SOW. Examples of SSI that the Contractor may access includes but not limited to, certain protected threat identification and properties and millimeter wave simulant formulations. Contractor will not be required retain CUI on behalf of the government. CUI will be kept in accordance to federal records schedule. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination. Contractors will use DHS SharePoint, SciTech, LabNet, and Homeland Security Data Network (HSDN) to collect, process, store or transmit any controlled unclassified information in connection with this SOW. SSI will/will not be shared with any third parties.

In addition to the incident reporting requirements in HSAR 3052.204-72(c), contractors and subcontractors shall report, within 24 hours, all known or suspected incidents (e.g., Privacy, security, IT, classified spill, etc.) to the following entities: **S&T Incident Reporting E-mail:** STIncidentReporting@st.dhs.gov.

Research work must be conducted in accordance with DHS privacy policies, to include the Fair Information Practice Principles (FIPPs). DHS privacy policy requires that privacy sensitive research programs and projects complete a Privacy Threshold Analysis (PTA). The PTA is a living document, which must be updated if there are changes to the activity, changes to data sets, user access to the data, and/or the technology and systems used. Additionally, the DHS Chief Privacy Officer schedules completed PTAs for mandatory review at least every three years. The project or activity will not be in compliance with Departmental privacy requirements until all necessary privacy compliance documentation requirements have been completed. Prior to any connectivity being established to DHS systems or access being granted, the performer and the S&T PM shall meet with S&T CIO and Privacy to clarify and refine the minimum set of requirements and access controls necessary for this effort. The performer must ensure compliance with NIST-800 Rev 5 and DHS 4300A security and privacy requirements, including the completion of an authorization to operate (ATO). These requirements collected by S&T CIO and S&T Privacy will drive the actual IT connections that are authorized.

The S&T program office will facilitate engagement with the respective DHS legal and Compliance Offices (to include, but not limited to, privacy, security, and the Compliance Assurance Program Office) to ensure adherence to applicable statutory requirements and DHS policies and guidance.

Secure Software Compliance

The purpose is to provide the Federal Government assurances that software used by agencies is securely developed and the Federal Government understands exactly what the constituent components of said software through an industry accepted reporting format. This information may be disclosed as generally permitted under Executive Order 14028, Improving the Nation's Cybersecurity (E.O. 14028) and Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18), as amended. This form collects contact information from vendor employees who make the attestation. Cybersecurity and Infrastructure Security Agency (CISA) has produced a Self-Attestation Common Form that is used and can be found here. It addresses numerous topics such as: the background on the requirement; what software is within scope; how attestation is to be performed; who is to sign the form; how compliance is to be demonstrated and other administrative items such as submissions for the same software to another Federal agency. Software used in the process of adding capabilities to a government project must follow the latest FAR regulations regarding identifying all coding libraries used to build any capability used in a government project. All code must be verified by the provider by way of a Letter of Attestation indicating the code (including all code libraries) developed by the software producer presently makes consistent use of the secure software development framework (SSDF) and is free of defects and does not have viruses, flaws or other imperfections that would cause harm.

All code and associated libraries are to be listed on a Software Bill of Materials (SBOM) in an industry standard format such as Software Package Data Exchange (SPDX), CycloneDX, or Common Platform Enumeration (CPE). The SBOM is a chained inventory that lists and records software components, effectively showing an entire supply chain.

Note: A "software bill of materials" (SBOM) has emerged as a key building block in software security and software supply chain risk management. A SBOM is a nested inventory, a list of ingredients that make up software components.

The contractor shall adhere to all applicable government laws, regulations, orders, guides, and directives pertaining to classified, Sensitive but Unclassified (SBU), FOUO, or personally identifiable information. The contractor shall safeguard SBU, FOUO information specifically in accordance with the DHS Management Directive 11042.1; and DHS Instruction 121-01-011.

Foreign end products and services are not applicable to this SOW.

If applicable, contractor support will not be needed for the completion of any privacy compliance documentation.

4.2 Access to DHS Facilities and Resources

DHS may exercise full control over granting, denying, withholding, or terminating unescorted access to DHS facilities, DHS systems, and/or sensitive DHS information for government/contract employees. Access will be based upon the results of a DHS fitness/suitability investigation. DHS may, as appropriate, make favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the government/contract employee to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full DHS fitness/suitability authorization will follow. The granting of a favorable EOD decision or a full DHS fitness/suitability authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the BPA/task order. No employee of the government/contractor shall be allowed unescorted access to a DHS facility, access to any sensitive DHS information, or access to DHS Systems without a favorable EOD decision or DHS fitness/suitability determination by the DHS HQ Office of Security. Government/contract employees assigned to the BPA/task order not needing access to sensitive DHS information, DHS systems, or access to DHS facilities will not be subject to DHS fitness/suitability screening. Government/contract employees waiting on an EOD decision may not begin work on the BPA. Limited access to DHS facilities is allowable prior to the EOD decision if the government/contract employee is escorted by an approved DHS employee. This limited access is to allow government/contract employees to attend briefings, nonrecurring meetings, and begin transition work. During one's limited access the government/contract employee will not have access to sensitive or classified DHS information.

