STATEMENT OF WORK
For
Immigration and Customs Enforcement (ICE)
Homeland Security Investigations (HSI)
Gang Intelligence Application
March 26, 2020

1.0 PURPOSE

This Statement of Work (SOW) is to procure software development, data analytic support, and cloud migration of a web-based application for use by Homeland Security Investigations (HSI) to identify, track, disrupt and dismantle Transnational Gangs in Virginia, West Virginia and Washington D.C. area of operations. The affected system will directly support HSI's mission to target Transnational Criminal Organizations in support of Executive Order (EO) 13773.

2.0 BACKGROUND

The Lehigh County, Pennsylvania's Regional Intelligence and Investigative Center (RIIC) originally developed the Gang Intelligence Application (GIA), a database repository of regional gang members and associated information, as a way for federal, State, and local law enforcement partners including ICE to collaborate and share data. HSI Washington DC uses the GIA to combat transnational gangs in and around the National Capitol Region, but HSI's use of the GIA is limited by the scope of information that ICE can securely upload, share, and control within the GIA.

HSI, in-part through the HSI Innovation Lab, is streamlining, modernizing, and enhancing HSI's investigative capabilities. In support of this effort, HSI requires expanded capability and information sharing from the GIA, including Cloud-based access, enhanced data-sharing security, and advanced data-analytics capabilities. This SOW defines the services and deliverables required to meet HSI's need.

The GIA supports HSI's Targeting efforts of Transnational Gangs by:

- Increasing intelligence gathering in the region which will foster greater communications
- Documenting known & suspected gang members
- Providing investigative leads
- Creating a singular, secure method for quickly accessing and disseminating gang related information to regional-based law enforcement partners
- Providing the ability to query multiple agencies' data sets to provide an accurate assessment and identification of transnational gang trends and patterns
- Providing the ability to search for people, vehicles, weapons, property, and phone numbers across police and prison records to target criminal organizations

3.0 SCOPE

The GIA houses a large regional dataset, including segmented HSI-specific data that is available to an assortment of approved law enforcement users. ICE requires greater control over its data than is currently provided by the GIA, facial recognition analysis of HSI queries and data, and additional security measures that will enable the GIA to interface directly with ICE systems. In order to meet these requirements, ICE requires architectural modification of the GIA including migration to the GovCloud environment to enable secure

integration of HSI gang specific data into a secure ICE compartmentalized tool, increased analytical and data support, and facilitation of secure sharing and future interfacing with ICE systems to further its mission to target transnational criminal organizations.

4.0 TASKS

The tasks required under this Statement of Work are as follows:

1. **Provide Access Control for HSI Users:** The Contractor shall develop access control for a compartmentalized HSI specific data and investigative tool set. The access control measures must permit HSI to maintain administrative control over who can access HSI's compartmentalized portion of the system.

2. **Data analyst resource support**: The Contractor shall provide analyst support to develop and integrate HSI specific data into the ICE-specific portion of the GIA.

    - The Contractor shall integrate intelligence information to disclose patterns, trends or evidence of gang activity; make recommendations and provide guidance and support to HSI users of the system;
    - The Contractor will familiarize ICE/HSI on the compartmentalized tool.
    - The Contractor shall develop an analytical capability to collect, collate, analyze and disseminate information concerning gang activity and/or gang investigations and curate the information stored on gang, clique, and member profile pages in the system such as but not limited to: social media, videos, audio files, documents, photos, facial recognition templates.

3. **Data Management:** The Contractor shall develop a data management capability for the HSI compartmentalized data to ensure data quality. The application shall ensure that HSI's data is retained on three-year and five-year cycles to be compliant with both the state and federal regulations. The Contractor shall develop a dashboard overview of gang populations based on geography (county, state, region, or nation) as well as profiles on individual gangs, gang sets and gang members. Information tracked in this system includes personal identifiers, artifacts such as videos, documents, images, social media information, associates, weapons, locations, and vehicles. The Contractor shall develop graphing algorithms and data visualization techniques in the application to help show the complex relationships that exist between gang members, affiliates, criminal justice personnel, as well as links to locations of interest, vehicles, weapons, and events such as arrests, incarcerations and police incidents.

