U.S. Immigration and Customs Enforcement

**For Official Use Only**

# INVESTIGATIVE CASE MANAGEMENT (ICM) OPERATIONS & MAINTENANCE (O&M) SUPPORT AND OPTIONAL ENHANCEMENTS

## Performance Work Statement

*May 15, 2019*

Immigration and Customs Enforcement

Homeland Security Investigations (HSI)

Mission Support

Homeland Security

**Investigative Case Management (ICM) System Operations & Maintenance, Support and Optional Enhancements**

## 1.0 PROJECT TITLE

Performance Work Statement (PWS) for ICM System Operations & Maintenance (O&M) , Support and Optional Enhancements

## 2.0 BACKGROUND

United States Immigration and Customs Enforcement (ICE) is the largest investigative branch of the Department of Homeland Security (DHS). As part of ICE, Homeland Security Investigations (HSI) is a critical asset in accomplishing the ICE mission and is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within and out of the United States.

HSI is continuing the process of transforming its Information Technology (IT) investment approach and processes for acquiring and delivering enhanced investigative capabilities to its 9,500-person global workforce. To this end, the ICE TECS Modernization Program has created an information technology solution that provides a broad set of mission focused functions as a replacement for the Customs and Border Protection (CBP)-managed legacy TECS system. This ICE TECS Modernization system now provides the core toolset used by HSI agents worldwide to develop and document their criminal investigations. Its functionality includes:

- Case Management – management of information relevant to investigative cases, including investigative reports and approval workflows
- Subject Management – management of information relevant to the various subjects under investigation, including people, businesses, vehicles, etc. and includes the sharing of subject information with CBP for lookout and seizure tracking purposes
- Search – ability to conduct unified searching across multiple systems both internal and external to ICE, primarily regarding subject-related information, around, and in support of investigative processes as well as supplying this data to additional consuming systems within ICE, eg. FALCON, Law Enforcement Information Sharing Services (LEISS), etc.
- Data Warehousing – ongoing management of an HSI data repository which supports both the routine and ad hoc reporting needs of ICE/HSI as well as the sharing of permitted information with external international, national, state and local/tribal law enforcement agencies

Investigative Case Management's (ICM) Initial Operating Capabilities (IOC) were delivered to HSI on June 26, 2016 and have been followed by regularly scheduled (monthly) enhancement/bug fix releases resulting in delivery of the Full Operating Capability (FOC) on August 20, 2017. Regularly scheduled enhancement/bug fix releases, in support of operations and maintenance (O&M), have and will continue.

ICE Office of the Chief Information Officer OCIO and ICE HSI desire to continue to enhance the culture of innovation developed during the delivery of ICE TECS Modernization, where the needs

of the investigative personnel can be quickly realized, often within a matter of weeks. Continuing improvements to ICE's Agile efforts will be enabled via the recent (December 2018) adoption of ICE cloud-based hosting and the ICE Development/Operations (DevOps) toolkit, as well as the continued leveraging of a business-centric approach to system design, which optimizes the adoption of common functionality and reduces the overall complexity associated with systems maintenance.

## 3.0 SCOPE

The subject of this Performance Work Statement is the Investigative Case Management portion of ICE TECS MOD. To deliver ICM functionality ICE employs commercial software, Palantir Technologies, Inc.'s Gotham Product, which has been configured specifically for HSI's operational needs. Current and future releases of ICM are required to have System Maintenance and Services support for the purpose of applying adaptive, perfective and corrective maintenance to the application as well as operating and maintaining the ICM infrastructure, and additionally delivering enhancements, as necessary and procured under this PWS, to the existing product. Support for other ICE TECS MOD components and functionality such as External Interface and Data Warehousing are outside the scope of this PWS.

ICM's broad base of functionality includes:

- Creation and management of ICE/HSI investigative cases and documents
- Creation and management ofcHSI subject records that include information related to persons, vessels, vehicles, aircrafts, businesses, and other thing(s)
- Linking of subject records to reports of investigation (ROIs) and investigative cases
- Creation and management of lookout records shared with Custom and Border Protection (CBP)
- Performing investigative research via system interfaces both internal and external to ICE and DHS
- Creation and management of case statistics (i.e., arrests and seizures)
- Capture and management of administrative data (such as agent work hours on cases)
- Generating operational reports on case-related data
- Managing digital images of artifacts, exhibits and photographs as part of the electronic case record

Under the terms of the proposed contract described in this PWS, Palantir, or any partnering organization capable of delivering the fixes/modifications/enhancements toPalantir Gotham, as configured for ICE/HSI (ICM), will work in close collaboration with all ICE TECS MOD teams and the system owner to support the overall capabilities of ICE TECS MOD via the efficient operation, management, and future enhancement of ICM.

## 4.0 APPLICABLE DOCUMENTS

**All ICE systems shall comply with the following guidelines and regulations:**

- DHS Acquisition Management Directive 102-01 Handbook
- ICE Enterprise Systems Assurance Plan
- ICE System Lifecycle Management (SLM) Handbook, Version 1.4, January, 2012
- ICE Technical Architecture Guidebook
- ICE Technical Reference Model (TRM) (Standards Profile)
    - The Offeror shall identify any hardware, software, and/or licenses required for its proposed solution. The Government is prepared to provide any hardware and software items that are included within the ICE TRM that would reasonably be utilized by Offerors for the system development. Test and evaluation tools listed within the TRM are not provided as Government Furnished Equipment (GFE).
- 4300A DHS Information Security Policy
- 4300A Sensitive Systems Handbook

The following documents are applicable to understanding the target ICE/HSI systems:

- International Information Systems Security Certification Consortium ($ISC^2$) Standards
- National Industrial Security Program Operating Manual (NISPOM), February 28, 2006
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)
    - o Guidelines
    - o Special Publications
    - o Standards
- NIST Special Publication 800-37, Guide for the Certification and Accreditation of Federal Information Systems
- Federal Information Processing Standard (FIPS) 199
- Federal Information Security Management Act (FISMA), November 22, 2002
- Federal Information Technology Security Assessment Framework (FITSAF), November 28, 2000
- Federal OMB Circular A-130, Management of Federal Information Resources
- Federal Privacy Act of 1974 (As Amended)
- Federal Records Act
- DHS 4300A, Sensitive Systems Policy Directive, Version 6.1.1, October 31, 2008
- DHS Management Directive (MD) 4300.1, Information Technology Systems Security, November 03, 2008
- DHS MD Volume 11000 – Security
- DHS Office of Chief Information Officer (OCIO) E-Government Act Report 2008

Please note that if newer versions of these documents are officially released, the Contractor shall comply with the updated versions within the timeframe established by the Government.

The Contractor must understand federal cyber security requirements to include, but not limited to the DHS 4300A Sensitive System Policy, applicable National Institute of Technology (NIST) 800 series documentation, and the Federal Information Security Management Act (FISMA) of 2014 and integrate the security controls in all technology proposed or developed for use in support of the ICE mission.

## 5.0 TASKS

The Contractor shall provide qualified, experienced personnel to deliver support for the continued System Maintenance, Operations and Services tasks associated with ICM in accordance with Palantir Gotham's standard O&M/Support Services Terms and Conditions. This requirement includes the tasks described in the following sections:

### 5.1 Tier 2 System Maintenance and Support

In consultation with the Contractor, items that cannot be resolved at the Tier 1 Support level shall be turned over to Tier 2 ICM System Maintenance and Support.

- The Contractor shall report the status of the ticket using Atlassian Jira tracking software;
- Typical Tier 2 activities would include patching systems and effecting minor fixes, etc. in accordance with Palantir Gotham's O&M/Support Services Terms and Conditions;
- Tier 2 System Maintenance and Support shall be operational in accordance with the performance levels identified in Section 6.0;
- The Contractor shall respond to all Tier 2 System Maintenance tickets in accordance with the contract;
- The Contractor shall implement an application feedback loop, whereas systemic issues identified during common Tier 1, 2, and 3 escalation procedures are routinely evaluated and reviewed with the appropriate Project Manager to assess the need for a System Change Request targeted for a future release.
- If Tier 2 System Maintenance Support cannot resolve the assigned ticket or perform the required tasks then the ticket shall be referred to the Tier 3 - System Maintenance and Support.