4.3 Classified Information

Classified information is government information which requires protection in accordance with Executive Order 13526, National Security Information (NSI) as amended and supplemental directives. If the government/contract employee has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. If the government/contract employee is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

Work on this contract cannot be performed unless the contractor personnel assigned to the labor categories are cleared at the appropriate levels as identified on each Task Order.

Prior to performing work, all contractor personnel must complete the suitability check process. All contractor personnel must execute non-disclosure agreements (NDAs, DHS Form 11000-6).

While contractor personnel are on-boarding and going through the suitability check process, the contractor shall submit information in its weekly reports to the COR indicating the progress, status, and action items for each individual going through the suitability check. The COR will further specify the format and due dates for the reports at award.

All work performed under this BPA should be considered unclassified unless specified otherwise. When classified work is required, DHS will provide specific guidance to the

contractor. The contractor shall adhere to all applicable government laws, regulations, orders, guides, and directives pertaining to Secret, Sensitive But Unclassified, FOUO, or personally identifiable information. The contractor shall safeguard Sensitive But Unclassified, FOUO information specifically in accordance with DHS Management Directive 11042.1.

The contractor shall establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of classified and sensitive government information, data, and/or equipment. If contractor personnel are ever uncertain about the handling or treatment of any information or data, they shall consult the COR.

All contractor personnel will be required to receive DHS Security Awareness Training and IT system rules of behavior training when performance commences, and thereafter. Contractors will significant security responsibilities may be required to receive specialized training. All personnel who access government IT systems will be monitored in their use. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer.

A DD Form 254 with a facility security clearance level of Top Secret that gives the Quoter the ability to hold clearances for its employees up to and including Top Secret/Sensitive Compartmentalized Information (SCI) will be completed and incorporated into the BPA. The Quoter will not need to store classified information at their facility.

The table below lists anticipated positions requiring clearances and their locations, although additional non-cleared positions will be required to support the contract. The Government may designate additional personnel as requiring clearance at time of task order award. At this time the Government anticipates that the clearance and locations listed below will be required. The Government may add or amend this list after award.

4.4 Security ID Requirements

Contractor personnel assigned to work at DHS S&T facilities may be issued a proximity pass that permits unescorted entry to the facilities without going through a daily visitor access process. Contractor personnel may also be granted certain other privileges such as email accounts and access to DHS information systems.

The Contractor shall obtain a government contractor identification card. The application for the card will be obtained through the COR or as directed by the Contracting Officer. The Contractor shall provide the COR written notice when all IDs have been processed and received. This card is in addition to contractor provided IDs. This access shall be provided solely at the discretion of DHS, and may be revoked or withdrawn at any time, without notice or cause, by the COR or Contracting Officer. The Contractor shall report in writing to the COR to request all personnel access to DHS facilities, email accounts, and information systems be terminated if:

- At any time during the term of this contract, contractor personnel issued a DHS pass or granted access to DHS email or any other DHS information system no longer require any further access; and/or

- At the completion, expiration, or termination of any such contract where access has been granted. Contractor personnel will be considered not to require access to DHS facilities for work performance upon expiration of this contract.

The contractor shall prepare and maintain a roster of its employees (both former and current) that have had government IDs issued in their names at any time during the term of this contract. This roster shall be submitted monthly, prior to the last day of each month, to the COR, or on request by the COR. The contractor may submit this report with the monthly progress report. Each contractor employee shall have the ID in his/her possession at all times when in the government facility. The employee shall surrender the card to the COR or issuing office at the end of employment, upon completion of this contract, or upon expiration of the form, whichever is sooner.

Contractor personnel must report the loss of a government ID as soon as possible to the COR or issuing office. Report the same day if lost during duty hours and by 9:00 a.m. the next workday if lost during non-working hours.

4.5 Encryption

All encryption shall be FIPS 197 Advanced Encryption Standard (AES) that has been FIPS 140-2 certified.

4.6 Critical IT System Duties and Responsibilities

In performing this requirement, the contractor shall abide by the following requirement, set forth in DHS Management Directive 4300A:

Components shall divide and separate duties and responsibilities of critical IT system function among different individuals to minimize the possibility that any one individual would have the necessary authority or system access to be able to engage in fraudulent or criminal activity. Independent Validation and Verification is but one critical systems function that needs to be performed by a provider (either government or contractor) other than the system designer-developer-operator.

4.7 Public Health Security and Bioterrorism Preparedness Response Act Requirements

All contractor personnel shall be subject to certain sections of the Public Health Security and Bioterrorism Preparedness Response Act of 2002. Specifically, as part of the suitability check process each contractor employee must complete a Federal Bureau of Investigation background check information form (OMB No. 1110-0039). Each contractor employee will be required to complete a training covering his or her responsibilities under the Act.

4.8 Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 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 & Appendix A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. 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.

4.8.1 Section 508 Requirements for Technology Services

4.8.1.1. When providing installation, configuration or integration services for ICT, the Contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

4.8.1.2. When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. - The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed upgrades, substitutions and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.2 508 (or successor versions). The template can be located at https://www.itic.org/policy/accessibility/vpat.

