U.S. Immigration and Customs Enforcement (ICE)
Office of Human Capital

Review of Physical Fitness Testing for Mission Critical Occupations

Performance Work Statement

August 2023

Part 1 General

1. General: The Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) Office of Human Capital (OHC) has a requirement for Physical Fitness Testing. ICE intends to conduct a comprehensive review of its current approaches to evaluating physical fitness both pre- and post-hire.

1.1 Description of Services/Introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other services necessary to perform *Review of Physical Fitness Testing for Mission Critical Occupations* as defined in this Performance Work Statement except for those items specified as government furnished property and services. All work completed by the contractor shall be in full accordance with employment selection and assessment best practices as specified in the *Uniform Guidelines on Employee Selection Procedures* (EEOC, 1978), *Standards for Educational and Psychological Testing* (AERA, 2014), *Principles for the Validation and Use of Personnel Selection Procedures* (SIOP, 2018), and *U.S. Merit Systems Principles.*

1.2 Background: To maintain physical fitness standards in two of its physically demanding mission critical occupations in accordance with the needs of the job and appropriate safety requirements, ICE intends to conduct a comprehensive review of its current approaches to evaluating physical fitness both pre- and post-hire. As the landscape evolves regarding regulations and approaches to physical fitness testing, ICE seeks to align its process to current best practices, particularly within the Federal government, as may be warranted.

1.3 Objectives: The contractor shall perform an assessment of pre-and post-hire physical fitness activities for two, physically demanding, mission critical occupations. The contractor shall:

1.3.1 Evaluate ICE's current physical fitness process and procedures.

1.3.2 Gather and assess available testing data within ICE programs.

The contractor will conduct reviews, collect data, conduct analyses, summarize, and provide recommendations. Services include oral and written reports of information gathered; cleaned and processed datasets; numerical analyses; and strategic recommendations.

1.4 Scope: Contractor executed reviews will encompass existing physical fitness test (PFT) data for two primary mission critical occupations over the course of five prior years, making an initial evaluation of current state and recommendations for future approaches.

1.5 Period of Performance: The period of performance shall be for one (1) Base Year of 12 months and one (1) 12-month option years. The Period of Performance reads as follows:

Base Year: September 2023 – August 2024
Option Year I: September 2024 – August 2025

1.6 General Information:

1.6.1 Quality Control: The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's quality control program is how the contractor assures that the work complies with the requirements of the contract. The QCP will be delivered with the contractor's proposal as it will serve as an evaluation factor. Three copies of a comprehensive written QCP will be submitted to the CO and COR within five (5) working days when changes are made thereafter.

1.6.1.1 The contractor's QCP shall contain, as a minimum, the following items:

a. A description of the inspection system to cover all services. Description shall include specifies as to the areas to be inspected on a scheduled and unscheduled basis, frequency of inspections, and the title and organizational placement of the inspector(s).

b. A description of the methods to be used for identifying and preventing defects in the quality of service being performed.

c. A description of how the records shall be kept. Records shall document all inspections and corrective or preventive actions taken.

1.6.1.2 Records of inspections shall be kept and made available to the Government throughout the contract performance period and for the period after contract completion until final settlement of any claims under this contract.

1.6.2 Quality Assurance: The government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government will do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.6.3 Recognized Holidays:

New Year's Day
Martin Luther King Jr.'s Birthday
President's Day
Memorial Day
Independence Day
Juneteenth
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

1.6.4 Hours of Operation: The contractor is responsible for conducting business between the hours of 8:00AM and 5:00PM Eastern Time, Monday thru Friday, except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. For other than firm fixed price contracts, the contractor shall not be reimbursed when the government facility is closed for the above reasons. The Contractor shall always maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

1.6.5 Place of Performance: The work to be performed under this contract shall primarily be remote; travel will not be required.

1.6.6 Type of Contract: The government will award a Firm Fixed Price Task order.

1.6.7 Security Requirements: Contractor personnel performing work under this contract will not be required to access sensitive information. The contractor security requirements will be determined in accordance with the PWS, and other DHS forms as needed.