### Tier 3 - System Maintenance and Support

The Contractor staff, COR and Program Manager will come to mutual agreement regarding issues that cannot be resolved in Tier 1 or Tier 2 (bug fixes, security patches, or upgrades) to determine whether such issues constitute SCRs (Minor, Moderate, or Major Changes requiring the use of assigned ICM maintenance resources or the procurement of optional development services). Cloud Hosting and Cloud Management Services (Section 5.2.4) actions do not require use of the SCR process. Additionally:

- All maintenance activities that reach this level shall have an SCR opened and be reported using Atlassian Jira;

- SCRs will be prioritized and agreed to by the authorized government personnel

and entered into the ICE approved management tracking tool. SCRs will be approved in writing by the government;

- The Contractor shall implement an application feedback loop, whereas systemic issues identified during common Tier 1, 2, and 3 escalation procedures are routinely evaluated and reviewed with the Government IT Project Manager to assess the need for a SCR in future release.

- The Contractor shall respond to all Tier 3 System Maintenance Support tickets in accordance with the contract;

The Contractor shall provide Software Maintenance Tier 2 and Tier 3 Support. Software Maintenance Tier 2 and Tier 3 normal support hours of operation shall be provided Monday through Friday during the core hours of 9am-5pm, ET, excluding holidays and weekends.

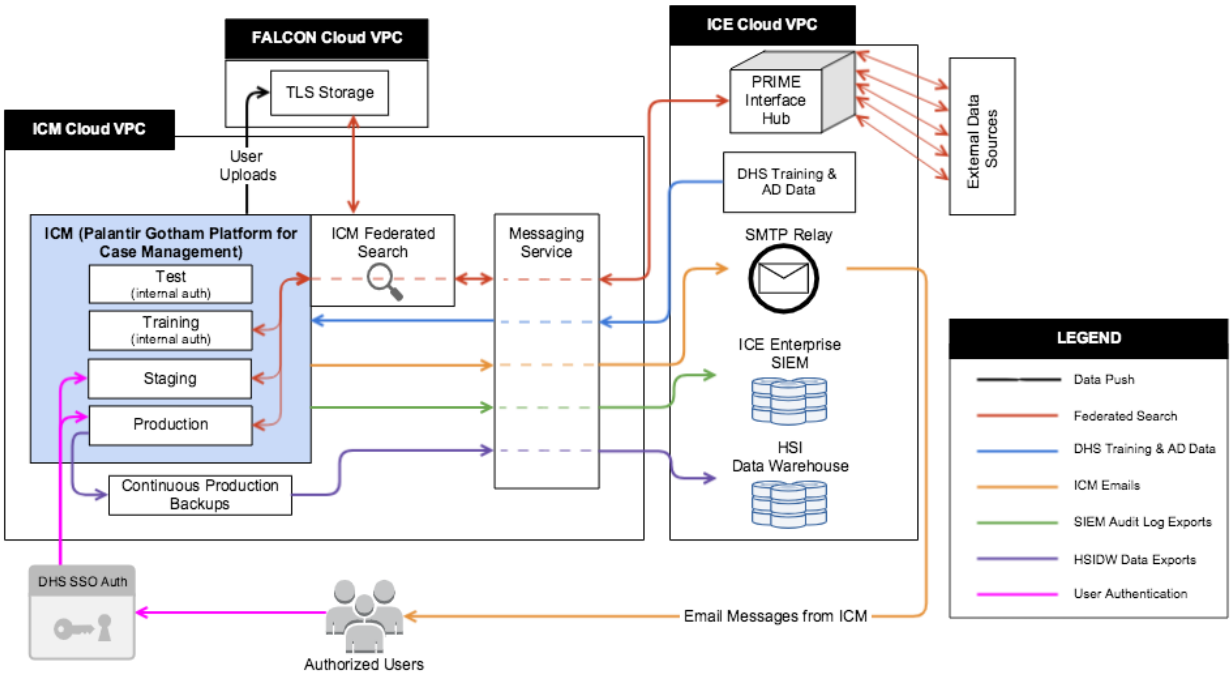
For emergency situations that involve a system outage or a widespread interruption in user access to ICM, both during and outside of the normal support hours of operation, the Contractor shall notify the ICE TECS MOD Program Manager and system owner (or designate) within 30 minutes of occurrence. Emergencies will be further defined as part of the Software Tier 3 Support procedures, but in general an emergency is when the system is down or when multiple users are unable to access ICM. The Contractor shall document all user problem notifications and solutions.

Operations and Maintenance Services consist of bug fixes, security patches, and upgrades in accordance with Palantir Gotham's standard O&M/Support Services Terms and Conditions attached hereto.

### 5.2 Operational Support

The Contractor shall provide Operational Support for the ICM system. Table 2 below details the cloud infrastructure/hardware currently in place for ICM. These assets are subject to change based on mutually agreed upon future expansion requirements.

**Table 2. ICM Cloud Infrastructure and Hardware Overview**




Additional operational support shall include the activities below:

### 5.2.1 Operational Support - Interfaces and Data Sources

The Contractor shall support interfaces that feed directly into and out of the ICM System. Most notable among these is the TLS data sourced from PenLink (Input) and the daily Java Script Object Notation (JSON) feed to the ICE TECS MOD Data Warehouse. The contractor shall ensure the continuation of and proper operation of all data pipelines to/from data sources external to ICM, conditional on those systems providing/accepting data in a format and structure and via a method consistent with agreed upon specifications. The Government recognizes that the Contractor is not able to guarantee continued access to data sources that reside outside the ICM environment, nor can it guarantee Service Level Agreements (SLAs) around the type/quality/quantity of the data such source systems provide. The Government additionally recognizes that breaking changes shall necessitate Minor, Moderate, or Major System Changes to ICM. Whether a breaking change requires a Major System Change to ICM in order to be remediated will be jointly agreed to by the Contractor and the Government.

The contractor must understand federal cyber security requirements to include, but not limited to the DHS 4300A Sensitive System Policy, applicable National Institute of Technology (NIST) 800 series documentation, and the Federal Information Security Management Act (FISMA) of 2014 and integrate the security controls in all technology proposed or developed for use in support of the ICE mission.

### 5.2.2 Operational Support - Database

The Contractor shall support all management and updates to the ICM data stores and indices. This includes all database structural changes and ontology updates to support bug fixes, security patches, and upgrades. In addition to Operations and Maintenance services, the Contractor shall provide or enable the Government to obtain statistical data regarding ICM utilization across HSI and HSI offices and functions.

### 5.2.3 Operational Support – System Tuning

The Contractor shall conduct performance tuning of the ICM system as a result of findings during regular system monitoring and/or as operational needs arise. The Contractor shall provide the ICE TECS MOD Program with recommendations regarding system performance improvements to foster a more stable and robust operational system. The Contractor shall integrate federal cyber security requirements, such as applicable ICE / DHS baseline settings, into network devices during the course of design and development.

#### 5.2.3.1 Operational Support – System Administration

The Contractor shall provide system administration activities to include regular monitoring of system resource utilization, disk storage utilization, identification of corrupt files or processes, system archiving, data archiving, installing operating system/software updates/versions and performing application backups; correcting flaws in software applications that escaped detection during testing of the system, or that have been introduced during previous maintenance activities; and improving software attributes such as performance, memory usage, and documentation. The Contractor shall coordinate security monitoring activities and scans with the ICE Network Operations Center (NOC) and the Security Operations Center (SOC). If the government determines a need to integrate additional monitoring or security capabilities, the Contractor will work with the ICM TECS MOD Program to prioritize such work against all other ongoing efforts. The Contractor shall maintain awareness of and comply with NOC and SOC procedures, to include notification of security incidents and outages, as well as adhere to the ICE Change Control Board (CCB) policies and procedures.

#### 5.2.3.2 Operational Support – System Decommissioning

Should any components or modules of the exiting ICM system be replaced by a follow-on component or module during the performance of this contract, or should the Government decide to halt use of a particular component or module, the Contractor shall facilitate decommissioning of that component or module, per software decommissioning standards and guidelines provided in guiding regulations.

### 5.2.4 Cloud Hosting and Cloud Management Services

The Contractor will provide cloud infrastructure including Combined GovCloud Instances, AWS support package, and SaaS Palantir Cloud.

5.2.4.1 The Contractor will provide AWS GovCloud as the underlying infrastructure for the ICM system's Development/Test, Training, Staging and Production environments.. Additionally, the contractor will manage and administer the ICM environment to ensure timely assessment and triage of issues related to the application when deployed. The contractor will have direct lines of communication to Amazon GovCloud. In summary, the contractor will be responsible for administration and maintenance of their ICM hosting solution, while respecting change management, system availability, system performance, security, and audit requirements.