4.8.1.3. When providing Platform as a Service (PaaS) or Software as a Service (SaaS), the contractor shall ensure services conform to the applicable Section 508 standards (including the requirements in Chapter 5 for software and WCAG Level A and AA Level 2.0 success criteria for web and software. When the requirements in Chapter 5 do not address one or more software functions, the Contractor shall ensure conformance to the Functional Performance Criteria specified in Chapter 3.). The agency reserves the right to request an Accessibility Conformance Report (ACR) for PaaS and SaaS offerings. The ACR should be created using the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat.

4.8.1.4. When providing cloud hosting services (Infrastructure as a Service, Platform as a Service, Software as a Service, etc.) the Contractor shall ensure user administrative screens, dashboards and portals used to configure, and monitor cloud services conform to the Section 508 standards.

4.8.1.5. The Contractor shall ensure cloud hosting services shall not reduce the level of Section 508 conformance for ICT migrated by DHS to the cloud hosting environment.

4.8.1.6. 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.

4.8.1.7. 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.

4.8.1.8. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.

4.8.1.9. 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.

4.8.1.10. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys,

dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester.

4.8.1.11. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

4.8.2 Section 508 Deliverables (include in the SOW, PWS, or SOO)

4.8.2.1. 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.

4.8.2.2. 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 BPA.

4.8.2.3. 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.

4.8.2.4. 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; and
- Documentation of remediation plans to address non-conformance to the Section 508 standards.

4.9 System Design Compliance Requirements

All IT systems (as defined by DHS Management Directive 0007.1) being planned, designed, developed, and maintained for the Department of Homeland Security, Science and Technology Directorate (DHS-S&T), its customers, and/or with DHS data, shall be:

- Aligned with DHS and/or S&T Federal Enterprise Architecture. All solutions and services shall meet DHS Enterprise Architecture policies standards and procedures;
- In compliance with appropriate Office of Management and Budget (OMB) Circulars, including but not limited to OMB Circulars A-11 and A-130 as implemented by the S&T CIO;
- In compliance with Federal Regulations including but not limited to the E-Government Act (including Privacy Impact Assessment), Paperwork Reduction Act, Federal Information Security Management Act (FISMA), and Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194;
- In compliance with DHS Management Directives including 0007.1, 4010.2, 1400, 4300.1, (and 4300A), 4900, and others as appropriate; and
- All solutions and services shall meet DHS Enterprise Architecture policies, standards and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

    - All developed solutions and requirements shall be compliant with the HLS EA;
    - All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile;
    - Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository;
    - Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines;
    - Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. V480Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations

of conformance defined in the USGv6 Test Program; and
- Other guidance and best practices related to the Secure Coding Initiative and secure coding verification also apply.

4.10 Option Periods

Upon government approval to execute an option, the option period(s) will include a continuation of base period requirements in addition to any required work to address IT-related concerns and/or feedback from internal and external stakeholders.

4.11 Period of Performance

The period of performance for this contract consists of one (1) one-year base period with four (4) one-year option periods as follows:

Base Period	March 22, 2026 through March 21, 2027
Option Period 1	March 22, 2027 through March 21, 2028
Option Period 2	March 22, 2028 through March 21, 2029
Option Period 3	March 22, 2029 through March 21, 2030
Option Period 4	March 22, 2030 through March 21, 2031

4.12 Place of Performance

The primary place of performance is the TSL S&T facility in Atlantic City, NJ. Ad hoc support, both remote and in person, shall be required for alternate locations such as DTC in Huntsville, AL. Support for locations outside of Atlantic City, NJ would occur via travel or remotely. There is not a requirement for the contractor to staff any alternate locations.

4.13 Telework

While much of the project tasking generally does not lend itself to telework, the COR/alternate COR, may in some circumstances authorize the Contractor to enable contract employees to perform situational telework when an on-site presence is not required. Situational telework is sometimes also referred to as episodic, intermittent, unscheduled, or ad-hoc telework. Situational telework examples include telework as a result of inclement weather, lapse in government appropriations, special work assignments or other non-recurring events as determined and approved by the COR/alternate COR. Standard telework agreements are not authorized under this contract.

The Contractor shall provide adequate oversight of telework products to ensure contract adherence. The Contractor shall convey to its employees that teleworking is a privilege, not a right. The Contractor shall have a formal telework policy in place and on file with the COR/alternate COR and CO before situational telework is requested. Situational telework arrangements may commence with the COR/alternate COR approval under the following conditions:

1. Situational telework shall not result in an increase in the contract price. Any situational telework hours that are worked shall be charged at the lowest available rate for that labor category.

2. Requests for situational telework shall be sent directly from the contractor PM to the COR/alternate COR for approval. Requests for situational telework outside of this process will not be approved. Situational telework shall not commence until the COR/alternate COR has provided written approval.

3. The Contractor is responsible for continuity of performance in accordance with the terms of the contract.

4. Any equipment provided by the Government for situational telework purposes shall be treated as Government Furnished Equipment (GFE). A valid property pass must be on file for any GFE utilized for situational telework.

5. Situational telework considerations shall be based on job function and not on the individual performing the task. The COR/alternate COR will be responsible for making the determination as to which functions on a contract or task order are telework eligible.
6. Contractors with onsite positions that have been granted situational telework privileges may need to share a cubicle/desk space.

