Title III and Linguists Unit (T3LU)
Communications Assistance for Law Enforcement Act (CALEA)
Network and Intercept Operation Support Services

Statement of Work (SOW)

Washington, DC

June 24, 2025

Contents

1.0 PROJECT TITLE

Statement of Work (SOW) for the Title III and Linguists Unit (T3LU) Communications Assistance for Law Enforcement Act (CALEA) Network and Intercept Operation Support Services.

2.0 BACKGROUND

The U.S. Immigration and Customs Enforcement (ICE), the largest investigative arm in the U.S. Department of Homeland Security (DHS), is responsible for identifying and shutting down vulnerabilities in the nation's border, economic, transportation, and infrastructure security.

The Homeland Security Investigation's (HSI), Cyber and Operational Technology (COT), Technical Operations Center (TOC), Title III and Linguists Unit is responsible for providing field-wide deployment and maintenance of telecommunications intercept collection systems in support of criminal investigations.

HSI utilizes the CALEA network to receive, process, buffer and transmit court authorized intercepted communications. The CALEA network is not part of the corporate infrastructure and is not supported by the Office of the Chief Information Officer (OCIO) corporate support solution. This network contains numerous law enforcement systems that have the sole purpose of conducting the lawful interception and collection of evidentiary information for criminal proceeding.

The Communication Intercepts Support Team (CIST) offers engineering and technical support for Title III equipment and the Communications Assistance for Law Enforcement Act (CALEA) network. CIST is tasked with overseeing and coordinating the placement of Government and Contractor system administrators, as well as Information Technology professionals, at designated regional collection facilities. Their role is to support the Title III systems deployed by the COT-TOC. These Title III systems are responsible for processing and displaying lawfully collected data from the regional CIST.
.

3.0 SCOPE OF WORK

The scope of this effort is to the T3LU CALEA Network and Intercept Operation Support Services. Specific services are:

- CALEA Network Support
- System Administration
- System Engineering Support
- Virtual Environment Support
- Active Directory Organizational Unit Administration Support
- Storage Administration Support
- CALEA Architecture Support
- Continuity of Operations (COOP) Site Support

- Field Operations Support
- Technical Service Support
- Inventory Support
- Data Analyst Support (Optional)

4.0 APPLICABLE POLICIES AND STANDARDS

The Contractor shall comply with the latest version of all technology standards and architecture policies, processes, and procedures applicable to the ICE Information Technology environment. These publications are available on request and include, but are not limited to, the following:

- DHS 4300A Sensitive Systems Handbook;
- DHS 4300A Sensitive Systems Policy Directive;
- DHS 4300B National Security Systems Handbook;
- DHS Management Directive (MD) 4300, IT Systems Security Publication;
- DHS MD 4010.2 (DRAFT), Section 508 Program Management Office &Electronic And Information Technology Accessibility;
- DHS Systems Engineering Life Cycle Guidebook;
- ICE Technical Reference Model;
- ICE Application Security Cyber Security Standard (CSS);
- ICE Architecture Test and Evaluation Plan;
- ICE Cybersecurity Standards;
- ICE Enterprise Systems Assurance Plan;
- ICE System Lifecycle Management (SLM) Handbook;
- ICE Web Standards and Guidelines;
- National Institute of Standards and Technology (NIST) Computer Security Resources Center (CSRC) standards, guidelines, and special publications;
- Privacy Act of 1974;
- Section 508 1194.2, Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220);

Further, the Contractor shall comply with the following DHS Enterprise Architecture (EA) requirements:

- All IT hardware or software shall be complaint with the DHS EA and ICE Technical Reference Model (TRM) Standards and Products Profile.
- All encryption shall be Federal Information Processing Standard (FIPS) 197 Advanced Encryption Standard (AES) that has been FIPS 140-2 certified;
- All data assets, information exchanges, and data standards, whether adopted or developed,

shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model;
- In compliance with Office of Management and Budget (OMB) mandate, all network hardware shall be Internet Protocol version 6 (IPv6) compatible without modification, upgrade, or replacement; and
- The Contractor shall not deviate from the SLM process without express approval granted by the Contracting Officer's Representative (COR).

4.1 DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture (EA) policies, standards, and procedures. Specifically, the Contractor shall comply with the following DHS EA requirements:

- All developed solutions and requirements shall be compliant with the DHS EA.
- 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 Enterprise Data Management Policy Directive 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. Government 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.

4.2 System Architecture Standards

4.2.1 ICE Application Architecture Compliance

The Contractor shall ensure that the application is designed and developed for browser independence; i.e., the application will generally work with any of the major browsers. ICE currently uses Chrome for Work, secured with centrally managed security policies. Browser specific implementations or limitations on browser independence must be approved in writing by ICE OCIO prior to development. Web Applications should be designed utilizing a responsive web design (RWD) approach, to provide an optimal viewing and interaction experience, independent of the particular platform capabilities the end user is utilizing. If ICE OCIO upgrades to a newer version of IE or Chrome for Work, the Contractor shall ensure the application is compatible with the future version.

4.2.2 Open Source Compliance

The Contractor shall follow the ICE Open Source Manifesto when evaluating any technologies, tools, software, and/or application programmable interfaces (API's) to support a system. The Contractor shall prioritize the adoption of, and migration to, Open Source technologies over proprietary or "closed" technologies.

5.0 TASKS

The objective of the T3LU CALEA Network and Intercept Operation Support Services is to acquire a qualified Contractor to provide the full range of technical services required for the Title III systems and CALEA network in support of the intelligence and investigative priorities of HSI's mission.

The Contractor shall provide qualified, experienced personnel to perform the service and support tasks listed in this SOW. The Contractor shall also proficiently manage well-qualified IT professionals who are geographically located throughout spread across the Continental United States (CONUS), plus U.S. territories.

5.1 CALEA NETWORK SUPPORT

The Contractor shall provide the necessary personnel and technical resources to provide full-time support and emergency after-hours support to a variety of operational technology systems at the Lorton, VA ICE office or other designated ICE Field Offices. The Contractor shall support the design, implementation, testing, operation, maintenance and administration of the CALEA Local Area Network (LAN) and Wide Area Network (WAN) infrastructure. The Contractor shall provide support with the installation of the LAN / WAN and related equipment. The Contractor shall be responsible for CALEA network. This includes:

a. Maintain the network, including the LAN/WAN links and connectivity, switches, routers, firewalls, servers (Microsoft Windows and Unix Operating System), Storage Area Network (SAN), media backup systems, fiber and Ethernet cabling, and other infrastructure components;
b. Provide network security, assuring the LAN shall only be available to personnel authorized by the Government; not permitting any non-Government authorized network LAN and WAN access;
c. Support the Government in the design of future network architecture to include, routers, switches, firewalls, Virtual Private Networks (VPNs), Servers, SAN, Virtualization Machine Ware (VMware) Environment, cable management systems and other network enhancements;
d. Analyze the network architecture utilizing metrics available from network management tools to identify modifications required to maintain optimum efficiency;
e. Support network design, development, test, implementation, and performance of maintenance and administration of the LAN/WAN and all associated support infrastructure components;
f. Perform steps to ensure maximum systems availability (minimize collection systems and end-users' downtime);