1.6.7.1 Physical Security: The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use.

1.6.8 Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the contracting officer will advise the contractor of how the government views the contractor's performance and the contractor shall apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.6.9 Contracting Officer Representative (COR): The (COR) will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the Contractor concerning technical aspects of the contract: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially regarding changes in cost or price, estimates or changes in delivery

dates. The COR is not authorized to change any of the terms and conditions of the contract or any resulting order.

1.6.10 Identification of Contractor Employees: All contractor personnel attending meetings, all communication with Government employees, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression to the public that they are Government officials. They shall also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

1.6.11 Contractor Travel: ~~Travel will not be required.~~ To meet the requirements of this contract, travel is required by ~~ICE and~~ contractor personnel, specifically, site visits to a geographically diverse set of locations will be undertaken. These visits will be used to collect data to produce status information (i.e., of existing tests) and inform potential new approaches. Travel estimates are included in the WLE-PAT Travel Summary Estimate, attached.

1.6.12 Other Direct Costs: The contractor may incur reproduction, shipping, and expenses associated with data review and reporting, and other miscellaneous expenses. A miscellaneous line item will be included to cover these costs at a limit of set by the Government after contract award.

1.6.13 Data Rights: The Government has unlimited rights to all documents and material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership and copyrights belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government will be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.6.14 Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (example, cost or pricing information, budget information or analyses, specifications, or work statements) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor

from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.15 Contractor Personnel

Contract personnel are required to have subject matter expertise and hands-on experience in areas related to behavioral and social sciences, quantitative psychology, law enforcement, physical fitness testing (PFT), adverse impact analysis, and database management. The following minimum personnel qualifications are to be considered mandatory for performance of the work:

1.6.15.0.1 Demonstrated experience to deliver professional and legally sound recommendations as specified in the PWS in full accordance with the *Uniform Guidelines on Employee Selection Procedures* (EEOC, 1978), *Standards for Educational and Psychological Testing* (AERA, 2014), *Principles for the Validation and Use of Personnel Selection Procedures* (SIOP, 2018), and *U.S. Merit Systems Principles*.

1.6.17.0.2 A sufficient staffing model capable of producing deliverables in an efficient and timely manner.

1.6.15.1. Key Personnel:

Senior Project Manager: the contractor shall provide a contract senior project manager who shall be responsible for the performance of the services. The names of the contract program manager shall be provided to the CO in writing prior to the beginning of the first performance period. If change in personnel is required, the contractor shall notify the Government immediately and identify a replacement for consideration. The contract program manager shall be able to read, write, speak, and understand English.

1.6.15.1.1 The Senior Project Manager will serve as the overall project lead and the primary point of contact for the customer. The individual filling this role shall have either a PhD in Industrial-Organizational Psychology or Quantitative Psychology as well as the following: A minimum of 10 years of experience conducting physical fitness testing research, development and validation and defense; a minimum of 10 years of experience in legal defense and litigation of physical fitness tests for federal law enforcement agencies; a minimum of 10 years project management experience with a well-documented ability to manage large-scale projects for federal-level government agencies.

1.6.15.1.2 The contract senior project manager shall have full authority to act for the contractor on all matters relating to daily operations of this contract.

1.6.15.1.3 The contract senior project manager shall be available during normal duty hours within two (2) hours to meet in a specified location with government personnel (designated by the CO) to discuss any problems or issues that may arise. After normal duty hours the contract manager shall be available within four (4) hours.

1.6.15.1.4 Psychometrician: The Psychometrician will serve as a member of the project team and shall be primarily in charge of planning, executing, interpreting, and

delivering statistical analysis results and datasets to the customer. The individual filling this role shall have either a PhD in Industrial-Organizational Psychology or Quantitative Psychology as well as the following: A minimum of 5 years of experience conducting analyses related to high-stakes selection and assessment testing and development (to include adverse impact analyses); a minimum of 5 years of experience in missing data value imputation and data simulation techniques (e.g., Monte Carlo data simulation, etc.).