7. Individuals with offsite positions are to report to the Government or contractor facility as listed in the contract unless situational telework has been previously authorized. Offsite positions shall not be interpreted as being telework or telework eligible positions. All offsite work shall be completed at an approved government or contractor location, not from the employee's home unless situational telework has been approved and the COR/alternate COR have provided concurrence.

8. Any equipment provided by the Government for telework purposes will be treated as Government Furnished Equipment. Telework will be used for situational and case by case bases, as determined by the CO and or COR/alternate COR. Alternative Work Schedule (AWS), is not authorized.

4.14 Hours of Operation

Contractor employees shall generally perform all work between the hours of 7:00 a.m. and 6:00 p.m. Eastern Time at the TSL, Monday through Friday (except Federal holidays). Overtime will not be permitted. Occasional work outside of normal business hours, on weekends, and on holidays may be required.

4.15 Travel

See BPA SOW Section 4.14.

Travel locations may include Washington DC/ S&T Headquarters; site visits with technology

partners; various test locations, other government facilities; and conference locations (all CONUS) No foreign travel is required. All travel is subject to advance Government approval, by the Contracting Officer or COR/alternate COR. Approved travel outside of the defined local area will be reimbursed in accordance with the limits set forth in FAR Part 31 and the Federal Travel Regulation (FTR). This travel expense shall not be burdened with profit or fee, overhead, or general and administrative expenses (G&A).

4.15 Government-Furnished Facilities

Basic facilities such as workspace and associated operating requirements (e.g., phones, desks, utilities, computers, and consumable and general-purpose office supplies) will be provided to the contractor personnel working at the TSL facility.

4.16 Government-Furnished Property

Government Furnished Property (GFP) will be provided to the contractor. The Contractor may receive a laptop, IronKey, and similar property as appropriate. Property records shall be maintained by the Government for all GFP provided to the contractor.

4.17 Government-Furnished Information

All system documentation will be provided to the contractor at the kick-off meeting. All system documentation shall be returned to the COR in accordance with the end of the contract. Information provided on the government furnished encrypted IronKey is considered GFI and shall be returned to the government, with the return of the IronKey.

4.18 Invoicing

The Contractor shall submit invoices via email to InvoiceSAT.consolidation@ice.dhs.gov. Additional invoicing guidance may be provided by the COR after award.

4.19 Reserved

4.20 Business Continuity Plan

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government within 30 business days after the date of award and will be updated on an annual basis. The BCP shall document contractor plans and procedures to maintain support during an emergency, including natural disasters, government shutdowns and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the contractor's emergency management procedures and policy;
- A description of how the contractor will account for their employees during an emergency or government shutdown;
- How the contractor will communicate with the Government during emergencies; and
- A list of primary and alternate contractor points of contact, each with primary and alternate:

- Telephone numbers; and
- E-mail addresses.

Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 24 hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life-threatening emergency, the COR/alternate COR shall immediately make contact with the contractor Project Manager to ascertain the status of any contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the contractor Project Manager and the COR/alternate COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and contractor);
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.);
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.); and
- Essential contractor work products expected to be continued, by priority.

The Government and contractor Project Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

Observance of Legal Holidays and Excused Absence

(a) The Government hereby provides notification that Government personnel observe the listed days as holidays:

- New Year's Day
- Martin Luther King's Birthday
- President’s Day
- Memorial Day
- Juneteenth National Independence Day
- Independence Day
- Labor Day
- Columbus Day
- Veterans' Day
- Thanksgiving Day
- Christmas Day

(b) In addition to the days designated as holidays, the Government observes the following days:

- Any other day designated by Federal Statute
- Any other day designated by Executive Order
- Any other day designated by the President's Proclamation

(c) It is understood and agreed between the Government and the contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation except as set forth within the contract. In the event the contractor's personnel work during the holiday, they may be reimbursed by the contractor; however, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

(d) When the Federal and governmental entities grant excused absence to its employees, the Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the CO or the COR/alternate COR.

(e) If Government personnel are furloughed, the contractor shall contact the CO, COR, and alternate COR to receive direction. It is the Government's decision as to whether the contract price/cost will be affected. Generally, the following situations apply:

(1) Contractor personnel that are able to continue contract performance (either on-site or at a site other than their normal workstation), shall continue to work and the contract price shall not be reduced or increased; and
(2) Contractor personnel that are not able to continue contract performance (e.g., support functions), may be asked to cease their work effort.

(f) In those situations that furloughed Government personnel are reimbursed, the contractor may not invoice for their employees working during the Government furlough, until such time as the special legislation affecting Government personnel is signed into law by the President of the United States.

(g) Nothing in this clause abrogates the rights and responsibilities of the parties relating to stop work provisions as cited in other sections of this contract.

4.21 Progress Reports

The Project Manager shall provide a monthly progress report to the Contracting Officer, COR and alternate COR via electronic mail by the 10th day of the month for the previous performance month and one hard copy to the COR. 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, risks, and anything requiring immediate COR/alternate COR attention. In addition to above, the MPR shall include:

- The number of open, in progress, and closed IT tickets (including those submitted to HQ) from users during the reporting period and cumulatively;
- Track and report the uptime and/or utilization rate of relevant DHS-resources such as Wifi, SAN, etc.;
- Contractor concerns and risks shall be a sperate section; and
- Contractor recommendations shall be a separate section.