g. Implement and maintain software and application configuration management and configuration reporting;
h. Install and update anti-virus software and anti-virus signature files on all network assets;
i. Install security patches to protect against Information Assurance vulnerabilities;
j. Operate and maintain SAN, application servers, archiving systems and computer clusters;
k. Install Government Public Key Infrastructure (PKI) server side certificates and implement Secure Sockets Layer (SSL) and other secure methods of data transmission including support to the VPN and VPN servers; and Structured Query Language (SQL) servers;
l. Support the Government certification and accreditation process, including applying approved security and vulnerability patches to all managed systems;
m. Support use of the DHS Personal Identity Verification (PIV) cards and PKI to support user authentication into the network, into applications, and for signing and encrypting electronic mail;
n. Test and deploy client software packages utilizing automated delivery and installation tools;
o. Responsible for any new peripheral or computer systems attached to the systems network;
p. Ensure uninterruptible power supplies are operational and the batteries hold charges;
q. Implement other best business practices for keeping the network infrastructure secure, efficient and responsive with the approval of the CIST Program Manager(s);
r. Support design and implementation of the LAN, infrastructure to include fiber and Ethernet cabling and other infrastructure components.
s. Support design of future network requirements to include network switches, servers, Storage Area Nodes, cable management systems and other network enhancements. Support migration of services and servers to enterprise platforms; and
t. Perform inventory, logistical, and clerical support for shipments and deliveries of operational equipment.

5.1.1 SYSTEM ADMINISTRATION AND SYSTEMS ENGINEERING SUPPORT

The Contractor shall provide systems analysis, evaluation, design, integration, documentation, and implementation applications**.** This includes:

a. Participate in phases of technical solution development to include analysis, evaluation, integration, testing and acceptance phases;
b. Support the Government in applying higher-level business or technical principles and methods to very difficult technical problems to arrive at automated engineering solutions;
c. Provide technical expertise in formulating system design and development;

d. Coordinate with CIST Program Managers at all levels to obtain information related to interface with systems at those levels to facilitate the acquisition and exchange of networked information;
e. Participate in technical working groups to arrive at solutions to IT problems encountered and to provide knowledge and information concerning state-of-the-art techniques and right-practices regarding complex software and hardware implementations;
f. Develop recommendations concerning major project ramifications and to offset adverse impacts;
g. Provide support with the replication to the Continuity of Operations location;
h. Support the Government in testing network engineering, directory services, network management, and Information Assurance technology integration, testing, training, and development of capabilities prior to fielding on the operational networks;
i. Maintain Windows Active Directory, Domain Name Server (DNS), Windows Server Update Services (WSUS), Transmission Control Protocol/Internet Protocol (TCP\IP), and switch and router configuration; and
j. Operate and maintain standard Internet TCP/IP, SSL and encryption.

5.1.2 VIRTUAL ENVIRONMENT SUPPORT

The Contractor shall provide systems administration, with a primary focus of server virtualization. This includes:

a. Utilize VMware (ESX 6.0+ VMware) in load/capacity analysis, trend monitoring, resource utilization, systems analysis, automated systems design, system development cycles and concepts, and information processing standards and methods to identify operational/processing problems, evaluate alternative approaches, adapt precedents and procedures, and plan and implement or recommend resolution;
b. Plan and coordinate the installation, testing, operation, troubleshooting, and maintenance of hardware, operating systems, and applications software;
c. Adapt and implement systems diagnostic and maintenance tools to ensure the availability and functionality of server information systems;
d. Administer the virtual environment administration for non-production lab environment;
e. Ensure security patches are installed in accordance with configuration management policies for all supported servers;
f. Maintain documentation for all aspects of the virtual environment;
g. Recommend improvements, evaluate alternate configurations, and develop concepts for modifications and future systems based on the capabilities and limitations of data processing equipment. This includes systems design methods.
h. Familiarity with federal, network management and IA approaches and

requirements;

i. Provide server virtualization services that support the organizational needs of the customer base through application of concepts, methods and practices for systems design, development, installation, operations; architecture, topology, protocol and remote access technology; and configuration management.
j. Plan, design, develop, and integrate networked systems architectures
k. Manage file access control permissions and coordinate file access with customer base. Assist the Government with defining the long-term requirements of the systems operation and administration;
l. Ensure the integrity of centrally managed servers and data. To include identifying areas requiring additional effort; execute action to remediate areas requiring additional effort; monitor and troubleshoot all versions of servers for availability; recover data in the event of hardware or software failure; and ensure customers receive current versions of supported software as they become available;
m. Troubleshoot, analyze and resolve anomalies in the virtual environment;
n. Maintain high level of reliability and availability of the CALEA directory services, and infrastructure;
o. Provide server administration, upgrades, patches and customer support to extend e-mail services; and
p. Ensure security patches are installed in accordance with configuration management policies for all servers assigned.

5.1.3 ACTIVE DIRECTORY ORGANIZATIONAL UNIT ADMINISTRATION SUPPORT

The Contractor shall be responsible for the following:

a. Plan and coordinate Organizational Unit administration, Group Policy Object (GPO) administration, and the installation, testing, operation, troubleshooting and maintenance of hardware, operating systems, and applications software;
b. Recommendation for improvements, evaluating alternate configurations, and concepts for modifications and future systems;
c. Maintain the Lightweight Directory Active Protocol (LDAP), Active Directory (AD), DNS, TCP\IP, and server configuration; standard Internet protocols (TCP/IP); and SSL and encryption.
d. Create user and compute accounts in AD;
e. Add user accounts to appropriate AD security groups;
f. Join computers to the domain and remove them as needed; and
g. Coordinate with COT-TOC security to move accounts between Organizational Units when needed.

5.1.4 STORAGE ADMINISTRATION SUPPORT

The Contractor shall provide storage administration;

h. Plan and coordinate the installation, testing, operation, troubleshooting and maintenance of hardware, operating systems, and applications software;
i. Maintain reliability and availability of CALEA storage services and infrastructure;
j. Troubleshoot, analyze and resolve anomalies; identify, and correct server security vulnerabilities; schedule downtime to minimize user impact;
k. Ensure security patches are installed in accordance with configuration management policies for all servers;
l. Maintain documentation for all servers and applications in SOP Repository;
m. Maintain storage management fundamentals, and a multitude of enterprise class SAN architectures; and
n. Maintain Common Internet File System (CIFS), Network File System (NFS), Network Technology File System (NTFS), Active Directory domain account permissions, TCP\IP, and server configuration.

5.1.5 CALEA ARCHITECTURE SUPPORT

The Contractor shall maintain technical documentation to the Standard Operating Procedures (SOPs) Repository located on the CALEA network for the CALEA infrastructure to include technical drawings of the cable plant, wiring diagrams for patch panels, detailed network diagrams, and other required documentation to ensure network knowledge transfer. The Contractor shall maintain documentation necessary to obtain and install certificates as required by the Government leads.

5.1.6 CONTINUITY OF OPERATIONS SITE SUPPORT

The Contractor shall support the backup systems and off-site storage as part of the Continuity of Operations Plan. The Contractor shall work with the Government to evaluate and improve current capabilities on an on-going basis. The Contractor shall provide technical support for any failure of the backup systems, critical components, and mission critical user support. The Contractor shall provide after-hours support on an on-call basis.

