Section H: Special Contract Requirements

H.1 52.216-18 -- Ordering (Oct 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from date of award through expiration of the contract period of performance.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered “issued” when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of Clause)

H.2 52.216-19 -- Order Limitations (Oct 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $1.00, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor --

(1) Any order for a single item in excess of the contract period of performance ceiling price for the contract year in effect;

(2) Any order for a combination of items in excess of the contract period of performance ceiling price for the contract year in effect; or

(3) A series of orders from the same ordering office within 365 days that together call for quantities exceeding the limitation in subparagraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 5 days after issuance, with written notice stating the Contractor’s intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source. (End of Clause)
H.3  52.216-21 - Requirements (Oct 1995)

(a) This is a requirements contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies or services specified in the Schedule are estimates only and are not purchased by this contract. Except as this contract may otherwise provide, if the Government's requirements do not result in orders in the quantities described as “estimated” or “maximum” in the Schedule, that fact shall not constitute the basis for an equitable price adjustment.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. Subject to any limitations in the Order Limitations clause or elsewhere in this contract, the Contractor shall furnish to the Government all supplies or services specified in the Schedule and called for by orders issued in accordance with the Ordering clause. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(c) Except as this contract otherwise provides, the Government shall order from the Contractor all the supplies or services specified in the Schedule that are required to be purchased by the Government activity or activities specified in the Schedule.

(d) The Government is not required to purchase from the Contractor requirements in excess of any limit on total orders under this contract.

(e) If the Government urgently requires delivery of any quantity of an item before the earliest date that delivery may be specified under this contract, and if the Contractor will not accept an order providing for the accelerated delivery, the Government may acquire the urgently required goods or services from another source.

(f) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period, provided, that the Contractor shall not be required to make any deliveries under this contract after 05 November 2019. (End of Clause)

H.4  Procedure for Activation of Additional ISAP III Field Office/Sub-Office Locations

In accordance with Attachment 4 Location Overview of the Statement of Work (SOW), it is the Government's intent to expand its ISAP coverage to additional Enforcement and Removal Operations (ERO) Field Office and Sub-Office locations under the ISAP III contract through the establishment of new contractor facilities and assignment of contractor personnel working on-site at government facilities. The awardee shall be notified in writing of the Government's intent to open a new ISAP III Field Office or Sub-Office location(s). This authorization letter shall be signed by the ISAP III Contracting Officer and issued to the ISAP III Program Director and/or Deputy Program Director. It should be noted that the designated field office and/or sub-office location(s) may require “Contractor Site” or “Government Site” services. The awardee shall have no more than thirty (30) calendar days for “Government Site” locations and no more than sixty (60) calendar days for “Contractor Site” locations from receipt of the letter to commence ISAP III services and fulfill all SOW requirements at the specific field office and/or sub-office location(s) identified herein. The awardee must be prepared with sufficient staff and equipment to provide ISAP III services for

Source Selection Information - - See FAR 3.104
the full (i.e., maximum) number of anticipated ISAP III participant slots for that location. Each written authorization letter issued by the Government is not a task order, and therefore, shall not have any funding associated with it. All funding for ISAP III services shall be awarded against the resultant award on an annual basis via task orders. These annual task orders shall be incrementally funded, as needed, by CLIN and/or SLIN for the various levels of supervision and Electronic Monitoring (EM) Technology-Only services.

H.5 Security Requirements

H.5.1 GENERAL
The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in the solicitation, 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.

H.5.2 PRELIMINARY DETERMINATION
ICE will exercise full control over granting; denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. ICE may, as it deems appropriate, authorize and make a favorable expedited pre-employment determination based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment determination or a full employment determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment determination or full employment determination by the OPR-PSU. Contract employees are processed under the DHS Management Directive 6.8.0. The contractor shall comply with the pre-screening requirements specified in the DHS Special Security Requirement – Contractor Pre-Screening paragraph located in this contract, if HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology (IT) Resources; and/or 3052.204-71, Contractor Employee Access are included in the Clause section of this contract.

H.5.3 BACKGROUND INVESTIGATIONS
Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Prospective Contractor employees shall submit the following completed forms to the Personnel Security Unit through the Contracting Offices Representative (COR), no less than 35 days before the starting date of the contract or 5 days prior to the expected entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P “Questionnaire for Public Trust Positions” Form will be submitted via e-QIP (electronic Questionnaires for Investigation Processing) (Original and One Copy)
2. Three signed eQip Signature forms: Signature Page, Release of Information and Release of Medical Information (Originals and One Copy)

3. Two FD Form 258, “Fingerprint Card”

4. Foreign National Relatives or Associates Statement (Original and One Copy)

5. DHS 11000-9, “Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act” (Original and One Copy)

6. Optional Form 306 Declaration for Federal Employment (applies to contractors as well) Original and One Copy)

Prospective Contractor employees who currently have an adequate current investigation and security clearance issued by the Department of Defense Central Adjudications Facility (DoD CAF) or by another Federal Agency may not be required to submit complete security packages, and the investigation will be accepted for adjudication under reciprocity.