4.22 Required Meetings

a) POST AWARD CONFERENCE (Kick Off Meeting) - The Contractor shall attend a post-award conference with the CO and the COR/alternate COR no later than 7 business days after the date of the award. The purpose of the post award conference, which will be chaired by the CO, is to address and discuss contract requirements, performance and objectives, discuss transition execution and review staffing/onboarding plans. The post-award conference will be held at the TSL facility, located in the William J. Hughes Technical Center in Atlantic City, New Jersey. The government will provide an agenda and the contractor shall summarize the post award conference in meeting minutes, due within three (3) business days after the post award conference agenda and the contractor shall summarize the post award conference in meeting minutes, due within 3 business days after the post award conference.

b) UPDATE MEETING – The Contractor and COR/alternate COR will have a monthly meeting to discuss deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. An agenda should be provided 1 business day prior to the meeting. Meeting minutes are not required unless otherwise requested by the COR/alternate COR. If necessary and due to developing circumstances, meetings will be held upon request. These meetings will be held at the TSL and can be accessed via teleconference.

c) CLOSE-OUT MEETING - The Contractor shall set up and facilitate a final meeting which will be required prior to the end of the contract to resolve open items and to ensure efficient close-out.

4.23 Project Plan

The Contractor shall deliver a task order project plan within 14 business days after task order award. The project plan and schedule serve as a guide to task execution and control, and shall document technical approach, resources, schedule baselines, anticipated travel; risks and risk mitigation; deliverables schedule; and other associated costs.

4.24 Task Order Transition

The task order transition is the coordinated transfer of all services and equipment from the relevant incumbent contractor(s) to the successor Contractor. It includes the Contractor's performance of all efforts, in alignment with the Government-approved Transition Management Plan (TMP), that are necessary to ensure that its subcontractors and its teaming partners are

ready to successfully assume full performance of the task order upon expiration of the transition period. It is critical that the Contractor provide the Government with a realistic transition plan which addresses all factors and risks, and includes contingency plans for missed milestones or other impacts to the schedule.

4.24.1. Phase-In Task Order Transition Period

The Contractor shall support and cooperate with TSL and its designated agents. During the task order transition period, the Contractor shall coordinate and support daily status meetings with TSL to ensure transition is on track for timely completion. TSL expects the low-risk, phased-in, smooth and seamless transition to occur during non-peak hours with no disruption to its operations or those of other contractors supporting TSL. The COR shall coordinate transition efforts among current service providers and the Contractor. TSL shall provide the Contractor with the information and data to effect transition to the performance expectations under the task order.

Task order transition shall be deemed successfully completed when the Contractor has demonstrated that it is prepared to assume full day-to-day performance of the task order. The Contractor shall successfully complete transition within 30 days after award. DHS will provide space for the Contractor's transition team at TSL to conduct required business, including conducting interviews and hiring actions. These activities may occur during normal business hours provided they are scheduled ahead of time to minimize interruptions to day-to-day work requirements.

The Contractor shall provide the Transition Management Plan with their proposal to the Government; addressing the task order transition methodology, processes, staffing, key milestones and schedule to assure a complete, effective and efficient transition of task order requirements from the incumbent within the 30-day period. The Contractor shall provide a final transition checklist to the COR indicating that it has successfully completed all transition activities and it is ready to assume full performance of the task order.

4.24.2 Phase-Out Task Order Transition Period

The Contractor shall cooperate fully and openly with any successor contractor assuming responsibility for TSL support services. Within 30 days of the Government's request, the Contractor shall develop a Phase-Out Task Order Transition Plan consisting at minimum, of the following:

- Actions, schedules and roles and responsibilities to assist in transitioning to a new contractor or entity;
- Lists of items to transition (e.g. Government-Furnished Equipment inventories, user IDs, passwords, training documentation, warranties, Government records, etc.);
- Transfer of all Government records;
- Update and transfer of any and all existing procedures;

- Conducting thorough turnovers (procedures, etc.) with other organizations or personnel;
- Transfer or closure of subcontracts;
- Government requested training in procedures (e.g., SOPs) to successor contractor;
- Introductions to subcontractors and mutual aid partners; and
- Removal of Contractor-owned property.

The Contractor shall submit a sufficient plan that includes an effective and efficient 30-day task order transition period and shall be subject to Government approval.

4.25 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 (Current Windows OS and Microsoft Office Applications) and in accordance with the Section 10.0, Performance Requirements Summary (PRS).

4.26 Limitation on Contractor Data Rights

The Contractor shall not use, release to others, reproduce, distribute, or publish the data deliverables or any data first produced in the performance of this contract without first receiving approval from the CO.