1.6.15.1.5 Data Analyst: The Data Analyst will serve as a member of the project team and shall assist the Psychometrician in data collection, cleaning, processing, and organization. The individual filling this role shall have either a master's degree in industrial-Organizational Psychology or Quantitative Psychology as well as the following: A minimum of 5 years of experience using SPSS, SAS, R, or Python to collect, clean, process, and organize large-scale datasets for analysis and delivery to customers.

1.6.15.1.6 Industrial-Organizational Psychologist: The Industrial-Organizational Psychologist will serve as a member of the project team and shall assist both the Senior Project Manager and Psychometrician with all activities related to best practice approaches to physical abilities testing in accordance with industry and field best practices (e.g., the Uniform Guidelines, Standards, Principles, etc.). The individual filling this role shall have a PhD in Industrial-Organizational Psychology as well as the following: A minimum of 5 years of experience conducting physical fitness testing research, development and validation and defense; a minimum of 5 years of experience in legal defense and litigation of physical fitness tests for federal law enforcement agencies.

1.6.15.1.7 Administrative: The Administrative position will serve as a member of the project team and shall assist all other members of the team with communications, logistics, and other administrative activities to facilitate data collection and general project progress. The individual filling this role shall have at least a High School diploma as well as the following: A minimum of 5 years of experience performing administrative duties and a well-documented ability to manage the logistical, administrative, and communications aspects of large-scale projects for federal-level government agencies.

1.6.15.2 Contractor Employees: the contractor shall not employ persons for work on this contract if such employee is identified to the contractor by the CO as a potential threat to the health, safety, security, general wellbeing or operational mission of the installation and its population.

1.6.15.2.1 Contractor personnel shall present a professional appearance and be easily recognized as contractor employees. This may be accomplished by wearing distinctive clothing bearing the name of the company or by wearing appropriate badges, which contain the company name and employee name in English.

1.6.15.2.2 The contractor shall not employ any person who is an employee of the U.S. Government if employing that person would create a conflict of interest.

1.6.15.2.3 An employee or their absence at any time shall not constitute an excuse for nonperformance under this contract.

1.6.16 Protected Information

1.6.16.1 Contractor access to information protected under the Privacy Act is required under this PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

1.6.20.11.6.18.2 Contractor access to proprietary information is required under this PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

PART 2
DEFINITIONS & ACRONYMS

2. **DEFINITIONS AND ACRONYMS:**
2.1. DEFINITIONS:

2.1.1. CONTRACTOR. A supplier or vendor having a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

2.1.2. CONTRACTING OFFICER (CO). A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment will be in writing and will state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor if that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5. DELIVERABLE. Anything that can be physically delivered but may include non-physical things such as meeting minutes.

2.1.6. KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.7. PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.8. QUALITY ASSURANCE. The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.9. QUALITY ASSURANCE Surveillance Plan (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.10. QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.11. SUBCONTRACTOR. One that enters a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.12. WORK DAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.12. WORK WEEK. Is defined as Monday through Friday, unless specified otherwise.

2.2. ACRONYMS:

ACOR	Alternate Contracting Officer's Representative
AFARS	Army Federal Acquisition Regulation Supplement
AIR	Adverse Impact Ratio
AR	Army Regulation
CCE	Contracting Center of Excellence
CFR	Code of Federal Regulations
CONUS	Continental United States (excludes Alaska and Hawaii)
CO	Contracting Officer
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off the Shelf
DA	Department of the Army
DD250	Department of Defense Form 250 (Receiving Report)
DD254	Department of Defense Contract Security Requirement List
DEIA	Diversity, Equity, Inclusion, and Accessibility
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DOD	Department of Defense
FAR	Federal Acquisition Regulation
FLETC	Federal Law Enforcement Training Center
HIPAA	Health Insurance Portability and Accountability Act of 1996
ICE	Immigration and Customs Enforcement
LEO	Law Enforcement Officer
MCO	Mission Critical Occupation
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
PEB	Physical Efficiency Battery
PFT	Physical Fitness Testing/Tests
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
TE	Technical Exhibit
USCG	United States Coast Guard

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES:

3.1. Materials**:** The Government will provide:

- relevant job analysis studies
- de-identified physical fitness training data.
- briefing slides
- technical reports
- relevant ICE policy documents to facilitate contractor activities.