An adequate and current investigation is one where the investigation is not more than five years old and the subject has not had a break in service of more than two years.

Required forms will be provided by ICE at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

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

H.5.4 TRANSFERS FROM OTHER DHS CONTRACTS:

Personnel may transfer from other DHS Contracts provided they have an adequate and current investigation (see above). If the prospective employee does not have an adequate and current investigation an eQip Worksheet will be submitted to the Intake Team to initiate a new investigation.

Transfers will be submitted on the COR Transfer Form which will be provided by the Dallas PSU Office along with other forms and instructions.

H.5.5 CONTINUED ELIGIBILITY

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

Source Selection Information - See FAR 3.104

2022-ICLI-00039 504
The OPR-PSU may require drug screening for probable cause at any time and/or when the contractor independently identifies, circumstances where probable cause exists.

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

ICE reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

**H.5.6 REQUIRED REPORTS:**

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

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

The Contractor will provide, through the COR a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation). The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

Submit reports to the email address pice.dhs.gov

**H.5.7 EMPLOYMENT ELIGIBILITY**

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

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

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

Source Selection Information - See FAR 3.104

2022-ICLI-00039 505
Subject to existing law, regulations and/or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

H.5.8 SECURITY MANAGEMENT
The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

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

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

H.5.9 INFORMATION TECHNOLOGY
When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS IT Security Program Publication DHS MD 4300.Pub. or its replacement. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

H.5.10 INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT
All contractor employees using Department automated systems or processing Department sensitive data will be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

Contractors who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

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

H.6 PRIVACY REQUIREMENTS

H.6.1 Definitions

“Breach,” as used in this clause, means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic. “Breach” may be used interchangeably with “Privacy Incident.”

“Personally Identifiable Information (PII),” as used in this clause, means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.

Examples of PII include: 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), Internet protocol addresses, biometric identifiers (e.g., fingerprints), 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 Personally Identifiable Information (Sensitive PII),” as used in this clause, is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (e.g., fingerprint, voiceprint, iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual’s name or other unique identifier plus one or more of the following elements:

1. Driver’s license number, passport number, or truncated SSN (such as last 4 digits)
2. Date of birth (month, day, and year)
3. Citizenship or immigration status
4. Financial information such as account numbers or Electronic Funds Transfer Information
5. Medical Information
6. System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable Information may be “sensitive” depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.

“Real Data,” as used in this clause, means data from a production system, vendor, or public records, or any other dataset which otherwise contains operational data.
Examples of real data include a dataset that is a ten-year old backup of an existing system and contains data about real individuals, matters, or cases, would be real data. A set of public records that was purchased from a vendor for use in testing would also be real data.

**H.6.2 Systems Access**

Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding systems the contractor operates on behalf of the Government under this contract, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

**H.6.3 Data Security**

Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.

The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.

The Department of Homeland Security (DHS) has determined that performance of the tasks as described in this contract requires that the Contractor, vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following:

1. The contractor will safeguard any PII information and conduct training regarding the handling and protection of PII.
2. The contractor must report all suspected or confirmed incidents involving the loss and/or disclosure of PII to the Contracting Officer's Representative (COR).
3. The contractor agrees to reimburse ICE for the full cost of procuring victim remediation services, acquired following a loss or compromise of any identifying information about individuals, due to any act or omission of contractor or its employees, agents, subcontractors, or lower tier subcontractors. In its sole discretion, ICE will determine what victim remediation services are reasonable under the circumstances. The contractor will promptly notify the COR of a 'security incident' as set forth in the DHS Handbook for safeguarding sensitive PII. Upon such notification, ICE/OAQ will secure from a Department entity or the Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.
4. The contractor will hold harmless and unconditionally indemnify the government for the full extent of any liability, loss, cost, claim, damage, or expense resulting from, or in connection with, a loss or disclosure of PII in connection with the work performed under this contract due to any act or omission of contractor or its employees, agents, subcontractors, or lower tier subcontractors.

Source Selection Information - - See FAR 3.104

2022-ICLI-00039 508
Note: The term 'data breach' means the loss, theft, or other unauthorized access to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Contractor agrees that failure to cooperate maybe deemed a material breach of the contract by the government. The DHS Handbook for safeguarding sensitive PII can be found at: http://www.dhs.gov/xlibrary/assets/privacy/privacy-guide-spii-handbook.pdf

H.6.4 Pass-Through to Subcontractors

The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.