4.27 Materials

The Contractor shall be required to purchase materials in support of this work effort. Before purchasing any individual item equal to or exceeding $500 that is required to support tasks performed pursuant to this SOW, the Contractor shall obtain written consent from the COR/alternate COR. The CO may lower or raise the aforementioned $500 threshold at his/her discretion and on written notice to vendor. All purchases made under the contract shall become the property of DHS. Contractor purchased materials required to support this requirement shall include:

- RAM/Internal Memory;
- Software;
- Computer components;
- Toner Cartridges and other small IT related equipment for approximately 20 network (SciTech, LabNet, LANA) and small local (on desk) user printers. This figure can vary slightly;
- External/Network Memory (e.g., iron keys, flash drives, passport drives, NAS drives)
- Laptop/Desktop Peripherals (e.g., docking stations, keyboards, mice, webcams, monitors, etc.); and
- Networking Hardware (e.g., KVM switches, cables and various other network interface & products).

4.28 Government Acceptance Period

The COR/alternate 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/alternate COR will send an e-mail to the contractor notifying it that the deliverable has been accepted.

The COR/alternate 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.

The COR/alternate COR will have 10 business days to review deliverables and make comments. Upon receipt of the Government comments, the contractor shall have 10 business days to incorporate the Government's comments and to resubmit the deliverable in its final form.

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.

5.0 DELIVERABLES

The Contractor shall deliver the following items in accordance with the SOW requirements. All electronic deliverables also shall be submitted to TSLdeliverables@st.dhs.gov in addition to the distribution listed below.

TABLE 3

Item	SOW Reference	Deliverable / Event	Due by	Distribution
1		Post Award Conference	7 Business Days after Post Award Conference	COR/alt COR, Contracting Officer
2		Project Deliverables Tracking System	Ongoing	COR/alt COR, Contracting Officer
3		Project Plans for major tasks or groups of tasks	As directed by COR/alt COR	COR/alt COR, Contracting Officer
4		Agendas for meetings	2 Business Days prior to scheduled meeting	COR/alt COR

5		Official Meeting Minutes	1 Business Day after meeting	COR/alt COR
6		Master Schedule of All Projects to include Resource Allocation	30 Days after award	COR/alt COR, Contracting Officer
7		Master Risk Register of All Projects	30 Days after award	COR/alt COR, Contracting Officer
8		Ad-hoc reporting as specified by COR/alt COR	As directed by the COR/alt COR	COR/alt COR
9		Conduct brown-bag, training, and/or informational meetings	As directed by the COR/alt COR	COR/alt COR
10		Telework Activity Report	Mondays for the previous week	COR/alt COR
11		Assist with the Drafting of Acquisition Support Documents for IT Related Acquisitions (i.e. SOW, Market Research)	As directed by the COR/alt COR	COR/alt COR
12		Helpdesk Ticketing Status Report	Due by the 10th of the Month for the previous Month	COR/alt COR
13		Business Continuity Plan	30 Business Days after Date of Award	COR/alt COR, Contracting Officer
14		Monthly Progress Reports including Project Expenditure Rates	Due monthly by the 10th of the Month	COR/alt COR, Contracting Officer
15		Security Incident Reporting	Upon Occurrence	COR/alt COR, Contracting Officer
16		Backup and recovery plan draft	90 days after contract award	COR/alt COR
17		Version Control	90 days after contract award	COR/alt COR
18		Back-up and Disaster recovery plans.	90 days after contract award	COR/alt COR

6.0 POINTS OF CONTACT

DHS S&T may change the individual designated as a Point of Contact (POC) upon notice to the Contractor of such change. Notice may be via contract mod and/or e-mail.

6.1 Government Points of Contact

DHS S&T Contracting Officer
Contracting Officer
U.S. Department of Homeland Security
Office of Procurement Operations
Science and Technology Acquisitions Division
Branch 2
E-mail: TBD
Telephone: TBD

DHS S&T Contracting Officer's Representative (COR)
TBD
U.S. Department of Homeland Security
Directorate of Science and Technology
E-mail: TBD
Telephone: TBD

DHS S&T Alternate Contracting Officer's Representative (COR)
TBD
U.S. Department of Homeland Security
Directorate of Science and Technology
E-mail: TBD
Telephone: TBD

6.2 Contractor Points of Contact

TBD

ATTACHMENT III – Labor Category Descriptions

Labor Category	Description	Certification/Experience (Years of experience, degree, skills, abilities, etc.)	Equivalent Proposed GSA Schedule LCAT
Project Manager Level II	Perform planning and scheduling, progress reporting, cost control analysis, organization and manpower planning, develop work breakdown structures, assess performance analysis, conduct technical risk analysis, financial planning, quality assurance, and quality control on all submitted deliverables; support the full scope of the contract to ensure that all contract staff adhere to the SOW; focuses on project execution and overall contract goals and keeps the customer informed of ongoing administrative concerns and risks.	10 years of program management experience in planning, managing, and implementing programs/projects AND shall have project management professional (PMP) certification from the Project Management Institute (PMI). OR a master's degree in either a business or technical from an accredited college or university and 5 years of program management experience in planning, managing and implementing projects AND shall have project management professional certification from the Project Management Institute (PMI). Shall possess demonstrated excellent communication skills, both oral and written.	54151S: Technical Project Manager
Cloud SME Level III-4	Understands Windows Operating Systems (Server 2008R2, Server 2012R2, and Server 2016). Understands and can deploy and configure	Microsoft Certified Systems Administrator or Microsoft Certified Solutions Expert or Specialized Certification in VMWare and MCSA; and 15 years related experience.	54151S: Senior II Scientist/Engineer/Systems Analyst