3.2. Services: The Government will facilitate access to ICE business, recruiting, and training units to permit data discovery and data collection on an "as needed" basis.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1. General: The Contractor shall furnish all supplies, equipment, facilities, and services required to perform work under this contract that are not listed under Section 3 of this PWS.

PART 5
SPECIFIC TASKS

5. Specific Tasks:

5.1. Conduct discovery and assessment of 1) pre-employment and 2) job-impacting, post-hire physical fitness test (PFT) and data collection activities for two mission critical career fields.

5.1.1. Detail the current state of pre-employment PFTs for two mission critical career fields, to include:

- Pre-employment PFT policy, protocol, test components, and criteria to determine pass/failure.
- Granularity and availability of pre-employment PFT data collected and recorded by pre-hire field locations.
- Consistency and uniformity of pre-employment PFT data collection, entry, and maintenance by pre-hire field locations, to include observed deviations from established testing policy and/or protocol in the field.

5.1.2. Detail the current state of job impacting, post-hire PFTs for two mission critical career fields, to include:

- Post-hire PFT policy, protocol, test components, and criteria to determine pass/failure.
- Granularity and availability of post-hire PFT data collected and recorded during career field training.
- Consistency and uniformity of post-hire PFT data collection, entry, and maintenance during career field training, to include observed deviations from established testing policy and/or protocol.

5.1.3. Based on results of 5.1.1. and 5.1.2., identify gaps in understanding of career field requirements, and collect all necessary job-related data needed to accurately specify appropriate physical requirements for pre-employment and post-hire PFTs for two mission critical career fields.

5.2. Identify, compile, process, and deliver pre-employment and job impacting, post-hire PFT data for ~~two~~ one mission critical career field~~s~~.

5.2.1. Identify, compile, process, and deliver all relevant pre-employment and job-impacting, post-hire PFT data including demographic (e.g., gender~~, race, ethnicity~~) and identifying data, individual exercises, final score, and test pass/fail data.

- Pre-employment – Anticipated data to identify, compile, and deliver spans fiscal years 2021 through 2023 ~~the five (5) most recent fiscal years~~ with approximately ~~4,800~~900 pre-employment PFT records ~~divided among both mission critical career fields~~.
- Post-Hire – Anticipated data to identify, compile, and deliver spans ~~the five (5) most recent fiscal years~~ fiscal years 2019 through 2022 with approximately ~~3,900~~1,300

multi-point assessment post-hire PFT records, ~~divided among both mission critical career fields.~~

5.2.1.1. Provide a summary of data collection, processing, and manipulation steps to include delivery of a data set code book clearly defining and summarizing the data set and each column variable in layman's terms.

5.2.1.2. Provide an assessment of collected data "as-is" to include potential impacts of missing data and sample size on possible future data analysis.

5.2.1.3. ~~Conduct all necessary data processing steps to address identified data issues and improve data analysis options (e.g., missing data value imputation, Monte Carlo data simulation, etc.) and d~~Deliver finalized datasets in a state ready for statistical analysis.

~~5.2.1.4. Provide analysis recommendations to calculate and examine adverse impact by demographic variables (e.g., Adverse Impact Ratios [AIRs], Cohen's *d* effect sizes, etc.) for individual exercises, final score, and test pass/fail data for both mission critical career fields.~~

5.3. Service Contract Reporting (SCR). This will be input in the www.sam.gov with guides available for all contractors to utilize on the website. The total amounts invoiced, and other items are described inside the links on the website. There is a link for quick start as referenced here, (https://www.sam.gov/SAM/transcript/SCR_QSG.pdf).

PART 6
APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS)

6.1. The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures including the *Uniform Guidelines on Employee Selection Procedures* (EEOC, 1978), *Standards for Educational and Psychological Testing* (AERA, 2014), *Principles for the Validation and Use of Personnel Selection Procedures* (SIOP, 2018), and *U.S. Merit Systems Principles* (5 U.S. Code § 2301, 1978).