4. **AWS GovCloud migration:** The Contractor will migrate the GIA to the GovCloud environment to enable future integration and development of geospatial intelligence and tracking capabilities in concert with the HSI Innovation lab.

5. **Integrate the Nobilis Horus Facial Recognition:** The Contractor shall incorporate NOBLIS Horus facial recognition technology to enable application to the ICE-specific portion of the application in order to allow gang members themselves and relationships among gang members to be more easily identified by ICE. The Contractor shall provide an Application Program Interface (API) of the Horus facial recognition system. The API shall allow the facial recognition system to consume all images uploaded into the system and shall provide a facial template for each image stored within the GIA for retrieval. In addition, the Contractor shall develop system-level configuration and managed roles and responsibilities of HSI and external law enforcement partners.

6. **Security:** The Contractor shall ensure that the system complies with security services and features and FedRamp controls as detailed in the Criminal Justice Information System (CJIS) Security Policy Requirements document. The Contractor shall ensure that the system complies with the following:

- *Activity logging*. The Contractor shall ensure that the system logs the following events:
  - Successful and unsuccessful system log-on attempts.
  - Successful and unsuccessful attempts to change account passwords.
  - Successful and unsuccessful attempts to change user permissions.
  - Successful and unsuccessful actions by an authenticated user.
  - Any updates, inserts, or deletes to any record in the system
- *Data Encryption*. The Contractor shall ensure that all data transited between system servers and user machines is encrypted and that all data in transit and at rest is encrypted.
  - Encryption of stored data (at rest) will meet the Federal Information Processing Standards (FIPS) 140-2 standard.
  - All management access and authentication shall occur via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Encryption shall be a minimum of 128 bits.
- Ensure that the repository integrates appropriate security rules and permissions. Ensure that the repository uses 2-Factor Authentication;
- *Comprehensive key management and protection.*
  - The Contractor shall ensure that a certificate policy and certification practice is documented and implemented for the issuance of public key certificates used in the system.
- *Integrated permission management and multi-factor authentication.*
  - Where technically feasible, the system shall enforce a limit of no more than five consecutive invalid access attempts by a user. The system shall automatically lock the account/node for a 20-minute time period unless released by an administrator.
  - The system shall use a layered authentication scheme; in addition to providing a username and password, the system requires the user to provide a system-generated PIN (that is emailed to the user's approved email account after the user's credentials are verified).
- *Intelligent threat detection and data loss prevention.*
  - The Contractor shall ensure that intrusion detection systems are deployed to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and shall make notifications of any event that violates any of those parameters.
- *Compliance Assessment*
  - The Contractor shall ensure that audit mechanisms and tools are implemented to ensure organizational practices are followed throughout the system lifecycle. Further documentation on the use of these mechanisms and tools will be provided prior to production deployment.

5.0 DELIVERABLES

Deliverables	Frequency
AWS Cloud Migration	Completed no later than12 months after contract award. Status reports shall be delivered quarterly.
Integration of the Noblis Facial Recognition	Completed no later than 12 Months after contract award.
Invoice Submittal to Burlington Finance Center & HSI COR/Program Manager	Monthly, within 30 days of invoice period of performance.

This schedule can be modified or changed only by written approval from the Contracting Officer.

5.1 ACCEPTANCE CRITERIA

HSI will accept or reject deliverables within fifteen (15) business days after delivery. If rejected, the Contractor shall make corrections as specified and resubmit the deliverable for review and approval within five (5) business days provided however that contractor is not dependent upon a third party for performance. If the government does not reply within the specific timeframe than the deliverable shall be determined acceptable.

6.0 PERIOD OF PERFORMANCE

The Period of Performance shall be 12 months from the date of award.

7.0 PLACE OF PERFORMANCE

All performance will occur at the Contractor's facility.

8.0 GOVERNMENT FURNISHED PROPERTY (GFP)

There will be no Government Furnished Equipment or Property associated with the performance of this requirement.

9.0 TRAVEL

Contractor travel is not required for this requirement. Local meetings or activities planned outside of the defined place of performance are permitted, but all expenses incurred are the responsibility of the contractor.

10.0 ACCESS TO GOVERNMENT PROPERTY AND FACILITIES

As determined by ICE, the Contractor may be allowed limited access to ICE facility(s) for meetings and will be escorted by appropriate government personnel in accordance with ICE policy. ICE will arrange access to ICE data/systems as required to perform this requirement.