5.2.4.2 PCloud operates with strict security procedures and has undergone extensive auditing and review to ensure compliance with a broad landscape of regulatory requirements and standards. P- Cloud is SSAE 16 SOC 2 compliant. The contractor team will work with the ICE security components including ISSO and IAD to facilitate testing and documentation as needed to validate the existing FISMA ATO. In addition, the contractor will obtain FedRamp certification as soon as possible.

5.2.4.3 To mitigate the risk of data breach or loss, Contractor managed Hardware Security Modules (HSMs) will be maintained in PCloud. These cloud-based HSMs enable secure data encryption, and will be dispersed across separate AWS regions to provide redundancy and multi-region support.

5.2.4.4 The contractor team will provide monthly Nessus scans of the ICM AWS environment. (Nessus scans systems, networks, and applications for weaknesses and vulnerabilities including malware detection and web application scanning. Nessus also provides the capability to complete external network scans to scan Internet-facing IP addresses for network and web application vulnerabilities. The Database (DB) and any running applications are included in these scans and vulnerabilities that would be visible over open ports are reported.) These scans shall encompass the full range of ports and perform an authenticated scan which checks local libraries, RPMs, etc. against known vulnerabilities or associated exploits; these scans will additionally cover all of the running applications and include network scanning.

5.2.4.5 The PCloud team will be responsible for providing ongoing system and operating system (OS)-level patches and updates as necessary to ensure the security of the ICM system and the data it contains. These configuration changes will not be subject to ICE/OCIO approvals prior to implementation in PCloud and any changes applied will not impact uptime or functional/performance requirements. However, these (and any other) system-level changes will be logged and provided to the ICE ISSO on a regular basis. These logs will include information on day-to-day maintenance activities conducted by the Amazon team and ICM support staff managing the application. Any changes that impact uptime, functional, or performance requirements will be discussed and coordinated with ICE/OCIO and the ICE ISSO for mitigation. Note that all application level SCRs (Tier 3) will follow appropriate approval routes through the ICE TECS MOD PMO before any change is implemented.

5.2.4.6 The Government recommends the contractor acquire an Amazon AWS support package sufficient to support the GovCloud hosting infrastructure stipulated above.

### 5.3 Configuration Management

The Contractor shall conduct application-level configuration management for all Major System Changes made to the system. The Contractor shall handle all requests for changes to established baselines and configuration management thereof via the ICE approved SCR process. The Contractor shall assign proper identification of all configuration items in accordance with agreed upon naming and numbering conventions.

### 5.4 Optional CLINs: Provision of Major System Changes

Although HSI does not intend to routinely and annually obtain Major System Changes (previously called Outcomes in earlier O&M contracts) during the period covered by this contract, the Government recognizes that unanticipated and urgent contingencies may arise that require such significant additions to the existing ICM system. Such contingencies may include national emergencies, significant new trends in transnational, cross-border crimes within HSI's purview, Congressional or court-ordered mandates, or major new law enforcement or regulatory intiatives ordered by ICE or DHS leadership.

The Contractor may perform Major System Changes as directed by the Government and mutually agreed upon in an associated Scope of Work under a separate optional task for Major System Changes; this task shall be for a defined period of performance, with each Major System Change inclusive of all software licenses required to support the requirement listed in the Scope of Work document associated with the Government's Operations and Maintenance Services for the initial period of performance. Upon exercise of the optional CLIN, the Government and Contractor will agree upon the scope and pricing of the Major System Change.

Contractor and the Government will mutually determine whether a request is a Major System Change and should be performed by the Contractor via the Optional Development Task or whether the request is for Minor or Moderate System Changes, meaning additive changes or configuration services, that are contained enough in scope to be considered part of the routine O&M services as defined in this PWS. If there is a dispute between the Contractor and Government over what constitutes a Major System Change, the dispute will be elevated to the Contracting Officer, who will determine the resolution with input from ICE OCIO and through mutual agreement with the Contractor.

#### 5.4.1 Project Plans and Schedules for Completion of Major System Changes

The Contractor shall submit to the ICE Program Manager, HSI and the ICM COR/ACOR, no later than thirty (30) calendar days after the Government has announced its intention to exercise an optional CLIN for Provision of a Major System Change, a draft Project Plan and Schedule. Such Project Plans and Schedules, mutually agreed to by HSI and the

Contractor, shall identify responsible parties required for project completion employed by the Contractor, the Government, and/or a third-party vendor(s), tasks and assignments, potential risks and blockers, and timelines. Progress on the work identified in Project Plans and Schedules will be documented in weekly written reports and will be orally reported on at regularly scheduled or ad-hoc meetings. Project Plans and Schedules may be amended by mutual agreement between the Government and Contractor.

## 6.0 PERFORMANCE STANDARDS

The following table defines the government's expectations in terms of performance standards for the ICM System Maintenance and Services effort and regarding maintaining overall system performance as new features, new data sets, and additional users are added.[1] Performance standards are contingent on the use of Palantir recommended hardware and/or cloud infrastructure.

**Table 5. Performance Standards**

| Tasks | Metric | Expected Service Level | How measured |
|---|---|---|---|
| ICM Search Response Time | Time required for completing a search transaction within ICM | 95% within 5 seconds | Time begins when the user hits enter after specifying the criteria and ends when the search results appear on the results page. |

[1].

| Tasks | Metric | Expected Service Level | How measured |
|---|---|---|---|
| Transaction Response Time | Time required for completing an individual transaction within ICM. | 95% within 5 seconds | Time begins when the user hits enter following data entry and ends when the response screen is displayed |
| Active Users Supported | Average number of users logged into the ICM system | Up to 10,000 unique users monthly | Average number of users logged into the ICM system and processing a transaction within a particular month. |
| System operational availability | System is operating and available to users | System is operational and available 99.07% of scheduled time | The system is considered available when it continues to meet all regular performance metrics for response time, user concurrency, and throughput capability. |

## 7.0 DELIVERABLES AND DELIVERY SCHEDULE

Specific deliverables related to each activity are outlined below.

### 7.1 System Lifecycle Management (SLM) Deliverables

The Contractor shall provide SLM deliverables as required for System Maintenance Services projects. All appropriate documentation shall be prepared in accordance with the guidelines specified by the SLM and the approved Project Tailoring Plan.

### 7.2 Quarterly Progress and QASP Report

The Contractor shall prepare a quarterly progress and QASP report. These reports are due within fifteen (15) calendar days after the completion of the quarter under review. The quarterly reports can be delivered via email and shall contain the following:

- Description of work accomplished (Accomplishments)
- Work planned for the following month (Planned Activities)
- QASP statistics
- Deviations from planned activities
- Open risks and issues

### 7.3 Certification and Accreditation (C&A) Documentation

The Contractor shall be responsible for maintaining and updating existing C&A artifacts to stay current with DHS/ICE and Federal requirements. These C&A updates will be required every three years unless a major change impacts security. The Contractor shall also be responsible for supporting the Information Systems Security Officer (ISSO) for any annual C&A activities, which may be requested (i.e. self-assessments, contingency plan tests, vulnerability scans, etc.).

### 7.4 Quality Assurance Surveillance Plan

The Quality Assurance Surveillance Plan (QASP) is the document used by the Government to evaluate Contractor actions while implementing the PWS. It is designed to provide an effective surveillance method of monitoring Contractor performance for each listed task in the PWS.

The QASP provides a systematic method to evaluate the services the Contractor is required to furnish. The Contractor, and not the Government, is responsible for management and quality control actions to meet the terms of this contract. The role of the Government is quality assurance monitoring to ensure that the contractual standards are achieved.

The Contractor shall be required to develop a comprehensive program of inspections and monitoring actions. Once the quality control program is approved by the Government, careful application of the process and standards presented in the QASP document will ensure a robust quality assurance program. The offeror will propose metrics they determine pertinent dependent upon the details surrounding their own technical approach in meeting the task order objectives.

- Measurements will be performed quarterly.
- Measurements will be carried out by Contractor.
- QASP measurement report will be turned in quarterly to the government Contracting Officer's Representative (COR) within fifteen calendar days after the end of the quarter under review.
- An overall quarterly QASP Rating will be computed for the Contractor by the COR.