	RedHat based Linux servers and appliances. Understands networking, subnetting, VLAN segmentation, and related routing and switching principles. Understands the Microsoft Windows Server environment including Active Directory Domain Services, DHCP, and DNS. Advises, designs and oversees the administration of server environment. Administers Windows domain infrastructure, virtualization utilizing VMWare and Hyper-V. Advises, develops, enhances and mentors the management of Two-Way Trust Active Directory, Group Policies. Distributed File Shares, Exchange/Office365, SQL Servers, clustered servers, SAN management, and administration. Designs and controls Virtual Machine templates that can be used to rapidly deploy virtual machines on both VMware and Hyper-V.	Experience keeping IT equipment and IT services running including troubleshooting and fixing IT enterprise issues such as Microsoft operating systems, active directory, Server, and hardware issues such as workstations, servers, and appliances; can support a Microsoft enterprise environment involving the understanding of software such as Active Directory, DHCP, DNS, and file and print servers. Experience with the installation, configuration and maintenance of VMware vSphere technologies: vCenter, ESX/ESXi, Horizon View. Has experience supporting Microsoft Hyper- V virtual environment including installation, configuring, troubleshooting break/fix and performing upgrades.	

Systems Engineer Level III-2	Troubleshoots and resolves configuration and application issues on Microsoft Windows client systems (Windows 10 and above) in Enterprise and stand-alone environments; applies patches and scans stand-alone workstations. Enforces configuration and security standards. Analyzes and modifies Active Directory Group Policy Objects and User and Computer Objects. Supports mobile solutions, such as, but not limited to Microsoft Exchange (Active Sync), Office 365, Mobile Device Management (MDM) such as AirWatch, JAMF Casper, with alternative token technology (ie-Derived Credentials) Supports messaging chat systems such as Skype for Business and Microsoft Teams. Collaboration software such as SharePoint, application-based firewall and proxy server(s), and operating systems. Deploys and hardens Windows Server 2012 R2 & 2016 Standard and Data Center,	Microsoft Certified IT Professional (MCITP), Microsoft Certified Solutions Expert (MCSE) or Microsoft Certified Solutions Associate (MCSA) certifications; and VMware Certified Professional (VCP) or CompTIA Security+ certifications; and 15 years or more performing Systems Engineering work. Experience with secure mobile solutions, such as, but not limited to: Microsoft Exchange (Active Sync), Office 365, Mobile Device Management (MDM) such as AirWatch with derived credentials, JAMF Casper; messaging systems such as Skype for Business, collaboration software such as SharePoint, application- based firewall and proxy server(s), and operating system; managing a Virtual Private Network (VPN) solution such as Cisco AnyConnect; managing Virtualization solutions such as VMware 6.0+ & Microsoft Hyper-V; deploying & hardening Windows Server 2012 R2 & 2016 Standard and Data Center, Apple OSX, IOS	54151S: Senior II Scientist/Engineer/Systems Analyst

	including Apple OSX, IOS platforms(s). Implement, administer, and deploy leading security tools including but not limited to: McAfee Enterprise Security Information and Event Management (SIEM), McAfee Endpoint Security, Symantec Endpoint Protection, McAfee ePolicy Orchestrator (ePO), McAfee Data Loss Prevention (DLP), McAfee Host Intrusion Prevention (HIP), Carbon Black (Cb), NESSUS Security Center, Privilege Access Management (PAM).	platforms(s); cloud service implementations with a focus on AWS and Azure; and implementing cloud automation such as Azure workflow and/or AWS application deployment. Experience deploying and using leading security tools, and experience deploying and hardening RedHat Linux 6.0+, implementing and managing RedHat, Satellite, Veritas NetBackup, Dell Compellent SAN and/or DAS.	
Systems Engineer Level III-4	Manages and responsible for software/patch management tools such as System Center Configuration Manager (SCCM), design and implementations of Microsoft SCCM at the enterprise level. Maintains and supports day to day operations and configuring/troubleshooting all aspects of SCCM effectively, including patch management, software distribution, Operating System Deployment, reporting, and logging.	Microsoft Certified Systems Administrator, Microsoft Certified Solutions Expert, and/or Microsoft Certified Professional in System Center Configuration Manager (SCCM) certification; and MCSA certification; and 15+ years of experience.	54151S: Senior II Scientist/Engineer/Systems Analyst

	Supports in Microsoft service management and monitoring tools such as SCOM and SCSM. Works in Microsoft client/server platforms, networking impacts on SCCM architecture, scripting (PowerShell), creating and deploying operating system images for Windows servers and workstation customized to organizational/operational and security requirements. Performs SQL/Database administration support including performing software and patch update on Microsoft SQL clustered servers. Performs and maintains SQL/Database scripting, database management including database normalization, and supporting SQL and Database administration functions such as MS SQL and scripts such as PoWerScript used to create custom reports. Responsible for installing, deploying, and managing Microsoft enterprise services software such as Active Directory, Dynamic Host		