5.2 FIELD OPERATIONS SUPPORT

The Contractor shall provide the necessary personnel and technical resources to provide full-time support to a variety of operational technology systems at designated ICE Field Offices and other HSI facilities. The Contractor shall perform system installation, set-up, administration, maintenance, troubleshooting, and user support to customer supplied electronic surveillance collection systems to support the investigative (Title III and Pen Register) priorities of Criminal Investigations. This includes logging, tracking, and monitoring of the health of the CMP, the collection systems installed therein, local and remote workstations, and

their LAN and WAN. In addition, the Contractor shall integrate and support associated feeder collection systems, as needed, to required external systems, services, and inputs to collect unprocessed evidence and intelligence data that will be used for further analysis in support of lawful investigations. This includes:

a) Provide day-to-day system and database administration of all aspects of the collection systems to include creating accounts in AD and the applications, changing passwords, unlocking user accounts, resetting user accounts, and setting user preferences;
b) Adding user accounts to appropriate AD security groups;
c) Join computers to the domain and remove them as needed;
d) Coordinate with COT-TOC security to move account between OU when needed;
e) Check logs for indication of application and hardware problems;
f) Replace failed hard drives;
g) Assist users with tasks such as connecting to printers;
h) Install and update application software when automated processes fail;
i) Use remote assistance to view a user's screen to assist with applications issues;
j) Update hostname and IP addresses setting as needed to facilitate workstations moves;
k) Assist COT-TOC personnel with installations, moves, and changes to equipment;
l) Troubleshoot coppers/fiber cabling between the devices and re-terminate cables as needed;
m) Maintain specific HSI collection systems. Perform periodic maintenance, monitor for problems, and resolve system and user issues;
n) Assist users with establishing authorized access to appropriate cases and lines;
o) Implement new and renewal intercepts and when court orders arrive;
p) Document all new intercepts in the CMP recordkeeping systems, and implement only lawfully authorized techniques;
q) Maintain and update SOPs, with Government supervision, guidance, and approvals;
r) Provide user support and training on specified COT-TOC-supplied systems;
s) Support systems within a regional model where regions often span multiple states;
t) Perform steps to ensure maximum systems availability (minimize collection systems and end-users' downtime);
u) Provide liaison with telecommunications service providers to engineer, implement, and troubleshoot telephony input lines;
v) Responsible for any new peripheral or computer systems attached to the systems network; and
w) Perform inventory, logistical, and clerical support for shipments and deliveries of operational equipment.

5.3 TECHNICAL SERVICE SUPPORT

The Contractor shall provide the necessary personnel and technical resources to provide support to a variety of operational technology systems in support of the fields technical service needs. The Contractor will **w**ork with various hardware devices and applications including, but not limited to, word processors, Share Point, spreadsheets, presentation graphics, database management systems, document management systems, e-mail programs, and communication systems. This includes:

a) Respond to telephone calls, emails and in-person requests for a variety of technical issues in a timely and courteous manner;
b) Identifies, researches, and resolves technical problems for end users;
c) Provision court authorized intercepts, troubleshoot intercept related issues, maintain reporting functions on intercept related data;
d) Setup and test systems, and will often image and deploy computers;
e) Provide remote support to end users in the field;
f) Assist the Government personnel with creating support documentation including knowledge base documentation and training information; and
g) Assist in the deployment of new applications and hardware.

5.4 INVENTORY SUPPORT

The Contractor shall provide the necessary personnel and technical resources to support ICE with processing Government Furnished Property (GFP), Government Furnished Equipment (GFE) and personal property within the Sunflower Asset Management System (SAMS) or other designated inventory management system. The Contractor will work with various hardware devices and applications including, but not limited to, word processors, spreadsheets, presentation graphics, database management systems, document management systems, e-mail programs, and communication systems. This includes:

a) Perform equipment inventory and maintain accountability for equipment issued to the field;
b) Work with ICE Offices to assist with local barcoded inventories within the prospective areas;
c) Assist ICE Field Offices with surveillance inventory corrections and user support when needed, including field verification and final dispositions;
d) Perform and assist with transfers within SAMS, in and outbound.
e) Verify transfers acceptance, investigate resolutions when issues with transfers occur;
f) Provide annual inventory assistance; field verification and final dispositions;
g) Provide verified input to the SAMS helpdesk to enter in all makes and models for all consumable, non-inventoried items to include supplies;
h) Maintain and update an inventory of all items located in the Technical Operations Center (TOC) facilities, other designated facility;
i) Assist with warehouse duties and front desk coverage;
j) Shipping, receiving and dispensing items to and from carriers;
k) Provide recommendations for continued system improvements to Program Managers and SAMS development team.

l) Preform SAMS training as requested by Program Managers;
m) Prepare ad hoc reports;
n) Assist Program Managers for possible management briefings; and
o) Assist Program Managers on validating SOPs and assist with management briefings.

6.0 GOVERNMENT FURNISHED EQUIPMENT (GFE)

ICE will provide GFE as necessary to support the T3LU CALEA Network and Intercept Operation Support Services.

Contractors will use GFE to perform work under this Task Order and are prohibited from placing ICE data on any non-GFE technology. Any equipment furnished by the Government to the Contractor to perform work under this task shall be returned to the Government at the end of the period of performance. All training materials, policies, procedures, and electronic work products generated as a result of this Task Order becomes the property of ICE.

The Contractor shall keep an inventory of GFE, which shall be made available to the COR upon request. The Government will provide basic equipment (e.g., laptops, tablets, iPhones, biometric equipment, PIV cards) in accordance with the Task Order. Contractor shall provide a fully executed Property Receipt to the ICE Property Custodian within 48 hours of receipt.

The Government will provide any test, analytical, and other IT equipment currently used on-site at the Government facilities to support the Contractor in supporting the Title III systems and CALEA network requirement under this Task Order. The Contractor shall provide its own network connectivity capability with a minimum connection speed of 10 Mbps.

7.0 TRAVEL

This Task Order requires Contractor personnel to travel to ICE Field Offices across the CONUS and other approved facilities (limited to CONUS only) at the discretion of the COR. The primary work locations shall be as follows, but are subject to change: California, Georgia, Minnesota, Oregon, Texas and Virginia.

The Contractor shall travel as required during the performance of this Task Order. All travel requires prior approval by the COR and be appropriately funded prior to incurring costs. Travel expenses shall be reimbursed consistent with Federal Acquisition Regulation (FAR) 31.205-46, the substantive provisions of the Federal Travel Regulation (FTR) and the limitation of funds available for travel as specified in this Task Order. The Contractor shall not be reimbursed for the following travel expenses: transportation expenses for assigned personnel for local commuting between their place of residence and their place of work or for local travel of personnel assigned to the Contractor's sites unless specifically authorized by the COR in writing, in advance. The Contractor shall not be reimbursed for moving or relocation expenses for the Contractor its employees, and / or subcontractors. There may be other travel expenses or other situations where travel expenses will not be reimbursed. Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoices. Only actual travel costs will be reimbursed, and the Contractor is permitted to charge labor hours for

time employees spend traveling. The Contractor shall not be reimbursed if the appropriate documentation is not provided with the invoice or approved in advance.

The following travel information shall be documented in the monthly report:

- Name of Traveler
- Destination
- Dates of Travel
- Cost (costs should be broken down by airfare, car rental, lodging cost, per diem, baggage cost, fuel and Taxi/subway)
- Approval Date
- Name of COR Approving Travel
- Detailed Travel Justification

The Contractor shall provide the COR a trip report which should include:

- Detailed Travel Summary, including Accomplishments
- Observations
- Findings
- Recommendations after travel.