### 7.5 Deliverables Table

The Contractor shall provide the following deliverables via email to the COR, unless noted otherwise:

| Deliverable | Frequency | Recipients |
|---|---|---|
| SLM Deliverables (Doc) & Software (SW) (Software includes updates/new versions of the primary Gotham platform; new workflow applications and updated versions of existing workflow applications | As Required | Electronic copy – PM & COR<br><br>Software (SW): ICE source control repository ((GIT); OCIO representative of ICE<br>TECS MOD Program |
| Project Plans and Schedules for optional tasks for Provision of a Major System Change, Section 5.4.1 | 30 calendar days following the Government's announcement of its intention to exercise the optional task | Electronic copy - PM, Contracting Officer, COR/ACOR |
| Quarterly Progress and QASP Reports, Section 7.2 | Quarterly, within 15 calendar days of the end of the quarter being reviewed | Electronic copy: PM, Contracting Officer, COR/ACOR |
| Certification and Accreditation Documentation | As Required | Electronic copy: PM, COR/ACOR |

| | | |
|---|---|---|
| Training Documentation | As Required | Electronic copy: PM, COR/ACOR |
| Transition In Plan- Final | 15 calendar days after award | Electronic copy: PM, Contracting Officer, COR/ACOR |
| Transition Out Plan | 120 calendar days before the end of the contract | Electronic copy: PM, Contracting Officer, COR/ACOR |
| Contractor's QASP Administration Plan | 15 calendar days after award | Electronic copy: PM, Contracting Officer, COR/ACOR |

### 7.6 Delivery Instructions

The Contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment to the COR. The electronic copies shall be compatible with MS Office 2010 or other applications as appropriate and mutually agreed to by the parties. The documents shall be considered final upon receiving Government approval. All deliverables shall be delivered electronically (unless a hardcopy is requested) to the COR. If a hardcopy is requested, it will be delivered to the designated COR, not later than 4:00 PM ET on the deliverable's due date. Once created, deliverables and work products are considered the property of the Federal Government. Any work that deviates from this contract and the approved deliverables listed herein shall not be accepted without prior approval from the COR.

### 7.7 Draft Deliverables

The Government will provide written acceptance, comments and/or change requests, if any, within 15 working days from receipt by the Government of each draft deliverable.
Upon receipt of the Government comments, the Contractor shall have 15 working days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

### 7.8 Written Acceptance/Rejection by the Government

The Government shall provide written notification of acceptance or rejection of all final deliverables within fifteen (15) calendar days. 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 appropriate Government authority to be considered "accepted." The Government will provide written acceptance, comments, or change requests within fifteen (15) calendar days from receipt by the Government, of all required deliverables.

### 7.9 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 fifteen (15) calendar days. Deficiencies shall be corrected within 30 days of the rejection notice. If the deficiencies cannot be corrected within 30 calendar days, the Contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten (10) calendar days.

### 7.10 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 PM and provide guidance to the Contractor.

## 8.0 CONSTRAINTS

### 8.1 General Constraints

The following project constraints are applicable to the ICM System Maintenance and Services task order:

- Existing ICM system is a version of a Commercial, Off the Shelf (COTS) productfrom , that has been specifically configured to meet HSI's needs;
- ICM will be primarily accessed from the existing ICE standard desktop;
- ICE-OCIO must approve in writing any exceptions to the established ICE-OCIO System Lifecycle Management (SLM) processes;
- The Contractor shall comply with all DHS information security regulations for all Law Enforcement sensitive data;
- The Contractor shall comply with all applicable technology standards and architecture policies, processes, and procedures defined in ICE OCIO Architecture Division publications;
- The Contractor shall comply with the ICM specific configuration management plan for all design and development artifacts in accordance with guidelines set forth in the Plan;
- ICE will provide Government Furnished Equipment as necessary to support all ICM System Maintenance and Services activities.

### 8.2 DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following: Homeland Security Enterprise Architecture (HLS EA), National Institute of Standards and Technology (NIST) & Federal Information Security Management Act (FISMA) requirements:

• All developed solutions and requirements shall be compliant with the HLS EA.

• All IT hardware and software shall be compliant with the HLS EA Technical Reference Model

(TRM) Standards and Products Profile.
• Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
• Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
• Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special 8 ITAR Quick Essentials Guide 2011 v2.0 Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.
• Integrate federal cyber security requirements to include, but not limited to the DHS 4300A Sensitive System Policy, applicable National Institute of Technology (NIST) 800 series documentation, and the Federal Information Security Management Act (FISMA) of 2014 into technical solutions and provide strategies to meet on-going operational security controls in areas such as security patching, configuration management, authentication, and security monitoring.

### 8.3 Project Governance

The Government and Contractor shall on a quarterly basis meet to review the state of the work performed under the PWS and discuss any issues regarding how the project is being conducted and mutually agree upon resolving any concerns. Such quarterly meeting shall include HSI management from the Government and executive leadership from the Contractor.

## 9.0 GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION

The Contractor shall keep an inventory of Government-furnished equipment (GFE), which shall be made available to the COR, Assistant COR, and Government Property Custodian upon request. The Government will provide basic equipment (e.g., laptops, desktops, etc.) in accordance with the contract. All GFE shall be entered into ICE's Property Inventory System (Sunflower) within Record hours of receipt. The Contractor shall provide their own network connectivity capability with a minimum connection speed of no less than 10Mbps.

Items of GFE which are inventoried and tracked in Sunflower include laptops and i-Phone handheld devices that will be listed on an inventory master list to be jointly maintained by the Government COR and the Contractor PM; all Record Receipt – Property Issued to Employee (Forms G570) documentation will be kept current.

### 9.1 Remote Access

Contractor shall be provided with remote access to the DHS network for mutual convenience

while the contractor performs business for the DHS Component.

## 10.0 OTHER DIRECT COSTS (ODCs)

Travel outside the local metropolitan Washington, DC area may be expected during performance of this contract. . Reimbursement for allowable costs will be made. Any travel and training expenditures shall be pre-approved by the COR. Costs for transportation, lodging, meals and incidental expenses incurred by Contractor personnel on official company business are allowable subject to FAR 31.205-46, Travel Costs. These costs will be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the Federal Travel Regulations. The Contractor will not be reimbursed for travel and per diem within a 50-mile radius of the worksite where a Contractor has an office. Local travel expenses within the Washington Metropolitan area will not be reimbursed (this includes parking). All travel outside the Washington Metropolitan area must be approved by the COR in advance. No travel will be reimbursed without prior approval from the COR. All travel in connection with this PWS by Contractor personnel to HSI facilities, outside of regularly scheduled meetings with ICE TECS MOD IPTs and support teams, shall require prior notification to and approval by the ICE TECS MOD Program Manager and COR. Contractor will not seek reimbursement for travel expenses.

## 11.0 PLACE OF PERFORMANCE

Work, meetings, and briefings will be performed primarily at Contractor facilities. Frequent travel to ICE offices located at 2450 Crystal Drive, Arlington, Virginia or 500 12th St SW, Washington, D.C will be required. Additionally, travel to the Law Enforcement Support Center (LESC) facility located in Williston, VT may be required.

## 12.0 PERIOD OF PERFORMANCE

The period of performance of the ICM System Maintenance and Services contract will consist of a base period of twelve (12) months plus four (4) twelve (12) month option periods.

## 13.0 SECURITY

Contractor personnel performing work under this PWS will require access to Sensitive but Unclassified, (SBU), For Official Use Only (FOUO) data. The contractor shall not employ any foreign subcontractor participation.

### 13.1 Section 508 Compliance

#### 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.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. 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.

**Item that contains Information and Communications Technology (ICT):** Investigative Case Management

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates; Electronic reports; Electronic training materials; Multi-media (video/audio)): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Electronic content and software authoring tools and platforms; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):**
Subject Management

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Electronic forms; Multi-media (video/audio); Interactive maps): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):**
Investigation Narratives

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and**

**components** (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates; Multi-media (video/audio)): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):** Internal Data Queries

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):** External Data Queries

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):** multimedia objects

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address

one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Multi-media (video/audio)): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):** seized asset tracking

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates; Multi-media (video/audio)): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Electronic content and software authoring tools and platforms; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):** Workflow

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Electronic forms; Multi-media (video/audio)): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

**Item that contains Information and Communications Technology (ICT):** Work Hour tracking

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater

accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates; Multi-media (video/audio)): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

**Applicable 508 requirements for software features and components** (including Web, desktop, server, mobile client applications; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

**Applicable 508 requirements for hardware features and components** (including Computers & laptops; Servers): All requirements in Chapter 4 apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

2. When providing and managing hosting services for ICT, the contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance before providing the hosting service.

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

4. 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 substitutions and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat

5. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.

6. When developing or modifying web and software ICT, the contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the

DHS Trusted Tester Methodology currently approved for use, as defined at https://www.dhs.gov/compliance-test-processes. The contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at https://www.dhs.gov/publication/trusted-tester-resources.

7. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/compliance-test-processes.

8. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

9. 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 January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

10. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

---

**Instructions:** Please include the following language in your solicitation package, and include with any associated ITAR approval requests. If you do not include this language in your package, you will not receive information from vendors needed to determine if they meet the accessibility requirements. This language can be included in the SOW or in other parts of the solicitation package based on the solicitation type. The following instructions are intended to provide offerors guidance on how to document the manner in which their proposed solution addressed the Section 508 requirements outlined in the previous section. This documentation shall be included with their proposal. These instructions shall also be included with any other instructions provided to potential offerors on how to respond to the solicitation. **Caution**: Do not misconstrue these instructions to be Section 508 requirements, evaluation factors, or acceptance criteria.

---

**Instructions to Offerors**

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed in accordance with all the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Supports", "Supports with Exceptions", "Does Not Support", and "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each ICT Item that will be developed, modified, installed, configured, integrated, or hosted by the contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.

3. For each commercially available authoring tool offered that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Offeror shall describe the level of Section 508 compliance supported for the content that can be generated.

4. The offeror shall describe plans for features that do not fully conform to the Section 508 Standards.

---

**Instructions:** Insert the following language into the Acceptance Criteria section of the solicitation, and include with any associated ITAR approval requests. If the solicitation uses the FAR Uniform Contract Format (UCF), this text would be placed in Section E., Inspection and acceptance. (See FAR 14.201-1, et. seq. and FAR 15.204-1, et. seq.)

---

**Acceptance Criteria**

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:

- Accessibility test results based on the required test methods.
- Documentation of features provided to help achieve accessibility and usability for people with disabilities.
- Documentation of core functions that cannot be accessed by persons with disabilities.
- Documentation on how to configure and install the ICT Item to support accessibility.
- Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).

2. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

### 13.2 General Clause

To ensure the security of the DHS/ICE information in their charge, ICE Contractors and Sub-contractors shall adhere to the same computer security rules and regulations as Federal Government employees unless an exception to policy is agreed to by the prime Contractors, ICE Information Systems Security Manager (ISSM) and Contracting Officer and detailed in the contract. Non-DHS Federal employees or Contractors who fail to comply with DHS/ICE security policies are subject to having their access to DHS/ICE IT systems and facilities terminated, whether or not the failure results in criminal prosecution. The DHS Rules of Behavior document applies to DHS/ICE support Contractors and Sub-contractors.

### 13.3 Security Policy References Clause

The following primary DHS/ICE IT Security documents are applicable to Contractor/Sub-contractor operations supporting Sensitive But Unclassified (SBU) based contracts. Additionally, ICE and its Contractors shall conform to other DHS Management Directives (MD) (Note: these additional MD documents appear on DHS-Online in the Management Directives Section. Volume 11000 "Security and Volume 4000 "IT Systems" are of particular importance in the support of computer security practices), NIST and FISMA requirements:

- DHS 4300A, Sensitive Systems Policy Directive
- DHS 4300A, IT Security Sensitive Systems Handbook
- ICE Directive, IT Security Policy for SBU Systems
- National Institute of Technology (NIST) 800 series documentation (all applicable)
- Federal Information Security Management Act (FISMA) of 2014

#### 13.3.1 Contractor Information Systems Security Officer (ISSO) Point of Contact Clause

The Contractor shall appoint and submit a name to ICE ISSM for approval, via the ICE COR, of a qualified individual to act as ISSO to interact with ICE personnel on any IT security matters.

### 13.3.2 Protection of Sensitive Information

The Contractor shall protect all DHS/ICE "sensitive information" to which the Contractor is granted physical or electronic access by adhering to the specific IT security requirements of this contract and the DHS/ICE security policies specified in the Reference Section above. The Contractor shall ensure that their systems containing DHS/ICE information and data be protected from unauthorized access, modification and denial of service. Further, the data shall be protected in order to ensure the privacy of individual's personal information.

### 13.3.3 Information Technology Security Program

If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall establish and maintain an IT Security Program. This program shall be consistent with the referenced DHS/ICE IT security policy documents and at a minimum contain and address the following elements:

- Handling of DHS/ICE sensitive information and IT resources to include media protection, access control, auditing, network security, and rules of behavior
- Certification and Accreditation (C&A) and FISMA compliance of Systems containing, processing or transmitting of DHS/ICE data
- Training and Awareness for Contractor personnel
- Security Incident Reporting
- Contingency Planning
- Security Reviews
- Contract Closeout Actions

### 13.3.4 Handling of Sensitive Information and IT Resources

The Contractor shall protect DHS/ICE sensitive information and all government provided and Contractor-owned IT systems used to store or process DHS/ICE sensitive information. The Contractor shall adhere to the following requirements for handling sensitive information:

- **Media Protection**. The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive information stored on media to be surplused, transferred to another individual, or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using DHS/ICE approved sanitization methods. The Contractor shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen. These procedures shall address the handling and protection of paper and electronic outputs from systems (computers, printers, faxes, copiers) and the transportation and mailing of sensitive media.)
- **Access Control.** The Contractor shall control user access to DHS/ICE sensitive information based on positive user identification, authentication, and authorization (Roles and Rules based) mechanisms. Access control measures employed shall provide

protection from unauthorized alternation, loss, unavailability, or disclosure of information. The Contractor shall ensure its personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. The Contractor shall divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process.

- **Auditing.** The Contractor shall ensure that it's Contractor-owned IT systems used to store or process DHS/ICE sensitive information maintain an audit trail sufficient to reconstruct security relevant events. Audit trails shall include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. The Contractor shall periodically review audit logs and ensure that audit trails are protected from modification, authorized access, or destruction and are retained and regularly backed up.
- **Network Security.** The Contractor shall monitor its networks for security events and employ intrusion detection systems capable of detecting inappropriate, incorrect, or malicious activity. Any interconnections between Contractor-owned IT systems that process or store DHS/ICE sensitive information and IT systems not controlled by DHS/ICE shall be established through controlled interfaces and documented through formal Interconnection Security Agreements (ISA). The Contractor shall employ boundary protection devices to enforce access control between networks, including Internet and extranet access. The Contractor shall ensure its e-mail systems are secure, properly configured, and that network protection mechanisms implemented in accordance with DHS/ICE requirements. The Contractor shall conduct periodic vulnerability assessments and tests on its IT systems containing DHS/ICE sensitive information to identify security vulnerabilities. The results, of this information, will be provided to the ICE OCIO for review and to coordinate remediation plans and actions.
- DHS employees and Contractors shall not transmit sensitive DHS/ICE information to any personal e-mail account that is not authorized to receive it.
- **Rules of Behavior.** The Contractor shall develop and enforce Rules of Behavior for Contractor-owned IT systems that process or store DHS/ICE sensitive information. These Rules of Behavior shall meet or exceed the DHS/ICE rules of behavior.
- The Contractor shall adhere to the policy and guidance contained in the DHS/ICE/NIST/FISMA reference documents.

**Safeguarding of Sensitive Information (March 2015)**

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

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying

information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as 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:

> (1) 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);
>
> (2) 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);
>
> (3) 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

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is

acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below. The Contractor must be cognizant of the requirement to support renewal of the ATO during the performance period of this contract and shall plan work and staffing accordingly.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation 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). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the 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 Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall

address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary

as determined by the Government, 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) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems. In accordance with DHS 4300A Sensitive Systems Handbook Attachment H and FISMA Policy, Contractor shall develop a remediation plan addressing any/all system weaknesses to be detailed in a Plan of Action and Milestones (POA&M). The POA&M shall be completed by the scheduled completion date.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of

discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, 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) Data Universal Numbering System (DUNS);
(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, email);
(v) Contracting Officer POC (address, telephone, 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 sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy 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 sensitive information 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, and
(iv) Data analyses and processing.

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

(h) *Additional PII and/or SPII Notification Requirements.*

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions 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 and 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, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information 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; and/or

(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 FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

### 13.3.5 Training and Awareness

The Contractor shall ensure that all Contractor personnel (including Sub-contractor personnel) who are involved in the management, use, or operation of any IT systems that handle DHS/ICE sensitive information, receive annual training in security awareness, accepted security practices, and system rules of behavior. If the Contractor does not use the ICE-provided annual awareness training, then they shall submit to the ICE ISSM their awareness training for approval. Should Contractor Training be approved for use, the Contractor shall provide proof of training completed to the ICE ISSM when requested.