	Configuration Protocol (DCHP), Domain Name System (DNS), and file and print servers. Keeps IT equipment and IT services running including troubleshooting and fixing IT enterprise issues such as Microsoft operating system, active directory, Server, and hardware issues such as workstations, servers, and appliances.		
O&M Systems Engineer Level II-4	Performs the installation, configuration, and maintenance of Microsoft Windows servers, running Microsoft Windows Server 2008/2012/2016 and Windows 10. Maintains IT equipment and services running, including, troubleshooting and fixing IT enterprise issues such as Microsoft operating system, active directory, Server, and hardware issues such as workstations, servers, and appliances.	Microsoft Certified Systems Administrator or Microsoft Certified Solutions Expert certification; and 10-15 years related experience.	54151S: Senior II Scientist/Engineer/Systems Analyst

	Supports and manages Microsoft enterprise environment and understanding of software such as Active Directory, DHCP, DNS, and file and print servers. Responsible with server performance tuning and monitoring tools, IP networking as it relates to local area networks, and working with Network Engineers to troubleshoot advanced server network issues. Provides the installation, configuration and maintenance of VMware vSphere technologies: vCenter, ESX/ESXi, Horizon View. Understands Microsoft Hyper-V virtual environment including installation, configuring, troubleshooting break/fix issues and performing upgrades.		

Applications Developer Level III-5	Designs, develops, enhances, debugs, and implements software. Troubleshoots production problems related to software applications. Researches, tests, builds, and coordinates the conversion and/or integration of new products based on client requirements. Designs and develops new software products or major enhancements to existing software. Evaluates effectiveness. Addresses problems of systems integration, compatibility, and multiple platforms. Consults with project teams and end users to identify application requirements. Performs feasibility analysis on potential future projects to management. Assists in the evaluation and recommendation of application software packages, application integration and testing tools. Troubleshooting, remediating	8+ years of experience using SharePoint 2013 or newer versions and SharePoint Designer, HTML and Javascript 8+ years of experience with relational database (i.e. SQL Server) 2+ years of experience using Nintex Workflows. 8+ years of experience consulting clients on potential SharePoint Solutions, client presentations, translating business requirements into technical requirements. 8+ years of experience with System testing and User Acceptance Testing. Certification: Microsoft Certified System Engineer (SharePoint 2013 or newer) preferred.	54151S: Senior I Scientist/Engineer/Systems Analyst

	and optimizing any and all SharePoint based issues, while also working with engineering requirements and providing strategic recommendations to management. Resolves problems with software and responds to suggestions for improvements and enhancements. Acts as team leader on projects. Instructs, assigns, directs, and checks the work of others on the development team. Participates in development of software user manuals and technical reports.		
Applications Developer Level II-5	Designs, develops, enhances, debugs, and implements SharePoint software. Troubleshoots production problems related to SharePoint applications. Researches, tests, builds, and coordinates the conversion and/or integration of new SharePoint products based on client requirements. Participates	5+ years of experience with SharePoint administration and development. 5+ years of experience with appropriate programming languages, operating systems, hardware and software. 5+ years of experience working with the interface of information technology and functional groups within an organization.	54151S: Intermediate II Scientist/Engineer/Systems Analyst

	in development of software user manuals and technical reports. Provides phone and in-person support to users in areas which include SharePoint applications and COTS and GOTS applications. Troubleshooting, remediating and optimizing any and all SharePoint based issues, while also working with engineering requirements and providing strategic recommendations to management. Act as point of contact for all business-related SharePoint feature and support issues. Diagnose and resolve application, configuration and code level technical issues. Contribute significantly to any design and refactoring discussions, demonstrate strong communication skills, and be able to articulate problems and solutions in a concise manner.	1+ year of experience providing help desk support for IT customer support issues including SharePoint.	

Systems/Data Architect Level III-5	Evaluates architectural options and defines overall architecture of the system. Designs, develops, implements and maintains complex custom SharePoint applications. Provides subject matter expertise and technical consulting support on internal applications and interfaces. Leads SharePoint Migration activities and Mobile support and integration with other O365 applications (OneDrive, Teams, etc.). Drives engagement with IT Security and Infrastructure teams to ensure secure development and deployment of solutions. Incorporates DevOps and Agile methodologies in implementing business solutions, mapping business strategies to Application Architecture and Delivery. Evaluates new and existing software products. Prepares cost-benefit and return-on-investment analyses to help management decide whether implementing the proposed system will be financially feasible. Provides solutions, mentors and guides project teams in development of	5+ years of experience w/ Enterprise Software architecture. 5+ years of experience SharePoint 2013/2016 Administration and design. Significant experience with O365 strategies/roadmaps. 5+ years of experience with Relational Database and operating systems. 5+ years of experience with Microsoft Active Directory Administration. 5+ years of experience with writing, modifying and running Powershell Scripts 5+ years of experience consulting clients on potential SharePoint Solutions, client presentations, translating business requirements into technical requirements.	54151S: Senior I Scientist/Engineer/Systems Analyst

	modern business methods/utilities, identification of best practices, and creating and assessing performance measurements. Clearly communicates complex technical solutions with Stakeholders.		