PART 7
ATTACHMENT AND TECHNICAL EXHIBIT LISTING

7. Attachment and Technical Exhibit List:

7.1 Attachment 1/Technical Exhibit 1 – Deliverables Schedule

Attachment 1 / Technical Exhibit 1 ("Deliverables Schedule") contains a basic breakdown of all products to be produced, briefings to be delivered, and data to be collected throughout the contract period of performance. Detailed requirements will be discussed during the contract kick-off and throughout the contract period of performance.

7.2 Attachment 2/Technical Exhibit 2 – Estimated Workload Data

Performance Requirements Summary

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective	Standard	Performance Threshold	Method of Surveillance
PRS #1: The contractor shall conduct at least monthly virtual progress report meetings with the technical team, to be accompanied by a written progress report on the completion status of all tasks to date [PWS paragraphs 5.1. through 5.3.]	• The contractor will present their monthly progress report update via Microsoft Teams along with a written status report on at least a monthly basis • Following each progress report meeting, and after reviewing the accompanying provided written status report(s), the technical team will make a group determination of whether the contractor is "on track" or "not on track" to complete all performance objectives	• No month passes in which no progress report meeting is not held • Not more than three total "not on track" determinations by the technical team through the life of the contract • No consecutive "not on track" determinations by the technical team through the life of the contract	• Direct observation by technical team • Progress report meetings with technical team • Written progress reports submitted to technical team

PRS #2: The contractor shall provide the technical team both interim and final versions of requested products (technical reports, datasets, etc.) as specified in all tasks [PWS paragraphs 5.1. through 5.3.]	• The contractor will submit interim deliverables to the technical team no later than 60 days prior to the end of the period of performance • The contractor will submit final deliverables to the technical team no later than 30 days prior to the end of the period of performance • For both interim and final deliverables, the technical team will review and submit revision requests as needed to accomplish contract goals • Once interim or final version revisions are completed, the technical team will again review the deliverable and make a group determination on whether the deliverable is acceptable to fulfill contract requirements	• Interim and final deliverables are provided to the technical team NLT 60 and 30 days prior to the end of performance, respectively. • All proposed changes made by the technical team to interim and final products are implemented by the contractor within 14 days of submission • The technical team approves interim and final deliverables with no additional requested changes	• Direct observation by technical team • 100% review of interim and final deliverables

PRS # 3: The contractor shall adhere to all Service Contract Reporting (SCR) requirements [PWS Paragraph 5.3.]	• The contractor provides a summary status/financial report to the technical team for each month of the period of performance • The contractor schedules a kick-off meeting with the technical team within 2 weeks of contract award • The contractor delivers an execution plan to the technical team within 4 weeks of contract award • The contractor provides all final deliverables for all tasks by the last day of the period of performance	• A summary status/financial report is submitted by the contractor for each month during the period of performance • The kick-off meeting is scheduled by the required deadline and delivered within 4 weeks of contract start • The execution plan is delivered by the required deadline • All final deliverables are provided to the technical team no later than the last day of the period of performance	Direct observation by the technical team

TECHNICAL EXHIBIT 1

ESTIMATED WORKLOAD DATA

ITEM	NAME	ESTIMATED QUANTITY	
1	Senior Project Manager (I-O Expert in Field)	1 –	1040 HRS (approx. 0.5 FTE)
2	Psychometrician	1 –	1560 HRS (approx. 0.75 FTE)
3	Data Analyst (I-O Specific, Junior)	1 –	1560 HRS (approx. 0.75 FTE)
4	I-O Psychologist (Senior)	1 –	2080 HRS (approx. 1.0 FTE)
5	Administrative	1 –	2080 HRS (approx. 1.0 FTE)

PART 8
CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Sensitive But Unclassified (SBU) Contracts
SECURITY REQUIREMENTS

GENERAL

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

PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor applicants/employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the Contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination by the Office of Professional Responsibility (OPR), Personnel Security Division (PSD). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination by OPR PSD. Contract employees are processed under 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, temporary, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through OPR PSD. Contractor applicant/employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR PSD, through the Contracting Officer Representative (COR), within 10 days of notification by OPR PSD 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 those with direct contact with detainees or armed positions)), "Questionnaire for Public Trust Positions" form completed online and archived by the Contractor applicant in their OPM e-QIP account.