Contractor and sub-Contractors shall encrypt all “Sensitive Personally Identifiable Information” (Sensitive PII) data provided to them, collected for, or created under the contract. This requirement applies to all Sensitive PII data at rest and in transit and regardless of the physical or logical location of the data. The encryption must meet FIPS PUB 140-2 (Federal Information Processing Standards, established by the National Institute of Standards and Technology). An example encryption method that meets FIPS PUB 140-2 is AES 256 bit encryption. If the Contractor does not meet these standards, it should be considered and dealt with as a nonperformance issue.


H.6.6 Required Privacy Training forContractors

Contractor shall provide training for all employees and sub-Contractors that have access to Sensitive PII as well as the creation, use, dissemination and / or destruction of Sensitive PII, at the outset of the sub-Contractor’s / employee’s work on the contract and every year thereafter. Said training would include procedures on how to properly handle Sensitive PII, to include security requirements for transporting of transmitting Sensitive PII information, reporting requirements for a suspected breach or loss of Sensitive PII information, etc.

The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information, regardless of their employment status, be they Federal or contract type employees, to take the annual Information Assurance Awareness Training (IAAT). In addition, all Contractor employees are required to complete ICE’s Records Management Training annually.

Both courses (IAAT and Records Management) can be obtained via government provided CD. Contractor shall maintain copies of certificates as a record of compliance. The Contractor must submit an annual e-mail notification to the ICE COR that the required training has been completed for all the Contractor’s employees.
H.6.7 Reporting Suspected Loss of Sensitive PII

Contractors must report the suspected loss or compromise of Sensitive PII to ICE in a timely manner and cooperate with ICE’s Inquiry into the incident and efforts to remediate any harm to potential victims. The contracts should require the following (for existing and all new contracts involving Contracts handling Sensitive PII):

1. Contractor must report the suspected loss or compromise of Sensitive PII by its employees or sub-Contractors to the ICE Contracting Officer's Representative (COR) or Contracting Officer within one (1) hour of the initial discovery.

2. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and sub-Contractors are trained to identify and report potential loss or compromise of Sensitive PII.

3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of Sensitive PII containing the following information:
   
   a. Narrative, detailed description of the events surrounding the suspected loss/compromise.
   b. Date, time, and location of the incident.
   c. Type of information lost or compromised.
   d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
   e. Names of person(s) involved, including victim, Contractor employee/sub-Contractor and any witnesses.
   f. Cause of the incident and whether the company's security plan was followed or not, and which specific provisions were not followed.
   g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
   h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

4. The Contractor must cooperate with ICE or other government agency inquiries into the suspected loss or compromise of Sensitive PII.

5. At the government's discretion, Contractor employees or sub-Contractor employees may be identified as no longer eligible to access Sensitive PII or to work on that contract based on their actions related to the loss or compromise of Sensitive PII.

H.6.8 Separation Checklist for Contractor Employees

Contractors shall enact a protocol to use a separation checklist before its employees terminate working in the contract. The separation check list would cover areas such as:

(1) Return of any government-furnished equipment;
(2) Return or proper disposal of Sensitive PII (paper or electronic) in the custody of the Contractor employee or independent Contractor, including the wiping of data on any computer systems or media as appropriate; and
(3) Termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access Sensitive PII.

Source Selection Information - - See FAR 3.104

2022-ICLI-00039 510
In the event of adverse job actions resulting in the dismissal of a Contractor employee or sub-Contractor, the Contractor shall notify the COR within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of the employment or work on the contract. The Contractor shall provide a copy of the checklist to the COR, if request by the COR, within 5-business days following the employee’s termination.

H.6.9 Restrictions on Testing Using Real Data Containing PII

The use of real data containing Sensitive PII, from any source, for testing purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing whenever feasible. ICE policy requires that any proposal to use real data or de-identified data for IT system testing be approved by the ICE Privacy Officer and Chief Information Security Officer in advance. In the event performance of the contract requires or necessitates the use of real data for system testing purposes, the Contractor in coordination with the CO or COR and government program manager shall obtain approval from OCIO and the ICE Privacy Office and complete any required documentation.

H.6.10 Restrictions on Training Using Real Data Containing PII

The use of real data containing Sensitive PII, from any source, for training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for training whenever feasible. ICE policy requires that any proposal to use real data or de-identified data for IT system training be approved by the ICE Privacy Officer and Chief Information Security Officer in advance. In the event performance of the contract requires or necessitates the use of real data for training purposes, the Contractor in coordination with the CO or COR and government program manager shall obtain approval from OCIO and the ICE Privacy Office and complete any required documentation.

H.6.11 Contractor IT Systems Hosting Government Data

The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor, or any subcontractor, on which Government data shall reside for purposes of IT system development, design, data migration, testing, training, or disposal. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract.

H.6.12 Support Completion of Privacy Compliance Documents

The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three 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 adequate support to complete the PIA in a timely manner, and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones.

Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website (www.dhs.gov/privacy) under “Privacy Compliance Process & Templates.” DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at
DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.