11.0 BUSINESS RELATIONS

The Contractor shall successfully integrate and coordinate all activity needed to execute the requirement. The Contractor shall effectively manage all staff, provide corrective action plans & identify issues timely. The Contractor shall seek to ensure customer satisfaction and professional and ethical behavior of all contractor personnel. The Contractor shall maintain the currency of their employees by providing initial and refresher systems training (as needed) to meet the SOW requirements. The Contractor shall be responsible for all management, supervision, transportation, training, and equipment for their employees unless identified otherwise within this SOW as being government furnished. The Contractor shall provide all necessary administrative support to its employees in a timely fashion (timekeeping, leave processing, pay, and emergency needs).

APPENDIX A. GENERAL CYBERSECURITY REQUIREMENTS

A.1 In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.

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

A.2 In accordance with ITAR 4.5.3.4 and ITAR 4.5.4.4 – Security Review

Security Review Terms and Conditions

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer 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 ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

A.3 In accordance with ITAR 4.5.3.7 – Supply Chain Risk Management

Supply Chain Risk Management Terms and Conditions

The Contractors supplying the Government hardware and software shall provide the manufacturer'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:

(i) How risks from the supply chain will be identified;

(ii) What processes and security measures will be adopted to manage these risks to the system or system components; and

(iii) 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 Representative (COR/CO) 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 a risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standard certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the CO. Contractors shall provide only Original Equipment Manufacturer (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 source and have them 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 U.S. 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 of 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 shipping 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 ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

A.4 In accordance with HSAR 3052.204-70 - Security requirements for unclassified IT resources, with ITAR 4.5.3.3 – Access to Unclassified Facilities, IT Resources, and Sensitive Information Requirement Clause Inclusion Instruction, with ITAR 4.5.3.9 – Security Requirements for Unclassified Information Technology Resources Clause, with ITAR 4.5.4.6 – Required Protections for DHS Systems Hosted in Non-DHS Data Centers, and with ITAR 4.5.4.7 – Contractor Employee Access Clause . As prescribed in (HSAR) 48 CFR 3004.470-3 **Contract clauses:**

Security Requirements For Unclassified Information Technology Resources (JUN 2006)

The Contractor shall be responsible for 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.

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.

Within 30 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 (CO), shall be incorporated into the contract as a compliance document.

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 FISMA of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

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.

Examples of tasks that require security provisions include:

a) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

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

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.

A.4.1 Contractor IT Security Accreditation

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the CO 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 CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

A.5 In accordance with HSAR 3052.204-71 - Contractor Employee Access

Contractor Employee Access (Sep 2012)

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

This definition includes the following categories of information:

a) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

b) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

c) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

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

e) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

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

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

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

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

A.6 In accordance with ITAR 4.5.3.10 – Contractor Employee Access Clause (use language from HSAR 3052.204-70 and alternates at 3052.204-71).

A.6.1 Alternate II

Sensitive Information Limited to U.S. Citizens and Lawful Permanent Residents (JUN 2006)

1) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.
2) 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

A.7 In accordance with White House Digital Government BYODTK – Privacy Expectations

Privacy Expectations

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

A.8 In accordance with HSAR Class Deviation 15-01, Special Clause, Safeguarding of Sensitive Information (MAR 2015)

Safeguarding of Sensitive Information (MAR 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.

(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.

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*.

A.9 In accordance with HSAR Class Deviation 15-01, Special Clause, Information Technology Security and Privacy Training (MAR 2015)

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.

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.

APPENDIX B. CLOUD SERVICES CONTRACT REQUIREMENTS

B.1 In accordance with ITAR 4.5.3.2 – Encryption Compliance

Encryption Compliance Terms and Conditions

If encryption is required, the following methods are acceptable for encrypting sensitive information:

a) FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.

b) National Security Agency (NSA) Type 2 or Type 1 encryption.

c) 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*).

B.2 In accordance with ITAR 4.5.3.5 and ITAR 4.5.4.5 – Interconnection Security Agreement (ISA)

ISA Terms and Conditions

Interconnections between DHS/ICE and non-DHS/ICE IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnection security agreements.