The Contractor shall ensure that all Contractor personnel, including Sub-contractor personnel, with IT security responsibilities, receive specialized DHS/ICE annual training tailored to their specific security responsibilities. If the Contractor does not use the ICE-provided special training, then they shall submit to the ICE ISSM their awareness training for approval. Should Contractor training be approved for use, the Contractor shall provide proof of training completed to the ICE ISSM when requested.

Any Contractor personnel who are appointed as ISSO, Assistant ISSOs, or other position with IT security responsibilities, i.e., System/LAN Database administrators, system analyst and programmers may be required to attend and participate in the annual DHS Security Conference.

### 13.3.6 Certification and Accreditation (C&A) and FISMA compliance

The Contractor shall ensure that any Contractor-owned systems that process, store, transmit or access DHS/ICE information shall comply with the DHS/ICE C&A and FISMA requirements.

Any work on developing, maintaining or modifying DHS/ICE systems shall be done to ensure that DHS/ICE systems are in compliance with the C&A and FISMA requirements. The Contractor shall ensure that the necessary C&A and FISMA compliance requirements are being effectively met prior to the System or application's release into Production (this also includes pilots). The Contractor shall use the DHS provided tools for C&A and FISMA compliance and reporting requirements.

### 13.3.7 Security Incident Reporting

The Contractor shall establish and maintain a computer incident response capability that reports all incidents to the ICE Computer Security Incident Response Center (CSIRC) in accordance with the guidance and procedures contained in the referenced documents.

### 13.3.8 Contingency Planning

If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall develop and maintain contingency plans to be implemented in the event normal operations are disrupted. All Contractor personnel involved with contingency planning efforts shall be identified and trained in the procedures and logistics needed to implement these plans. The Contractor shall conduct periodic tests to evaluate the effectiveness of these contingency plans. The plans shall at a minimum address emergency response, backup operations, and post-disaster recovery.

### 13.3.9 Security Review and Reporting

The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

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 DHS/ICE, including the Office of Inspector General, ICE ISSM, and other government oversight organizations, access to the Contractor's and Sub-contractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. 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 DHS/ICE data or the function of computer systems operated on behalf of DHS/ICE, and to preserve evidence of computer crime.

### 13.3.10 Use of Government Equipment

Contractors are not authorized to use Government office equipment (IT systems/computers) for personal use under any circumstances, unless limited personal use is specifically permitted by the contract. When so authorized, Contractors shall be governed by the limited personal use policies in the referenced documents.

### 13.3.11 Contract Closeout

At the expiration of this contract, the Contractor shall return all sensitive DHS/ICE information and IT resources provided during the life of this contract. The Contractor shall certify that all DHS/ICE information has been purged from any Contractor-owned system used to store or process DHS/ICE information. Electronic media shall be sanitized (overwritten or degaussed) in accordance with the sanitation guidance and procedures contained in reference documents and with DHS/NIST/National Security Agency (NSA) approved hardware and software. Note that these procedures may be wavied by the COR, contingent upon approval of a follow-on contract with the current Contractor.

### 13.3.12 Personnel Security

DHS/ICE does not permit the use of non U.S. Citizens in the performance of this contract or to access DHS/ICE systems or information.

All Contractor personnel (including Sub-contractor personnel) shall have favorably adjudicated background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/ICE sensitive information.

The Contractor shall ensure all Contractor personnel are properly submitted for appropriate clearances.

The Contractor shall ensure appropriate controls have been implemented to prevent Contractor personnel from obtaining access to DHS/ICE sensitive information before a favorably adjudicated background investigation has been completed and appropriate clearances have been issued. At the option of the Government, interim access may be granted pending completion of a pre-employment check. Final access may be granted only upon favorable completion of an appropriate background investigation based on the risk level assigned to this contract by the Contracting Officer.

The Contractor shall ensure its personnel have a validated need to access DHS/ICE sensitive information and are granted the most restrictive set of access privileges needed for performance of authorized tasks.

The Contractor shall ensure that its personnel comply with applicable Rules of Behavior for all DHS/ICE and Contractor-owned IT systems to which its personnel have been granted access privileges.

The Contractor shall implement procedures to ensure that system access privileges are revoked for Contractor personnel whose employment is terminated or who are reassigned to other duties and no longer require access to DHS/ICE sensitive information.

The Contractor shall conduct exit interviews to ensure that Contractor personnel who no longer require access to DHS/ICE sensitive information understand their obligation not to discuss or disclose DHS/ICE sensitive information to which they were granted access under this contract.

### 13.3.13 Physical Security

The Contractor shall ensure that access to Contractor buildings, rooms, work areas and spaces, and structures that house DHS/ICE sensitive information or IT systems through which DHS/ICE sensitive information can be accessed, is limited to authorized personnel. The Contractor shall ensure that controls are implemented to deter, detect, monitor, restrict, and regulate access to controlled areas at all times. Controls shall be sufficient to safeguard IT assets and DHS/ICE sensitive information against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. Physical security controls shall be implemented in accordance with the policy and guidance contained in the referenced documents.

## 13.4 ISO Terms and Conditions for Sensitive but Unclassified Requests

### 13.4.1 DHS Security Policy Requirement

The following terms and conditions should be included in all acquisition documents.
All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

#### 13.4.1.1 Encryption Compliance Requirement

The following terms and conditions should be included in all acquisition documents.

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
2. National Security Agency (NSA) Type 2 or Type 1 encryption.
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

#### 13.4.1.2 Security Review Requirement

The following requirements should be included in all acquisition documents.

##### 13.4.1.2.1 Security Review

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 DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), 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 the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. 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 DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

#### 13.4.1.3 Interconnection Security Agreement (ISA)

The following requirements should be included in the acquisition document if the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity.

##### 13.4.1.3.1 Interconnection Security Agreement Requirements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

### 13.4.2 Required Protections for DHS Systems Hosted in Non-DHS Data Centers

The following requirements should be included in acquisition documents for information systems which are hosted, operated, maintained, and used on behalf of DHS at non-DHS facilities. Contractors are fully responsible and accountable for ensuring compliance with all Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) and related DHS security control requirements (to include configuration guides, hardening guidance, DHS Security Policy, Procedures, and Architectural guidance). The contractor security procedures shall be the same or greater than those that are provided by DHS Enterprise Data Center(s). Please note that all of the subsections from **Security Authorization** to **Log Retention** are included in this requirement.

### 13.4.3 Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COTR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these requirements. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

### 13.4.4 Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture in accordance with applicable laws and DHS policies to the satisfaction of the DHS COTR. Areas of consideration could include:

1. Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
2. Compliance to DHS Identity Credential Access Management (ICAM)
3. Security reporting to DHS central control points (i.e. the DHS Security Operations Center (SOC) and integration into DHS Security Incident Response
4. Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
5. Performance of activities per continuous monitoring requirements
6. Maintain awareness of and comply with ICE NOC and SOC procedures to include notification of security incidents and outages;
7. Integrate federal cyber security requirements, such as applicable ICE / DHS baseline settings, into network devices during the course of design and development.

### 13.4.5 Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management
5. Log Integration
6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

### 13.4.6 Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

#### 13.4.6.1 Security Operations

The Contractor shall operate a SOC to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform

continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan.

#### 13.4.6.2 Computer Incident Response Services

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

#### 13.4.6.3 Firewall Management and Monitoring

The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

#### 13.4.6.4 Intrusion Detection Systems and Monitoring

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

#### 13.4.6.5 Physical and Information Security and Monitoring

The Contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

#### 13.4.6.6 Vulnerability Assessments

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating

systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

#### 13.4.6.7 Anti-malware (e.g., virus, spam)

The Contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

#### 13.4.6.8 Patch Management

The Contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

#### 13.4.6.9 Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

#### 13.4.6.10 Supply Chain Risk Management Requirement

Supply Chain risks result from adversarial exploitation of the organizations, people, activities, information, resources, or facilities that provide hardware, software, or services. These risks can result in a loss of confidentiality, integrity, or availability of information or information systems. A compromise to even minor system components can lead to adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

**Authorities:**
Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management
Department of Homeland Security, Security Policy for Sensitive Systems 4300A
Homeland Security Presidential Directive 23, Cyber Security and Monitoring, 8 January 2008
Office of Budget and Management Circulation A-130, Appendix III

•National Institute of Standards and Technology, Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

#### 13.4.6.10.1 Supply Chain Risk Management

The following requirements should be included in all hardware and software requests to ensure the confidentiality, integrity, and availability of government information.
The Contractors supplying the Government hardware and software shall provide the manufacture's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state and/or domain of registration and DUNs number of those suppliers must also be provided.
Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.
The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.
Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.
The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.
The Supply Chain Risk Management Plan shall address the following elements:

1. How risks from the supply chain will be identified,
2. What processes and security measures will be adopted to manage these risks to the system or system components, and
3. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Technical Representative (COTR) 30 days post award.
The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.
The Contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.
The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.
The Contractor shall be excused from using new OEM (i.e. "grey market," previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e. until the “end of life.”). Software updates and patches must be made available to the government for all products procured under this contract.
Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.
All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.
These records must be readily available for inspection by any agent designated by the US Government as having the authority to examine them.
This transit process shall minimize the number of times en route components undergo a change of custody and make use tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government’s request, shall be able to provide shipping status at any time during transit. The Contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

#### 13.4.6.11 Personal Identification Verification (PIV) Credential Compliance

Authorities:

- HSPD-12 “Policies for a Common Identification Standard for Federal Employees and Contractors”
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 “Acquisition of Products and Services for Implementation of HSPD-12”
- NIST FIPS 201 “Personal Identity Verification (PIV) of Federal Employees and Contractors”
- NIST SP 800-63 “Electronic Authentication Guideline”
- OMB M-10-15 “FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management”

##### 13.4.6.11.1 Personal Identification Verification (PIV) Credential Compliance Requirement

Procurements for products, systems, services, hardware, or software involving controlled facility

or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.
Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.
PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.
If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

### 13.4.7 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006) (3052.204-70 Security requirements for unclassified information technology resources.)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within ["insert number of days"] days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include—

(1) Acquisition, transmission or analysis of data owned by DHS with significant

replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e)Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.
(End of clause)

### 13.4.8 CONTRACTOR EMPLOYEE ACCESS (SEP 2012) (3052.204-71 Contractor employee access.)

(a) 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:

(1) 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, Pub. L. 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);

(2) 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);

(3) 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

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) “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.

(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 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.

(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 sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. 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.

(f) 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.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR 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 COTR, 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.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. 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.

## 14.4 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**GENERAL**

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in 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.

**PRELIMINARY DETERMINATION**

ICE will exercise full control over granting; denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. ICE may, as it deems appropriate, authorize and make a favorable expedited pre-employment determination based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment determination or a full employment determination 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 or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment determination or full employment determination by the OPR-PSU. Contract employees are processed under the ICE Management Directive 6-8.0. The contractor shall comply with the pre-screening requirements specified in the DHS Special Security Requirement – Contractor Pre-Screening paragraph located in this contract, if HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology (IT) Resources; and/or 3052.204-71, Contractor Employee Access are included in the Clause section of this contract.

**BACKGROUND INVESTIGATIONS**

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, 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 the Personnel Security Unit. Prospective Contractor employees, whether a replacement, addition, subcontractor employee, or vendor employee, shall submit the following security vetting documentation to OPR-PSU, in coordination with the Contracting Officer Representative (COR), within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1. Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by applicant in their OPM e-QIP account.

2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by applicant in their OPM e-QIP account.

3. Two (2) SF 87 (Rev. March 2013) Fingerprint Cards. **(Two Original Cards sent via COR to OPR-PSU)**

4. Foreign National Relatives or Associates Statement. **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant's OPM e-QIP account prior to electronic "Release" of**

**data via on-line account)**

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant's OPM e-QIP account prior to electronic "Release" of data via on-line account)**

6. Optional Form 306 Declaration for Federal Employment **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant's OPM e-QIP account prior to electronic "Release" of data via on-line account)**

**7.** Two additional documents may be applicable if applicant was born abroad and/or if work is in a Detention Environment. If applicable, additional form(s) and instructions will be provided to applicant.

Prospective Contractor employees who currently have an adequate, current investigation and security clearance issued by the Department of Defense Central Adjudications Facility (DoD CAF) or by another Federal Agency may not be required to submit a complete security packet. Information on record will be reviewed and considered for use under Contractor Fitness Reciprocity if applicable.

An adequate and current investigation is one where the investigation is not more than five years old, meets the contract risk level requirement, and applicant has not had a break in service of more than two years.

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

To ensure adequate background investigative coverage, contract support applicants must reside in the United States or its Territories. Additionally, applicants are required to have resided within the Unites States or its Territories for three or more years out of the last five (ICE retains the right to deem an applicant ineligible due to insufficient background coverage). This time-line is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Applicants 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.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

**TRANSFERS FROM OTHER DHS CONTRACTS:**

Personnel may transfer from other DHS Contracts provided they have an adequate and current investigation (see above). If the prospective employee does not have an adequate and current investigation a DHS 11000-25 with ICE supplemental page will be submitted to PSU to initiate a new investigation.

Transfers will be accomplished by submitting a DHS 11000-25 with ICE supplemental page indicating "Contract Change."

**CONTINUED ELIGIBILITY**

If a prospective employee is found to be ineligible for access to Government facilities or information, the COR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU will conduct reinvestigations every 5 years, or when derogatory information is received, to evaluate continued eligibility.

ICE reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

**REQUIRED REPORTING:**

The Contractor will notify OPR-PSU, via the COR, of terminations/resignations of contract employees under the contract within five days of occurrence. The Contractor will return any 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.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, via the COR, a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation) . 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.

CORs will submit reports to psu-industrial-security@ice.dhs.gov

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 NDA for contractor access to sensitive information. The NDA will be administered by the COR to the 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 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.

**EMPLOYMENT ELIGIBILITY**

The contractor will agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility Verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represents the best means currently available for employers to verify the work authorization of their employees.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

**SECURITY MANAGEMENT**

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU 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 the OPR-PSU 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 in order to effect compliance with such requirements.

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former

Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

**INFORMATION TECHNOLOGY**

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor 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 IT Security Program Publication DHS MD 4300.Pub. or its replacement.* Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not 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 Chief Information Office 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, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractors, 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 PALMS or by contacting ICE.ADSEC@ICE.dhs.gov. Department contractors, 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. Supervisors 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).

(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.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. 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 also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the 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.

### 14.4.11 Non-Disclosure Agreement

Contractors are required to sign DHS 11000-6, Attachment 9 - Non-Disclosure Agreement, due to access to a sensitive ICE system. Non-Disclosure Agreements shall be provided to the COR and CO prior to the commencement of work on this task order.

## 15. Additional Privacy Clauses

**PRIV 1.4: Separation Checklist for Contractor Employees:** Contractors shall enact a protocol to use a separation checklist before its employees, Subcontractor employees, or independent Contractors terminate working on the contract. The separation checklist must cover areas such as: (1) return of any Government-furnished equipment; (2) return or proper disposal of Sensitive PII (paper or electronic) in the custody of the Contractor/Subcontractor employee or independent Contractor, 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 performing work related to this contract, Subcontractor employee, or independent Contractor, the Contractor shall notify the Contract 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.

**PRIV 1.7: Privacy Act Information:** In accordance with FAR 52.224-1, PRIVACY ACT NOTIFICATION (APR 1984), and FAR 52.224-2, PRIVACY ACT (APR 1984), this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974. The Agency advises that the relevant system of records notices (SORNs) applicable to this Privacy Act information are as follows:

- All ICE SORNS
- DHS/CBP006 - Automated Targeting System
- DHS/CBP011 - U.S. Customs and Border Protection TECS
- DHS/CBP013 - Seized Assets and Case Tracking System
- DHS/CBP017- Analytical Framework for Intelligence (AFI) System of Records
- DHS/NPPD004 - DHS Automated Biometric Identification System (IDENT)
- DHS-USCIS007 - Benefits Information System
- DHS/USVISIT001- Arrival and Departure Information System (ADIS)
- FBI/001 - National Crime Information Center (NCIC)

These SORNs may be updated at any time. The most current DHS versions are publicly available at www.dhs.gov/privacy. SORNs of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System of the Government Publishing Office, available at http://www.gpo.gov/fdsys/.

**PRIV 2.1: Restrictions on Testing Using Real Data Containing PII:** Except as required to fulfill contract requirements, the use of real data containing Sensitive PII, from any source, for testing purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing whenever feasible. ICE policy requires that any proposal to use real data or de-identified data for IT system testing be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system testing purposes, the Contractor in coordination with the CO or COR and government program manager shall obtain approval from OCIO and the ICE Privacy Office and complete any required documentation. Within 90 days of the execution of Option Year 2, the Contractor will submit Proposal to Use Real Data for Testing questionnaire(s) to the ICE Privacy Officer and CISO for any currently occurring testing using real data. Once the ICE Privacy Officer and CISO have reviewed and provided feedback, the Contractor will promptly correct any identified security and privacy deficiencies.