7.1 GENERAL TRAVEL GUIDELINES

- The Contractor shall track, monitor and maintain a current log of all employees on travel;
- The Contractor shall clearly document in the trip report the purpose of the travel, estimated cost, locations, travel dates, Government requester, supported work, and any other justifications or supportive documentation required by the COR;
- As a first option, the Contractor shall have available and assign local resources (within fifty (50) miles of work location) to work on task. Request local resource exception if labor not available. Note: hotel selection has to be within five (5) miles of work location, special exception should be requested if none available, this exception request should include list of three (3) hotels and prices nearby the work location;
- The Contractor shall ensure all appropriate prior approvals are obtained before any travel is scheduled or performed. The Contractor shall ensure the approved request is provided to the COR / GTM, as applicable, by the end of the next business day. If per diem is required it must be included in the prior approval request and cost estimate;
- The Contractor shall ensure all traveling staff is provided a copy of the approved request to carry with them;
- The Contractor shall notify the COR in accordance with the established approval levels, in writing or email for prior approval when the actual cost is projected to exceed the estimated cost prior to incurring the cost and prior to invoicing the Government for the additional cost; and
- The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the trip's purpose.

7.2 TYPES OF TRAVEL

Local Travel – Reimbursement for local travel is not authorized. Local travel is defined as within 50 miles of the work location. All travel requires prior approval from the COR. Travel outside of local travel is travel that is required when the Contractor must go to a location that is other than the normal duty location and that location is more than 50 miles from the normal duty location. The Contractor shall also demonstrate that this location is more than 50 miles from the traveling staff's official residence. The allowable reimbursement under travel is the number miles above 50 miles from the normal duty location. (Example: If the number of miles to the location is 60 miles from the normal duty location, the allowable costs for that traveling staff is 10 miles both ways for a total of 20 miles).

CONUS Travel – CONUS travel is considered as travel within the continental 48 states which includes Washington D.C. All CONUS travel or travel arrangement being made by the Contractor requires prior approval from the COR.

Outside the Continental United States (OCONUS) Travel – OCONUS travel is considered as travel outside the continental 48 States (such as Alaska, Hawaii, Puerto Rico, U.S. territories, and any international travel). All OCONUS travel or travel arrangement being made by the Contractor requires prior approval from the COR. The Contractor shall ensure all staff performing OCONUS travel has the required traveling documentation to include passport, shot records, approved travel request, emergency contact, etc.

8.0 PLACE OF PERFORMANCE

Work, meetings, and briefings shall be performed primarily at Government facilities. On-site support will be at ICE Field Offices across the CONUS and other approved facilities (limited to CONUS only). The primary work locations shall in the following states:

- California at zip code 92154;
- Georgia at zip code 30344;
- Minnesota at zip code 55111;
- Oregon at zip code 97239;
- Texas at zip code 75062, and;
- Virginia at zip codes 22079 and 20191

OCONUS travel *may* be required under this Task Order to other ICE facilities. Zip codes are subject to change to accommodate office moves and or relocations.

9.0 PERIOD OF PERFORMANCE

The Period of Performance for this Task Order is the following:

- Base Year is 12 months inclusive of 30 calendar days for the Transition-In Period;
- Option Year 1 is 12 months;
- Option Year 2 is 12 months;
- Option Year 3 is 12 months, and;

- Option Year 4 is 12 months inclusive of 30 calendar days for the Transition-Out Period.

10.0 WORK SCHEDULE

10.1 HOURS OF WORK

Regular business hours under this Task Order shall be an eight (8) hour workday, between 7:00 a.m. to 5:30 p.m., Monday to Friday local time. All dedicated Contractor support personnel positions require shift work providing 24/7 coverage and on-call access. To the extent that work hours are dependent upon task deadlines, limited access to workspace or Government furnished information, as well as the requirement to have Government employee oversight or availability, CIST may require variances in work hours or limit access to space only when Government employees are available/present to direct performance.

Alternate work schedules must be pre-approved in writing by the COR to ensure coverage and services availability and will be approved on a case-by-case basis by the COR. Variable work schedules may approved by the COR on a case-by-case basis if deemed necessary by the Government to address mission needs. Requested overtime shall require prior written approval from the COR.

10.2 HYBRID WORK SHEDULE

Contractor personnel located within the Cyber and Operational Technology Division in Lorton, VA are permitted to work a hybrid work schedule of three (3) days in office and two (2) days telework. The telework schedule needs to be optimized to ensure office coverage by at least one individual. Operational needs may necessitate changes to the schedule as required by the COR. Situational instances of telework may be permitted upon the approval of the COR.

The Government will not provide space or internet access for teleworking personnel. Contractor or its personnel are responsible for providing the necessary office space and internet access to support working in a telework environment.

Positions authorized to work a hybrid work schedule are subject to the hours of work specified in Section 10.1.

11.0 TECHNICAL TRAINING

The Contractor shall be responsible for providing training to their personnel. The Contractor shall ensure all appropriate Contractor staff attend and any applicable Government required training at Contractor expense when needed for COTS applications and tools. The Contractor shall ensure all Contractor staff skills and knowledge are kept current via retraining at Contractor expense to the appropriate level based on their responsibilities.

The COR may approve reimbursable job-specific technical training that is deemed outside of the basic technical skill sets required to fulfil their responsibilities. The Contractor shall be reimbursed for actual allowable, allocable, and reasonable training costs incurred during performance of this effort.

The Contractor shall ensure that Contractor staff complete all mandatory Government training requirements on Government on – site IT resources before the required deadline. Most training are generally web – based modules.

Examples of such training are:

- Security Awareness Training
- Information Assurance Awareness
- Records Management
- Security Handling off ICE Sensitive But Unclassified / For Official Use Only
- A Culture of Privacy Awareness
- Prevention of Sexual Harassment
- DHS Sunflower Asset Management System
- Other specialized training as required (e.g. for individual with significant security responsibilities)

12.0 DELIVERABLES AND DELIVERY SCHEDULE

The Contractor shall submit all deliverables to the COR and other Government Representatives.

Please note that for any work produced under this Task Order, such as: configuration scripts, security scripts, software written, user manuals, data models, interface control documents, user manuals, technical descriptions of the software and scripts, user operations manuals, system maintenance manuals, and anything else produced under this Task Order would be a deliverable item and that delivery is subject to FAR 52.227-17 (Rights in Data – Special Works).

Deliverables and Delivery Schedule Table

Deliverable/Description	Type	Delivery Method(s)	Delivery Date/Frequency
Kick-Off Presentation Meeting with Meeting Minutes Report	Presentation; Document;	MS PowerPoint; MS Word;	7 calendar days after start of Task Order performance; 5 calendar days after Presentation Meeting
Transition-In Plan	Document	MS Word	7 calendar days after start of Task Order performance.
Transition-Out Plan	Document	MS Word	30 calendar days prior to completion of the overall Task Order Period of Performance (PoP)
Project Management Plan	Document	MS Word	30 calendar days after start of Task Order performance

Monthly Project Status Report	Report	MS PowerPoint	Monthly, by 5th day or next following business day (for previous month)
Standard Operating Procedures (SOPs)	Document	MS Word	30 calendar days after Task Order award. Subsequent SOPs will be "as required" by the COR
Meeting Agenda Report	Document	MS Word	As required by the COR
Meeting Minutes Report	Document	MS Word	As required by the COR
Program Management Review Report	Document	MS PowerPoint	Quarterly
Data Call Response Report	Document	MS Word	Within 7 calendar days of the due date for a data call request.
GFE Inventory Report	Report	MS Excel	Within 24-hours after initial request

12.1 KICK-OFF PRESENTATION (POST-AWARD) MEETING

The Contractor shall present Kick-Off Presentation within 7 calendar days after start of Task Order award performance, to include an overview of the project team, scope of work, deliverables, communication approach, initial risks or issues, and next steps. The Contractor shall also document Contractor positions at all ICE locations. The Contractor shall develop and provide a Meeting Minutes Report within 5 calendar days after the Kick-Off Presentation Meeting.