B.3 In accordance with ITAR 4.5.3.6 and ITAR 4.5.4.6 – Required Protections for DHS/ICE Systems Hosted in Non-DHS/ICE Data Centers

1) Security Authorization Terms and Conditions

A Security Authorization of any infrastructure directly in support of DHS/ICE information system shall be performed as a general support system (GSS) prior to DHS/ICE 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 (SA) shall be performed in accordance with DHS/ICE Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of DHS/ICE information system.

At the beginning of the contract, and upon request thereafter (generally at the deployment of a new system or renewal of a System Authority to Operate), the contractor/Cloud Service Provider (CSP) 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/ICE applies in the SA process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into DHS/ICE POA&M Management Process. ICE shall use 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 DHS/ICE POA&M Management

Process. CSP procedures shall be subject to periodic, unannounced assessments by DHS/ICE officials. The documented physical aspects associated with CSP activities shall also be subject to such assessments. Inspections of CSP physical facilities will be scheduled in advance and coordinated with the provider in accordance with their facility procedures.On a periodic basis, DHS and its Components, including DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but is 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 CSP and reseller shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS/ICE information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS/ICE, 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/ICE in the event of a security incident.

2) *Enterprise Security Architecture Terms and Conditions*

The CSP shall utilize and adhere to DHS/ICE Enterprise Security Architecture in accordance with applicable laws and DHS/ICE policies to the satisfaction of DHS/ICE COR.

3) *Continuous Monitoring Terms and Conditions*

The CSP shall participate in the DHS/ICE Continuous Monitoring methodologies and, shall provide a Continuous Monitoring capability over their resources as required by FedRAMP. 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 CSP shall adhere to all ITAR and FedRAMP continuous monitoring requirements and ensure that DHS/ICE can implement and integrate the following processes:

a) Asset Management
b) Vulnerability Management
c) Configuration Management
d) Malware Management
e) Log Integration
f) Security Information Event Management (SIEM) Integration
g) Patch Management
h) Providing near-real-time security status information to DHS/ICE SOC Specific Protections Terms and Conditions
i) Specific protections that shall be provided by the CSP include, but are not limited to the following:

Specific Operations Terms and Conditions

The Contractor shall operate a SOC to provide security for the below mentioned services. The CSP shall support regular reviews with DHS/ICE Information Security Office to coordinate and synchronize the security posture of the CSP hosting facility with that of DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The CSP 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 CSP staff shall also maintain a trouble

ticket system in which incidents and outages are recorded. In the event of an incident, the CSP facility SOC shall adhere to the incident response plan.

4) *Computer Incident Response Services Terms and Conditions*

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

5) *Network Intrusion Detection Systems (NIDS) and Monitoring Terms and Conditions*

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 for their facility(s). 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 made available to DHS/ICE upon request. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

6) *Physical and Information Security and Monitoring Terms and Conditions*

The CSP shall provide a facility using appropriate protective measures to provide for physical security. All facilities will be located within the United States. The CSP shall maintain a process to control physical access to all DHS/ICE IT assets. DHS/ICE IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS/ICE security office upon request.

7) *Vulnerability Assessments Terms and Conditions*

The CSP and reseller shall provide all information from any managed device to DHS/ICE, 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.

8) *Anti-malware (e.g., virus, spam) Terms and Conditions*

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

9) *Log Retention Terms and Conditions*

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

B.4 In accordance with ITAR 4.5.3.8 – Personal Identification Verification (PIV) Credential Compliance

Personal Identification Verification (PIV) Credential Compliance Terms and Conditions

a) 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.

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

c) 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.

d) 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.