**PRIV 2.2: Restrictions on Training Using Real Data Containing PII:** Except as required to fulfill contract requirements, the use of real data containing Sensitive PII, from any source, for training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for training whenever feasible. ICE policy requires that any proposal to use real data or de-

identified data for IT system training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for training purposes, the Contractor in coordination with the CO or COR and government program manager shall obtain approval from OCIO and the ICE Privacy Office and complete any required documentation. Within 90 days of the execution of Option Year 2, the Contractor will provide the ICE Privacy Officer and CISO with a summary of how real data is currently being used for training. This summary will describe the environment in which training occurs, the positions of the recipients of the training, and the security and privacy measures taken to ensure real data is protected throughout the training process. Once the ICE Privacy Officer and CISO have reviewed and provided feedback, the Contractor will promptly correct any security and privacy deficiencies.

**PRIV 2.5: Requirement for Privacy Lead:** The Contractor shall identify a Contractor employee to serve as Privacy Lead. 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 Office, the Office of the Chief Information Officer, and the Records Management Branch 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 Office 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.

**REC: 1.1: Required DHS Basic Records Management Training:** The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to Sensitive PII as well as the creation, use, dissemination and/or destruction of Sensitive PII at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site. The Agency may also make the training available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance. The Contractor must submit an annual e-mail notification to the Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

**REC 1.2: Deliverables are the Property of the U.S. Government:** Except as stated in the Performance Work Statement, Terms and Conditions (Sections B-J), and the Contractor's

Commercial License Agreement, the Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable without the express permission of the Contracting Officer or Contracting Officer's representative. The Government Agency owns the rights to all data/records produced as part of this contract.

**REC 1.3: Contractor Shall Not Create or Maintain Unauthorized Records:** The Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records. The Contractor shall not create or maintain any records containing any Government Agency data that are not specifically tied to or authorized by the contract.

**REC 1.4: Agency Owns Rights to Electronic Information:** Except as stated in the Performance Work Statement, Terms and Conditions (Sections B-J), and 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 created as part of this contract. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

**REC 1.5: Comply With All Records Management Policies:** The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

**REC 1.6: No Disposition of Documents without Prior Written Consent:** No disposition of documents related to this contract will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

**REC 1.7: Contractor Obtain Approval Prior to Engaging Sub-Contractor Support:** 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.
(End of clause)

## 16.0 LIST OF ACRONYMS

The list of acronyms in connection to this PWS is attached as Appendix A.

## 17.0 PALANTIR TECHNOLOGIES LICENSING AGREEMENT & TERMS AND CONDITIONS

Palantir's License and Services Agreement and Palantir's Operations & Management/Support Services Terms and Conditions are attached as Appendix B.

## PWS Appendix A: List of Acronyms

| | |
|---|---|
| AHS | Application Hosting Services |
| ADIS | Arrival and Departure Information System |
| AIDW | Automated Information Data Warehouse |
| AJAX | Asynchronous Java and XML |
| API | Application Programming Interface |
| ATS | Automated Targeting System |
| C&A | Certification and Accreditation |
| CCB | Change Control Board |
| CCDI | Consular Consolidated Database |
| CFR | Code of Federal Regulation |
| CLAIMS | Computer Linked Application Information Management System |
| CO | Contracting Officer |
| COB | Close of Business |
| COR | Contracting Officer's Representative |
| COTR | Contracting Officer's Technical Representative (same as COR) |
| COTS | Commercial Off-The-Shelf |
| CPIC | Capital Planning and Investment Control |
| CPU | Central Processing Units |
| CSIRC | Computer Security Incident Response Center |
| CSRC | Computer Security Resource Center |
| DARTTS | Data Analysis and Research for Trade Transparency System |
| DC | District of Columbia |
| DCID | Director of Central Intelligence Directive |
| DHS | Department of Homeland Security |
| DISCO | Defense Industrial Security Clearance Office |
| DoJ | Department of Justice |
| E3 | Next Generation of ENFORCE |
| EA | Enterprise Architecture |
| EADM | Enforcement Alien Detention Module |
| EARM | Enforcement Alien Removal Module |
| EID | Enforcement Integrated Database |
| EIT | Electronic and Information Technology |
| EIU | Executive Information Unit |
| ELMS | Electronic Library Management System |
| ENFORCE | Enforcement Case Tracking System |
| EOD | Entry on Duty |

| | |
|---|---|
| ETL | Extract, Transfer and Load |
| E-VERIFY | Eligibility Verification |
| FAR | Federal Acquisition Regulations |
| FINS | Former Immigration Naturalization Service |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| FITSAF | Federal Information Technology Security Assessment Framework |
| FRD | Functional Requirements Document |
| FTR | Federal Travel Regulations |
| GFE | Government Furnished Equipment |
| GFI | Government Furnished Information |
| GFP | Government Furnished Property |
| GNR | Global Name Recognition |
| GOTS | Government Off-The-Shelf |
| GWA | Greater Washington, DC Area |
| HSI | Homeland Security Investigations |
| HSTC | Human Smuggling and Trafficking Center |
| I2MS | Investigative Information Management System |
| IBM | International Business Machines |
| ICE | Immigration and Customs Enforcement |
| ICEPIC | ICE Pattern Analysis Information Collection Tool |
| ICE/SAC | ICE Special Agent in Charge |
| ICM | Investigative Case Management (New TECS) |
| ID | Identification Card |
| IPT | Integrated Project Team |
| IRRIS | Investigation Records Review for Information Sharing |
| ISA | Interconnection Security Agreements |
| ISB | Investigative Systems Branch |
| ISC2 | International Info Systems Security Certification Consortium |
| ISSM | Information Systems Security Manager |
| ISSO | Information Systems Security Officer |
| IRS | Intelligence Research Specialist |
| IT | Information Technology |
| ITCR | Information Technology Change Request |
| KITE | Palantir Data Ingestion |
| LECAD | Law Enforcement Centralized Access Development |
| LEISS | Law Enforcement Information Sharing System |
| LESC | Law Enforcement Support Center |

| | |
|---|---|
| LPR | Lawful Permanent Residents |
| MCC | Mobile Command Center |
| MD | Management Directive |
| MS | Microsoft |
| NCIC | National Crime Information Center |
| NISPOM | National Industrial Security Program Operating Manual |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NSEERs | National Security Entry and Exit Registration System |
| O&M | Operations and Maintenance |
| OAST | Office on Accessible Systems and Technology |
| OCIO | Office of the Chief Information Officer |
| OCONUS | Outside of the Continental United States |
| ODC | Other Direct Cost |
| OI | Office of Investigations |
| OIT | Office of Information and Technology |
| OMB | Office of Management and Budget |
| OPR | Office of Professional Responsibility |
| PCN | Potomac Center North |
| PCTS | Parole Case Tracking System |
| PHOENIX | Palantir Big Data Platform |
| PM | Program Manager |
| PMO | Program Management Office |
| PMP | Project Management Professional |
| POP | Period of Performance |
| PSU | Personnel Security Unit |
| QAP | Quality Assurance Plan |
| QASP | Quality Assurance Surveillance Plan |
| QCP | Quality Control Plan |
| RAPTOR | Palantir Data Index Tool |
| RELRES | Relationship Resolution |
| RFD | Request for Deviation |
| ROI | Records of Investigation |
| SBU | Sensitive But Unclassified |
| SCI | Sensitive Compartmented Information |
| SCR | System Change Request |
| SDA | System Design Alternative |
| SDD | Systems Development Division |

| | |
|---|---|
| SEACATS | Seized Asset and Case Tracking System |
| SELC | System Enterprise Lifecycle |
| SEN | Significant Event Notification |
| SEVIS | Student Exchange Visitor Information System |
| SLA | Service Level Agreement |
| SLM | System Lifecycle Management |
| SOP | Standard Operating Procedure |
| SOW | Statement of Work |
| SRD | System Requirements Document |
| SW | Software |
| TAIS | Telecommunications and Automated Information Systems |
| TLS | Telephone Linking System |
| TMP | Transition Management Plan |
| TO | Task Order |
| TRM | Technical Reference Model |
| TS | Top Secret |
| TTU | Trade Transparency Unit |
| UAT | User Acceptance Testing |
| USCIS | United States Citizenship and Immigration Services |
| US-VISIT | United States Visitor and Immigrant Status Indicator Technology |
| VPN | Virtual Private Network |