2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable). These forms are completed online and archived by the Contractor applicant in their OPM e-QIP account.

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

4. Optional Form 306 Declaration for Federal Employment. This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD. This form is completed online and archived by the Contractor applicant in their OPM e-QIP account.

5. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards). This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD. This form is completed online and archived by the Contractor applicant in their OPM e-QIP account.

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

form is completed online and archived by the Contractor applicant in their OPM e-QIP 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 5 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 (IAW Executive Order 13488 amended under Executive Order 13764 and DHS Instruction 121-01-007-01).

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

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

Only U.S. citizens and Lawful 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.

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. OPR PSD 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 PSD, via the COR, of all terminations/resignations of Contractor employees under the contract within five days of occurrence via a Contractor Employee Separation Clearance Checklist (ICE Form 50-005). 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 OPR PSD, 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 [redacted] no later than the 10th day of each January, April, July and October.

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

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

SECURITY MANAGEMENT

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

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

INFORMATION TECHNOLOGY SECURITY

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

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

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

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

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

PART 9
SAFEGUARDING OF SENSITIVE INFORMATION – (MAR15)

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.
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.

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

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.

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.

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.

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.

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.

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 (19) 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.

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.

PART 10
INFORMATION TECHNOLOGY SECUIRTY AND PRIVACY TRAINING (MAR2015)

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.

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.

PART 11
PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.
Limiting Access to Privacy Act and Other Sensitive Information
In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have

access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment

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

Prior Approval Required to Hire Subcontractors

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

Separation Checklist for Contractor Employees

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

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

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

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

Privacy Lead Requirements
If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.
The Privacy Lead:
- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

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

met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

APPENDIX A
CYBERSECURITY CONTRACT REQUIREMENTS

A.1 ICE Cyber Security Requirements In accordance with ITAR 4.5.4.1 – Compliance with DHS Security Policy Terms and Conditions.

Compliance with DHS Security Policy Terms and Conditions:

All hardware, software, and services provided under this contract must be compliant with DHS 4300B DHS Sensitive System Policy and DHS 4300B 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 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:

A.4 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 sixty (60) 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.5 Contractor IT Security Accreditation

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.7.2 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.

APPENDIX B
CYBERSECURITY COMPLIANCE REQUIREMENTS

B.1 A.8 I (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.

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– ISA

ISA Terms and Conditions
Interconnections between DHS and non-DHS 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 4.5.3.8 – 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.4 In accordance with ITAR 4.5.4.2 – Encryption Compliance

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 1 40-1 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.5 In accordance with ITAR 4.5.4.3 – Handling or Processing of Classified Information

Handling or Processing of Classified Information
Contractor access to classified information is required under this procurement. The maximum level of classification is (SECRET). Details will be provided in a Department of Defense (DD) Form 254.
(Appendix (G) contains DD FORM 254 security clearance documentation)

Handling or Processing of Classified Information Terms and Conditions
a) Classified information is Government information which requires protection in accordance with Executive Order 12958, National Security Information (NSI) as amended and supplemental directives. If the contractor has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. *b)* Contractor shall comply with all government facility and security requirements while on government property, including obtaining and displaying identification badges, obtaining vehicle decals and proper vehicle operation. *c)* The contractor shall have a facility security clearance up to (SECRET) level. All personnel supporting this procurement shall be required to obtain and maintain a (SECRET) level clearance. The Government reserves the right to approve or deny suitability of the contractor's individual employees based on security risks, unsatisfactory performance, or disruptive influence on mission accomplishment.

Requirements for Handling Sensitive Information Terms and Conditions

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, an attachment to the contract, and the NISPOM for protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service.