B.5 In accordance with ITAR 4.5.4.2 – Encryption Compliance

The following requirement should be incorporated into acquisition documents for ***CLASSIFIED REQUESTS****:*

Encryption Compliance Terms and Conditions

National Security Systems, requiring encryption shall comply with the following standards:

a) Products using FIPS 197 AES algorithms with at least 256 bit encryption that has been validated under FIPS 140-2 (**Note:** The use of triple DES [3DES] and FIPS 140-1 is no longer permitted. A waiver or exception is required for systems where AES cannot currently be used.)

b) NSA Type 2 or Type 1 encryption

B.6 In accordance with FedRAMP

Note: *The following requirements/clauses apply to both* ***SBU and CLASSIFIED REQUESTS****.*

1) FedRAMP IT Systems Security Requirements

a) The Federal agency will determine the security category for the cloud system in accordance with Federal Information Processing Standard 199; then, the contractor/Cloud Service Provider (CSP) shall apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance to security standards. The FedRAMP baseline controls are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

b) The CSP shall maintain a security management continuous monitoring environment that meets or exceeds the requirements outlined in the latest edition of FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

2) FedRAMP Privacy Requirements

Contractor shall be responsible for the following privacy and security safeguards:

a) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

b) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

c) The contractor shall also comply with any additional FedRAMP privacy requirements.

d) The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, contractor shall be responsible for the following privacy and security safeguards:

(i) The Contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception—Disclosure to a Consumer Agency for purposes of C&A verification.

(ii) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include, but is not limited to: Authenticated and unauthenticated operating system/network vulnerability scans Authenticated and unauthenticated we b application vulnerability scans Authenticated and unauthenticated database application vulnerability scans Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

(iii) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(iv) If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

3) Sensitive Information Storage

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorize personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

4) Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed because of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as SBU information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The government will retain unrestricted rights to government data. The government retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The government-owned data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

5) Security Classification

The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level unless a higher level is specified.

6) Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government, and must be submitted to the COTR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-14 Rights in Data-General.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the CO.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

7) Disclosure of Information

Any information made available to the Contractor by the Government shall be used only for carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

8) FedRAMP Security Requirements Overview:

a) The minimum requirements for low and moderate impact cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

b) The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.

c) FedRAMP requires cloud service providers to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.

d) The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

e) Federal agencies will be able to leverage the provisional Authorization granted by FedRAMP and any documentation prepared by the contractor to issue their own authority to operate.

f) The vendor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://FedRAMP.gov.

9) FedRAMP Security Compliance Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP baseline controls are based on NIST SP 800-53, Revision 4. The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

10) Required FedRAMP Policies and Regulations

The contractor shall comply with FedRAMP Security Assessment Framework – describing a general security Assessment Framework for the Federal Risk and Authorization Management Program (FedRAMP). This document details the security assessment process which must be used to achieve FedRAMP compliance. Download here:

https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

11) Assessment and Authorization

DHS/ICE ICE may choose to cancel the contract/award and terminate any outstanding orders if the contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

12) Assessment of the System

a) The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at http://FedRAMP.gov :

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)
- IT System Contingency Plan (CP)
- IT System Contingency Plan (CP) Test Results
- POA&M Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements.

b) Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

c) The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements (https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf). Review activities include but are not limited to scanning operating systems, web

applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

d) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a POA&M document. Depending on the severity of the gaps, the Government may require them to be remediated before a provisional authorization is issued.

e) The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

REQUIRED SECURITY LANGUAGE FOR SENSITIVE /BUT UNCLASSIFED (SBU) CONTRACTS

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 FITNESS 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 Fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination 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 preliminary Fitness determination or final Fitness determination by OPR-PSU. Contract employees are processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or successor thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. (Sexual Abuse and Assault Prevention Standards) implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003)

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Contractor employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR-PSU, through 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 the contractor employee 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 the contractor employee in their OPM e-QIP account.

3. Two (2) SF 87 (Rev. December 2017) 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 contractor employee from OPR-PSU – must be signed and archived into contractor employee'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 contractor employee from OPR-PSU – must be signed and archived into contractor employee'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 contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

7. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

8. One additional document may be applicable if contractor employee was born abroad. If applicable, additional form and instructions will be provided to contractor employee. (If applicable, the document will be sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under reciprocity. The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

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. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01)

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 by the COR.

To ensure adequate background investigative coverage, contractor employees must currently reside in the United States or its Territories. Additionally, contractor employees 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 a contractor employee 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. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving

in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. Citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007-001. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007-001.

TRANSFERS FROM OTHER DHS CONTRACTS:

Contractor employees may be eligible for transfer from other DHS Component contracts provided they have an adequate and current investigation meeting the new assignment requirement. If the contractor employee does not meet the new assignment requirement a DHS 11000-25 with ICE supplemental page will be submitted to OPR-PSU to initiate a new investigation.