12.2 PROJECT MANAGEMENT PLAN

The Contractor shall submit a Project Management Plan for outlining the project execution and project control, including the approach, roles, responsibilities, cost, schedule, and scope within 30 calendar days after start of Task Order performance. The document shall be used to facilitate key decision points, milestones, and communication among key stakeholders.
The Project Management Plan shall also take into consideration competing priorities across tasks (including dependencies), business alignment, success factors, improving product quality, development of a product roadmap, addressing technical debt, and reducing delivery cycles.

12.3 MONTHLY PROJECT STATUS REPORT

The Contractor shall submit the Monthly Project Status Report by the 5th day or next following business day (for previous month). The intended audience includes senior

management and executive leadership within ICE. The Contractor shall include historical information for trending purposes, details of work performed, hours spent, accomplishments, staffing, travel, overtime, issues, risks, mitigation strategies, and any action plans. Please note that the Monthly Status Report is not required during the Transition-In Activity.

12.4 STANDARD OPERATING PROCEDURES (SOPS)

The Contractor shall submit the SOPs by the 30 calendar days after Task Order award. Subsequent SOPs will be "as required" by the COR. The Contractor under direct Government collaboration and approval shall develop and implement SOPs the Contractor's progress in the creation, maintenance, and or modification of an applicable SOP for documenting scrum and software development activities. Each SOP shall be written to be an effective guide for on- boarding resources to include workplace logistics, escalation procedures, account and access request processes, and code development guidelines.

12.5 MEETING AGENDA REPORT

The Contractor shall submit "as required" by the COR a Meeting Agenda Report. This includes agenda information relating to the T3LU CALEA Network and Intercept Operation Support Services.

12.6 MEETING MINUTES REPORT

The Contractor shall submit "as required" by the COR a Meeting Minutes Report. This includes details of the meeting relating to the T3LU CALEA Network and Intercept Operation Support Services.

12.7 PROGRAM MANAGEMENT REVIEW REPORT

The Contractor shall submit quarterly a Program Management Review Report. This includes program requirement information relating to the T3LU CALEA Network and Intercept Operation Support Services.

12.8 GFE INVENTORY REPORT

Within 24 hours after initial request from the COR, the Contractor shall provide a GFE Inventory Report. This report shall include asset tag information, serial number, assigned resource, primary office location, the date issued, and a description of the asset.

12.9 DATA CALL RESPONSE REPORT

Within 7 calendar days of the due date for a data call request the Contractor shall provide a Data Call Response Report. This includes data call response requirement information relating to the T3LU CALEA Network and Intercept Operation Support Services.

12.10 DELIVERY INSTRUCTIONS

The Contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via by e-mail. E-mail deliverables should be clearly marked in the subject line as a deliverable (requiring review and/or action by the Government). The electronic copies shall be compatible with Microsoft Office 2003 or greater or other applications as appropriate and mutually agreed to by the parties.

12.11 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government shall provide written notification of acceptance or rejection of all final deliverables within 14 calendar days of receipt. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection. Items must be approved by the COR and/or the Contracting Officer (CO) to be considered "accepted."

Deliverables shall be deemed acceptable if the document adequately covers all required topics, meets general quality measures; and, is professionally prepared in terms of format, clarity and readability; and is delivered in electronic copy on time to the designated delivery location. General quality measures, as set forth below, shall be applied to each work product received from the Contractor.

- **Accuracy:** Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style;
- **Clarity:** Work Products shall be clear and concise. Any/All diagrams and graphics shall be easy to understand and be relevant to the supporting narrative;
- **File Editing:** All text and diagrammatic files shall be editable by the government;
- **Format:** Work Products shall be transmitted via e-mail and in media mutually agreed upon prior to submission; and
- **Timeliness:** Work Products shall be submitted on or before the due date specified in this statement of work or submitted in accordance with a later scheduled date determined by the government.

The documents shall be considered final upon receiving government acceptance. Unless otherwise stated, all deliverables shall be delivered via e-mail not later than 4:00 PM Eastern Time (ET) on the deliverable's due date.

12.12 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. The Government will provide written notification of non-conforming products or services within 14 calendar days of receipt. Deficiencies shall be corrected within 14 calendar days of the rejection notice. If the deficiencies cannot be corrected within 14 calendar days, the Contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within 10 calendar days of receiving the non-conforming products or service notification.

12.13 NOTICE REGARDING LATE DELIVERY

The Contractor shall notify the COR as soon as it becomes apparent to the Contractor that a scheduled delivery will be late. The Contractor shall include in the notification the rationale for late delivery, the expected date for the delivery, and the impact of the late delivery on the project. The COR will review the new schedule with the Program Manager and provide guidance to the Contractor.

12.14 DRAFT DELIVERABLES

The Government will provide written acceptance, comments and/or change requests, if any, within 7 calendar days business days from receipt by the Government of each draft deliverable. Upon receipt of the Government comments, the Contractor shall have 7 calendar days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

12.15 TRANSITION-IN PLAN

The Contractor shall be responsible for the transition of all technical activities identified in this Contract. The Contractor shall submit a Transition-In Plan within 7 calendar days after start of Task Order performance reflecting all necessary activities to facilitate the transition of services to the Contractor and expected completion dates of those activities. All activities must be completed within 30 calendar days after start of Task Order performance. The following technical activities shall be included in the Transition-In Plan:

- Inventory and orderly transfer of all Government Furnished Equipment and Property (GFE/GFP), software and licenses;
- Transfer of current project activities;
- Workplace logistics and staffing plan;
- Coordination of knowledge transfer sessions with the incumbent Contractor;
- Favorable EOD for all Contractor staff from the ICE Personnel Security Unit.

The Transition-in Plan shall be approved by the COR and describe the Contractor's process for transitioning from the incumbent with no disruption in operational services.

12.16 TRANSITION-OUT PLAN

The Contractor shall be responsible for the transition-out of all technical activities identified in this Contract during the final, awarded period of performance. The Contractor shall submit the Transition-Out Plan 30 calendar days prior to the completion of the overall Task Order Period of Performance (PoP) of this Task Order. The Contractor's Transition-Out Plan shall be approved by the COR. The Contractor shall complete the transition activities by the end of the period of performance of this Task Order. The following technical activities shall be included in the Transition-Out Plan:

- Inventory and orderly transfer of all GFE, software, and licenses;
- Submit all contract deliverables to date, including designs, documents, briefings,

reports, spreadsheets, and source code;
- Transfer of current project activities.
- Workplace logistics and staffing plan;
- Coordination of knowledge transfer sessions with the successor Contractor;

The Contractor shall fully support the transition of all Contract requirements to the successor to ensure no disruption in operational services.

13.0 CONTRACTOR PERSONNEL

The Contractor shall identify a Contractor representative as a Point of Contact (POC) for all work under this Task Order.