B.6 As referenced in ITAR 4.5.4.3 and in accordance with FAR 52.204-2 Security Requirements (MAR 2021)

Security Requirements (Mar 2021)
(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."
(b) The Contractor shall comply with-
(1) The Security Agreement DD Form441), including the *National Industrial Security Program Operating Manual* (32 CFR part 117); and
B.7 (2) Any revisions to that manual, notice of which has been furnished to the Contractor.
B.8 (c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.
B.9 (d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.
(End of clause)
Security Clearances
At the time of award, the contractor shall have the appropriate Top Secret or Secret security clearances for the employees as required by the Work Assignment they will

work under on this contract. Affected employees must have a current investigation in place or being processed for a periodic reinvestigation.
A Department of Defense Contract Security Classification Specification (DD Form 254) shall be issued by the Government Contracting Activity (GCA)CO to the contractor at the time of contract award (FAR 4.403) (c)(1)). The contracting officer shall also provide a copy to the DSS and the GCA COR. In accordance with DoD Manual 5200.22M, Industrial Security Manual for Safeguarding Classified Information, the Contractor shall have a Facility Clearance issued by DSS.

B.10 Patch Management Terms and Conditions

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

Data Ownership Contract Requirements Language

1. **Accessibility of Government-owned Data**
   All stored program data associated with this acquisition shall be owned by the Government. As such, it shall be made accessible to the Government in accordance with the Minimum Data Access Capability described below. This accessibility is required to allow full data transparency, flexibility in performing data analytics, and integration with data from other government programs.

   In addition to the Minimum Data Access Capability, the Government prefers, but does not require, that program data be accessible via Enhanced Access Capabilities as described below.

   Definition of **"program data"**: Program Data refers to any data resulting from ICE and DHS organizational activity. Examples of such data include but are not limited to administrative data resulting from human resource, management, and financial actions, as well as operational data resulting from performance of the ICE mission.

   Definition of "**associated with this acquisition"**: Program Data is associated with an acquisition if it is created by DHS organizational activity that is facilitated by the contractor. Examples of how a contractor might facilitate organizational activity follow:
   - Program data is stored by contractor personnel

- Program data is stored by software that is managed, developed, or used by the contractor
- Program data is stored in a repository that is managed, developed, or used by the contractor

2. Minimum Data Access Capability

- The current version of all Program Data is accessible to the Government within 24 hours of request, as well as on any pre-defined schedule as required by the Government.

  Data access can occur by various means, provided that Government security requirements are met, and data is accessible in a format that is acceptable to the Government. Examples include but are not limited to APIs that are consumable by the Government, files made available for Government download (e.g., Excel Spreadsheets), or direct database query by federal or contractor personnel.

- The contractor shall format program data accessed by the Government to anticipate the maximum file size of any data to be accessed. File size shall be small enough to assure rapid processing by government applications.

- The contractor shall provide the means for the Government to interpret accessible Program Data as follows:

  - Data elements and groupings of data elements shall be clearly identifiable by labels embedded in the data itself, or by a separate schema or file layout which allows such elements and groupings to be identified.
    In the case of a relational database schema defined through Data Definition Language (DDL), data elements would be represented as columns, and groupings of data would be represented as tables. In addition, relationships between tables would be described as foreign key relations.
  - Labels or names used to identify data elements and groupings of data elements shall be approved by the Government. In addition, each label or name shall be associated with a government approved definition which describes the content of data held therein.
  - Program data delivered to the Government shall conform to the Government approved definition for each data element and grouping of data elements.
  - All data accessible by the Government shall be both machine readable and human-readable in plain text.
  - All reference data associated with Program Data also needs to be accessible to the Government. Such reference data is required to provide complete understanding of a record.

Reference Data Example: Program data may include a city code which uniquely identifies a city. Reference data associated with a city code may include its name, geographic boundaries, population, median income, etc. This example is provided for clarification of the meaning of reference data and may or may not apply to this specific acquisition. Examples of other reference data codes would include codes representing eye color, gender, country of origin, etc.

3. **Enhanced Access Capabilities**

The Government prefers that sharing of program data take place via an Application Programming Interface (API) or multiple APIs. APIs allow the Government to efficiently consume data via a widely recognized standard where the data has been completely abstracted from the technology platform that produces it.

In addition, the Government prefers that sharing of program data take place using techniques that enhance efficiency, such as Change Data Capture (CDC). CDC enhances efficiency of data transfer by providing only incremental updates to program data as opposed to providing all program data each time data is shared.