Transfers will be accomplished by submitting a DHS 11000-25 with ICE supplemental page indicating "Contract Change." The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

CONTINUED ELIGIBILITY

ICE reserves the right and prerogative to deny and/or restrict facility and information access of any contractor employee whose actions conflict with Fitness standards contained in DHS Instruction 121-01-007-01, Chapter 3, paragraph 6.B or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a contractor employee from contract support. The OPR-PSU will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued Fitness of contractor employees.

REQUIRED REPORTS

The Contractor will notify OPR-PSU, via the COR, of all terminations/resignations of contractor employees under the contract within five days of occurrence. The Contractor will return any expired ICE issued identification cards and building passes of terminated/ resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contractor 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 contractor employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of contractor employees 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 as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information* and ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information*."

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

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with 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.

INFORMATION TECHNOLOGY SECURITY CLEARANCE

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 MD 4300.1, *Information Technology Systems Security*. or its replacement. Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, 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.

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

training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

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

13) Authorization of System

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

14) Reporting and Continuous Monitoring

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

All deliverables shall be labeled "Law Enforcement Sensitive/Sensitive But Unclassified." External transmission/dissemination of "Law Enforcement Sensitive/Sensitive But Unclassified," to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."

15) Non-Repudiation

The Cloud Service Provider vendor shall provide a system that is capable of implementing NIST SP 800-53 Control AU-10 approved controls, which provides for origin authentication, data integrity, and signer non-repudiation. This binds the identity of the information producer with the information to and provides the means for authorized individuals to determine the identity of the producer of the information.

16) Identification and Authentication (Organizational Users)

The vendor shall support a secure, multi-factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.

The vendor shall support multi-factor authentication including Users are required to pass a two-factor authentication process. First, the user must provide a username and password (only the

password hash is stored). If the provided credentials are valid, the system will send an email containing a 4-character code to a pre-approved government email address. The user must then enter this code in the system to be granted access. Once a user is authenticated, the system will restrict what the user can see and interact with based on their authorization level.

Identification and Authentication (Non-Organizational Users)

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Vendor Administrators that will allow vendor-designated personnel the ability to perform management duties on the system.

17) Incident Reporting Timeframes

Cloud Service Providers are required to report all computer security incidents to the United States Computer Emergency Readiness Team (U.S.-CERT) in accordance with U.S.-CERT "Incident Categories and Reporting Timeframes" in , Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to U.S.-CERT within 1 hour of detection regardless of the incident category reporting timeframe.

18) Media Transport

The vendor shall document activities associated with the transport of Federal agency information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas.

Digital media, containing Federal agency information, that is transported outside of controlled areas must be encrypted using a Transport Layer Security 1.2+ (TLS/HTTPS); non-digital media including but not limited to CD-ROM, floppy disks, etc., must be secured using the same policies and procedures as paper.

On the AWS GovCloud:

In Transit

• All communication outside of controlled areas is encrypted over using Transport Layer Security 1.2+ (TLS/HTTPS). Internal communication (API and database calls) is encrypted as well.

At Rest

• All databases (relational and graph) logs, backups, and snapshots are encrypted using use the industry standard AES-256 encryption.

• All files stored using AWS S3 will use the industry standard AES-256 encryption.

Media, containing Federal Agency information that is transported outside of controlled areas must ensure accountability. This can be accomplished through Auditing of user events, (including searches, data modification, password changes, failed login attempts, etc.), are logged and available for audit and review.

Federal Agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard 12 drives, and SD cards) must be encrypted using industry standard AES-256 encryption (Note: the encryption algorithm is subject to change, but the minimum will be 256-bit encryption). All Federal Agency data residing on laptop computing devices must be protected with approved encryption software.

19) Boundary Protection

The CSP/Reseller shall route all external connections through a Trusted Internet Connection (TIC).

20) Protection of Information At Rest

The CSP shall provide security mechanisms for handling data at rest and in transit in accordance with FIPS 140-2.

21) Security Alerts, Advisories, and Directives

The CSP/Reseller shall provide a list of their personnel, identified by name and role, with system 1 administration, monitoring, and/or security responsibilities that are to receive security alerts, two advisories, and directives. This list shall include ICE SOC.