The Government has determined that the following key personnel labor categories and their associated locations are required:

Position Type	Labor Category	Location/Zip Code*
KEY	SME – Network and Computer Systems Administrators	22079
KEY	SME – Network and Computer Systems Administrators	22079
KEY	Senior Computer Systems Analyst	22079
KEY	Senior Computer Systems Analyst	22079
KEY	Network and Computer Systems Administrator	22079
KEY	Network and Computer Systems Administrator	20191
KEY	Network and Computer Systems Administrator	92154
KEY	Network and Computer Systems Administrator	30344
KEY	Network and Computer Systems Administrator	55111
KEY	Network and Computer Systems Administrator	97239
KEY	Network and Computer Systems Administrator	75062
KEY	Journeyman Management Analyst	22079
KEY	Journeyman Management Analyst	22079
OPTIONAL	SME – Network and Computer Systems Administrator	22079
OPTIONAL	Journeyman Management Analyst	22079

*All positions must be located within the zip codes provided.

It is expected that a minimum of thirteen (13) key personnel will serve in a full-time capacity for the duration of the Task Order or until an equivalent replacement is nominated by the Contractor and accepted by the COR. Optional personnel may be required, if/when exercised by the Government. If exercised, it is expected optional personnel will also serve in a full-time capacity for the duration of the Task Order or until an equivalent replacement is nominated by the Contractor and accepted by the COR

The Contractor shall propose at minimum thirteen (13) key personnel for this SOW who meet the required skills set below. Any certifications not obtained prior to award must be achieved within six months of an individual Contractor's Entry-On-Duty (EOD). All key personnel must exhibit critical soft skills including:

- Excellent active listening and verbal communication skills;
- Strong business writing ability;
- Flexible and adaptable attitude;
- Can conform to shifting priorities, demands, and timelines; and
- Ability to discuss technical issues with non-technical, executive-level government officials.

13.1 SME NETWORK AND COMPUTER SYSTEMS ADMINISTRATOR

The SME Network and Computer Systems Administrators will have overall responsibility to perform system installation, set-up, administration, maintenance, troubleshooting and end-user support to CALEA network. This includes:

- Supervising other Contractors and functioning as a technical expert across multiple network project assignments;
- Optimize system operation and resource utilization;
- Perform system capacity analysis and planning;
- Resolve performance problems with the servers, desktops and network components;
- Serves as a key contact for CIST Program Managers to obtain clarification of problems; and
- Provide resolution of system failures and degradations.

Required Education: Bachelor's degree in Information Technology, engineering or a related academic focus area. Five additional years of related work experience may be substituted for a bachelor's degree.

Required Skills and Experience Required: 10 years or more of relevant experience in an enterprise IT network and computer systems environment;

- Microsoft Certified Solutions Associate (MCSA) Certification – preferred;
- Microsoft Certified Systems Engineer (MCSE) with (+ security) Certification – preferred;
- Project Manager Professional (PMP) Certification – preferred;
- Experience managing IT projects leveraging network infrastructure;
- Proficient in systems administration, using Windows operating systems and high-level Active Directory administration;
- Familiarity with Linux and a general understanding of enterprise virtualization for desktops and servers is desirable;
- Experience to handle multiple IT related projects from inception through to implementation;
- Experience shall include day-to-day administration and operation of complex networked computer-based systems distributed across its geographic region;
- Proficient supporting specialized, intelligence-based computer systems and applications, with the ability to replace hard drives, memory modules, motherboards, power supplies, etc.;
- Competency in infrastructure management techniques such as change management, problem management, configuration management, and system lifecycle;
- Proficient using SAN/Redundant Array of Independent Disks (RAID) and removable storage media, including Compact Disc/Digital Versatile Disc (CD/DVD) and Blu-Ray Discs;
- Excellent verbal and written communications in English to include strong teamwork skills;

This includes being able to communicate complex information with case agents, language services personnel, intelligence analysts, vendors and telephone carriers; and
- The candidate must be capable of performing duties without direct supervision.
- Physical Demands / Work Environment: The physical demands and work environment are the following:

    - While performing the duties of this job, the Contractor is regularly required to walk, sit, stand, kneel, crouch, crawl, reach, lift, carry, push, pull, or otherwise move objects up to 50 lbs. and occasionally lift and/or move up to 80 lbs. Use of a hand truck and/or lift cart is required; This includes:
    - Critical sensory requirements include general vision, close vision, distance vision, color vision, peripheral vision, depth perception, and ability to focus; and
    - Hearing or listening in normal range;

The noise levels vary based on the size/amount of servers located within the facility, but are usually moderate in sound.

13.2 NETWORK AND COMPUTER SYSTEMS ADMINISTRATOR

The Network and Computer Systems Administrator will have overall responsibility to perform system installation, set-up, administration, maintenance, troubleshooting and end-user support to COT-TOC-supplied Title III and Pen Register systems. This includes:

- Provides technical and management input on major tasks or technology assignments;
- Perform system capacity analysis and planning;
- Serves as a key contact for local and remote locations and customers to obtain clarification of problems; and
- Provide resolution of system failures and degradations.

Required Education: Bachelor's degree in Information Technology, Homeland Security, engineering or a related academic focus area. Five additional years of related work experience may be substituted for a bachelor's degree.

Required Skills and Experience Required: 3 years or more of relevant experience in an enterprise IT network and computer systems environment;

- Microsoft Certified Solutions Associate (MCSA) Certification – preferred;
- Microsoft Certified Systems Engineer (MCSE) with (+ security) Certification- preferred;
- Project Manager Professional (PMP) Certification – preferred;
- Experience with domain and technical expertise in networking;
- Experience managing IT projects leveraging network infrastructure;
- Experience in an enterprise IT network and computer systems environment;
- Proficient in systems administration, using Windows operating systems and high-level Active Directory administration;
- Familiarity with Linux and a general understanding of enterprise virtualization for

desktops and servers is desirable;
- Experience to handle multiple IT related projects from inception through to implementation;
- Proficient supporting specialized, intelligence-based computer systems and applications, with the ability to replace hard drives, memory modules, motherboards, power supplies, etc.;
- Competency in infrastructure management techniques such as change management, problem management, configuration management, and system lifecycle;
- Proficient using SAN/RAID and removable storage media, including (CD/DVD) and BLU-RAY Discs;
- Excellent verbal and written communications in English to include strong teamwork skills; This includes being able to communicate complex information with case agents, language services personnel, intelligence analysts, Vendors and telephone carriers.
- Excellent interpersonal skills to relate with technically-trained agents, case agents, telecommunication specialists, system analysts, supervisory linguists, linguists, and end-users who have differing levels of technical skills; and
- The candidate must be capable of performing duties without direct supervision.

Physical Demands / Work Environment:

The physical demands and work environment are the following:

- While performing the duties of this job, the Contractor is regularly required to walk, sit, stand, kneel, crouch, crawl, reach, lift, carry, push, pull, or otherwise move objects up to 50 lbs. and occasionally lift and/or move up to 80 lbs. Use of a hand truck and/or lift cart is required; This includes:
- Critical sensory requirements include general vision, close vision, distance vision,
- color vision, peripheral vision, depth perception, and ability to focus; and
- Hearing or listening in normal range;

The noise levels vary based on the size/amount of servers located within the CMP facility, but are usually moderate in sound.

13.3 JOURNEYMAN MANAGEMENT ANALYST

The Journey Management Analyst will have overall responsibility to primarily support the government processing government owned property (GFP), equipment (GFE) and personal property within the SAMS or other designated inventory management system. Also support a variety of operational technology systems, troubleshooting and end-user support to COT-TOC- supplied equipment and inventory management functions in support of the intelligence and investigative priorities HSI's mission.

Required Education: Bachelor's degree from a nationally accredited college/university. 4 additional years of related work experience may be substituted for a bachelor's degree.

Required Skills and Experience Required: 4 years or more of relevant experience in logistic /inventory support;

- The candidate must be proficient using Windows operating systems and a general understand of Microsoft Office products;
- The candidate must possess knowledge and experience working with Sunflower Assets Management Systems (SAMS);
- Project Manager Professional (PMP) Certification - *preferred*
- Excellent verbal and written communications in English to include strong teamwork skills;
- Excellent interpersonal skills to relate with technically-trained agents, case agents, telecommunication specialists, system analysts, supervisory linguists, linguists, and end-users who have differing levels of technical skills;
- The candidate must be capable of performing duties without direct supervision;

Physical Demands / Work Environment:

The physical demands and work environment are the following:

- While performing the duties of this job, the Contractor is regularly required to walk, sit, stand, kneel, crouch, crawl, reach, lift, carry, push, pull, or otherwise move objects up to 50 lbs. and occasionally lift and/or move up to 80 lbs. Use of a hand truck and/or lift cart is required; This includes:
- Critical sensory requirements include general vision, close vision, distance vision, color vision, peripheral vision, depth perception, and ability to focus;
- Hearing or listening in normal range

13.4 SENIOR COMPUTER SYSTEMS ANALYST

The Senior Computer System Analyst will support the analysis of data processing problems to implement controls and improve computer systems for the end user of those systems. This will involve determining user requirements to deliver products and results the end user needs in their daily operations. This will include a variety of COT-TOC systems as determined by the specific need expressed by the user, and in support of the intelligence and investigative mission of HSI.

Required Education: Bachelor's degree from a nationally accredited college/university. 4 additional years of related work experience may be substituted for a bachelor's degree.

Required Skills and Experience Required

- Proficiency in using Windows operating systems and a basic understanding of Microsoft Office products.;
- Strong verbal and written communication skills in English, with a focus on effective teamwork.
- Excellent interpersonal skills to interact with a diverse group of individuals, including technically trained agents, case agents, telecommunications specialists, system analysts, supervisory linguists, linguists, and end-users with varying levels of technical expertise.
- Ability to work independently and perform tasks without direct supervision.

14.0 SECURITY

GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

POSITION DESIGNATION

IAW Title 5, CFR part 731, dated December 18, 2024, and 5 CFR 1400. Agencies are required to designate position risk and sensitivity level for all contractor employees to determine the commensurate level of background investigation. The public trust risk of a position is the assessment of the degree of potential damage to the efficiency or integrity of the service that could arise from misconduct by the incumbent in the position.

Therefore, once the contract is awarded and before the vendor starts submitting personnel for security vetting, the contractor will provide, through the Contracting Officer's Representatives (CORs) a list of all positions, to include titles and specific description of the duties for each of positions assigned to support the contract.

PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for contractor applicants/employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination by the Office of Professional Responsibility (OPR), ICE Personnel Security Division (PSD). No employee of the contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination by OPR PSD. Contract employees are processed under 5 CFR 731 dated December 18, 2024, and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, or successors thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. Sexual Abuse and Assault Prevention Standards implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003)).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporary, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position

sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through OPR PSD. Contractor applicant/employees are nominated by a Contracting Officer Representative (COR) for consideration to support this contract via submission of the DHS Form 11000-25 and ICE Supplement to the DHS Form 11000-25 to OPR PSD. This contract shall submit the following security vetting documentation to OPR PSD, through the COR, within 10 days of notification of initiation of an Electronic Application for Background Investigations (eAPP), or successor thereto, in the Office of Personnel Management (OPM) automated on-line system:

1. Standard Form 85P (Standard Form 85PS (with supplement to 85P required for those with direct contact with detainees or armed positions)), "Questionnaire for Public Trust Positions" form completed online and archived by the contractor applicant/employee in their NBIS eAPP account.

2. Signature Release Forms (Three total) generated by NBIS eAPP upon completion of Questionnaire (e-signature recommended/acceptable). Completed online and archived by the contractor applicant/employee in their NBIS eAPP account.

3. Electronic fingerprints taken at an approved facility **OR** two (2) SF 87 Fingerprint Cards (current revision) sent to OPR PSD. Additional information regarding fingerprints will be sent to the contractor applicant/employee from OPR PSD.

4. Optional Form 306 Declaration for Federal Employment. This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

5. Social Security Administration 89 form (SSA-89): Authorization for the Social Security Administration (SSA) to Release Social Security Number (SSN) Verification. This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

6. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards). This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

7. One additional document may be applicable if the contractor applicant/employee was born abroad. If applicable, the document will be sent as an attachment in an e-mail to OPR PSD from the contractor applicant/employee.

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under transfer of trust. The questionnaire related to 6 CFR § 115.117 listed above in item 5 will be required for positions designated under PREA. OPR PSD will determine if personnel meet transfer of trust requirements at the initial stage of processing and prior to requesting a new security questionnaire.

With respect to break-in-service requirements for transfer of trust, OPM removed the 24-month break-in-service provision. This requirement is replaced with a new process, established in the Federal Personnel Vetting Investigative Standards issued by the Suitability, Credentialing, and Security Executive Agents, which expands this window of time up to sixty months using a tiered, risk-based approach of graduated levels of investigation.

IAW 5 CFR 731 and E.O. 13764, the fixed five-year periodic reinvestigation for public trust positions and national security positions will soon be eliminated and only once personnel are enrolled in a continuous vetting program. Therefore, PSD will continue the reinvestigation process until this process is completed.

Required information for submission of security packet will be provided by OPR PSD at the time of award of the contract. Only complete packages will be accepted by OPR PSD as notified by the COR.

To ensure adequate background investigative coverage, contractor applicants/employees must currently reside in the United States or its Territories. Additionally, contractor applicants/employees are required to have resided within the United States or its Territories for three or more years out of the last five (ICE retains the right to deem a contractor applicant/employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007, Revision 2, dated August 10, 2024. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007, Revision 2, dated August 10, 2024.

CONTINUED ELIGIBILITY

ICE will exercise full control over granting, denying and/or restrict facility and information access of any contractor employee whose actions conflict with Fitness standards contained in 5 CFR 731 and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a contractor employee from contract support.

The Federal Government is transitioning to Trusted Workforce (TW) 2.0. TW 2.0 is a whole-of-government background investigation reform effort overhauling the personnel vetting process by creating a government-wide system that allows transfer of trust across organizations. All contractor employees will be subjected to the transition and will be enrolled into a continuous vetting system. Enrollment will include multiple requirements from all personnel and potential changes to processes,

procedures, and systems. This contract will comply with all requirements that facilitate the mandated transition to TW 2.0.

OPR PSD will evaluate concerns received via multiple sources under the continuous vetting process, to evaluate continued Fitness of contractor employees. If concerns cannot be mitigated, the contractor will be removed from the ICE contract upon notification from OPR PSD.

REQUIRED REPORTS

The contractor will notify OPR PSD, via the COR providing an ICE Form 50-005, Contractor Employee Separation Clearance Checklist, of all terminations/resignations of contractor employees under the contract within five days of occurrence to the ICEDepartureNotification@ice.dhs.gov group box. The contractor will return any expired ICE issued identification cards and building passes of terminated/resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

IAW DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, the Contracting Officer's Representatives (CORs) notify the servicing personnel and industrial security offices when a contractor employee is no longer working for DHS on any contract and report any derogatory information concerning the individual immediately, in accordance with the contract requirements. Report this information to PSD-CEP-REPORTING@ice.dhs.gov. The report shall include the contractor employees' name and social security number, along with the adverse information being reported.

The contractor will provide, through the COR, a Quarterly Report (on a Microsoft Excel Spreadsheet) containing the names of contractor employees who are actively serving on their contract. The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy. This list is what ICE Industrial Security uses to reconcile the contract quarterly. CORs will submit reports to PSD-Industrial-Security@ice.dhs.gov no later than the 10th day of each January, April, July and October.

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include 'law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information Non-Disclosure Agreement (NDA) for contractor employee access to sensitive information. The NDA will be administered by the COR to all contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies

in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information* and ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information*."

Any unauthorized disclosure of information should be reported to ICE.ADSEC@ice.dhs.gov.

SECURITY MANAGEMENT

The contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OPR PSD through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the contractor.

The COR and OPR shall have the right to inspect the procedures, methods, and facilities utilized by the contractor in complying with the security requirements under this contract. Should the COR determine that the contractor is not complying with the security requirements of this contract, the contractor will be informed in writing by the Contracting Officer of the proper action to be taken to effect compliance with such requirements.

INFORMATION TECHNOLOGY SECURITY

When sensitive government information is processed on Department telecommunications and automated information systems, the contract company agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1*, Information Technology Systems Security* (or its replacement). Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, regardless the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Office of the Chief Information Officer (OCIO) requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Cybersecurity Awareness Training (CSAT) will be required upon initial access and annually thereafter. CSAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on the ICE Training System (ITS) or by contacting ICE.ADSEC@ice.dhs.gov. Contractor employees with significant security responsibilities

shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. System Administrators should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

15.0 PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), 52.224-3 Privacy Training – Alternate I (DEVIATION), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

LIMITING ACCESS TO PRIVACY ACT AND OTHER SENSITIVE INFORMATION

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

PROHIBITION ON PERFORMING WORK OUTSIDE A GOVERNMENT FACILITY/NETWORK/EQUIPMENT

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

PRIOR APPROVAL REQUIRED TO HIRE SUBCONTRACTORS

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

SEPARATION CHECKLIST FOR CONTRACTOR EMPLOYEES

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

CONTRACTOR'S COMMERCIAL LICENSE AGREEMENT AND GOVERNMENT ELECTRONIC INFORMATION RIGHTS

Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

PRIVACY LEAD REQUIREMENTS

If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

APPENDIX A: ACRONYMS

Acronym	Descriptions
AD	Active Directory
CALEA	Communications Assistance for Law Enforcement Act
CD/DVD	Compact Disc/Digital Versatile Disc
CIFS	Common Internet File System
CIST	Communication Intercepts Support Team
CMP	Centralized Monitoring Plant
CONUS	Continental United States
COOP	Continuity of Operations Plan
COR	Contracting Officer
COR	Contracting Officer's Representative
COTS	Commercial Off the Shelf
DNS	Domain Name Server
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FTE	Full Time Equivalent
FTR	Federal Travel Regulations
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GOTS	Government Off the Shelf
GPO	Group Policy Object
HSI	Homeland Security Investigations
LAN	Local Area Network
LDAP	Lightweight Directory Active Protocol
MCSA	Microsoft Certified Solutions Associate
MCSE	Microsoft Certified Systems Engineer
NFS	Network File Systems
NTFS	Network Technology File System
OCIO	Office of the Chief Information Officer
OCONUS	Outside the Continental United States
COT-TOC	Operational Technology and Cyber Division
PII	Personal Identified Information
PIV	Personal Identity Verification

PKI	Public Key Infrastructure
PMP	Project Manager Professional
RAID	Redundant Array of Independent Disks
SAMS	Sunflower Asset Management System
SAN	Storage Area Network
SOP	Standard Operating Procedure
SOW	Statement of Work
SSL	Secure Socket Layer
T3LU	Title III Intercepts and Linguists Unit
TCP/IP	Transmission Control Protocol/Internet Protocol
TOC	Technical Operations Centers
VPN	Virtual Private Network
WAN	Wide Area Network
WSUS	Windows Server Update Services

HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JULY 2023)

(a) *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an

international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any

person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

(End of clause)

ALTERNATE I (JULY 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

HSAR 3052.204-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION: INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

(a) *Definitions*. As used in this clause—

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

> (i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or
>
> (ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or

countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;

(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) *Handling of Controlled Unclassified Information*.

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements*.

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on *https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules*. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
(v) Contracting Officer POC (address, telephone, and email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements*.

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections;
(ii) Investigations;
(iii) Forensic reviews;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

(5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information*. Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization*. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

(f) *Other Reporting Requirements*. Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) *Subcontracts*. The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) *Authority to Operate*. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including templates. These policies and templates are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(i) *Security Authorization Package*. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and

management level deficiencies as outlined in NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp*. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are

created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

HSAR 3052.204-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (JULY 2023)

(a) *Definitions*. Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);
(ii) Date of birth (month, day, and year);

(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;
(v) Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *PII and SPII Notification Requirements*.

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII or SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements*. The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

HSAR Class Deviation 15-01, Revision 1 - Safeguarding of Controlled Unclassified Information: Information Technology Security Awareness Training (JULY 2023)

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed

within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(End of clause)

DHS FAR Class Deviation 17-03, Revision 1 HSAR 52.224-3 Privacy Training – Alternate I (DEVIATION)

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

Appendix # 1: General Cybersecurity Requirements

Compliance with DHS Security Policy Terms and Conditions:

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and DHS 4300A Sensitive Systems Handbook.

Security Review Terms and Conditions

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized COR, and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations

external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

Contractor Employee Access (Sep 2012)

Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy.

This definition includes the following categories of information:

a) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
b) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
c) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
d) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
e) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the CO. Upon the CO's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation

prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

The CO may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason. Including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

Contractor IT Resource Access (Sep 2012)

1) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the COR will arrange and complete any nondisclosure agreement furnished by DHS.

2) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

3) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS Component. It is not a right, a guarantee of access, a condition of the contract, or GFE.

4) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

5) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be grantedonly with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

   a) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
   b) The waiver must be in the best interest of the Government.

6) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the CO.

Privacy Expectations

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed - through that device.

Appendix # 2 Section 508 Accessibility Supplement

1. Section 508 Requirements

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.

1.1 Section 508 Requirements for Technology Services

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.

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

3. 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. 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.

5. When developing or modifying hardware components of ICT, including closed systems (for example – kiosks), the Contractor shall demonstrate conformance to the applicable Section 508 standards

(including the Chapter 4 hardware requirements). Where the requirements in Chapters 4 do not address one or more functions of ICT, the Contractor shall demonstrate conformance to the Functional Performance Criteria specified in Chapter 3. The Contractor shall use a test process capable of validating conformance to all applicable Section 508 standards for hardware functionality delivered pursuant to this contract.

1.2 Section 508 Deliverables

1. **Section 508 Test Plans**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

2. **Section 508 Test Results**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

3. **Section 508 Accessibility Conformance Reports**: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.