DEPARTMENT OF HOMELAND SECURITY (DHS)

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)

ICE DIRECTOR'S OFFICE

INTERNET BASED THREAT RISK MITIGATION AND MONITORING SERVICES

STATEMENT OF OBJECTIVES

Date TBD

1. Background:

ICE's mission is to promote homeland security and public safety through the criminal and civil enforcement of approximately 400 federal laws governing border control, customs, trade and immigration.

Over the last two years, ICE has experienced an increased level of external threat activity directed towards its Senior leaders, personnel and facilities. Much of this threat activity originates from social media and online postings and has since expanded to physical attacks on ICE facilities and the homes of ICE employees. In order to prevent adversaries from successfully targeting ICE Senior leaders, personnel and facilities, ICE requires real-time threat mitigation and monitoring services, vulnerability assessments, and proactive threat monitoring services.

2. Point of Contact

The Contractor shall provide a point of contact responsible for coordinating work performance. The point of contact shall have full authority to act on behalf of the Contractor on all matters relating to the daily operation of this contract. The Government point of contact will be the Contracting Officer's Representative (COR) as later determined and delegated.

3. Description of Services/Introduction:

The Contractor shall provide all necessary personnel, supervision, management, equipment, materials and services, except for those provided by the Government, in support of ICE's desire to protect ICE Senior Leaders, personnel and facilities via internet-based threat mitigation and monitoring services. These efforts include conducting vulnerability assessments and proactive threat monitoring.

Minimum services include full data aggregation to provide proactive threat monitoring and vulnerability assessments stipulated in the following Tasks Objectives in Section 5. The Contractor will utilize the following Tier Level categories to identify the minimum deliverable and reporting requirements as stipulated in Section 6.

Tier Level	Tier Level Coverage	Tier Level Description
Tier 1	ICE Senior Leaders *(Minimum 12 Targets)*	Tier 1 provides detailed and tailored executive open-source Vulnerability Assessments and Proactive Threat Monitoring for ICE Senior Leaders, and, as requested by ICE OPR, their immediate family members.
Tier 2	General ICE Population and Facilities *(Minimum 100 Targets)*	Tier 2 provides detailed open-source Vulnerability Assessments and Proactive Threat Monitoring for threats towards ICE employees and facilities in general. Tier 2 will also provide for the assessment and monitoring of threats and/or disruptions to general ICE operations.
Tier 3	Specific ICE Employees, Operations and Facilities as requested by ICE OPR *(Minimum 15 Targets)*	Tier 3 provides detailed open-source Vulnerability Assessments and Proactive Threat Monitoring for threats against designated ICE employees, their immediate family members and facilities on an AD-HOC basis. Tier 3 will also provide for the assessment and monitoring of threats and/or disruptions to specific ICE operations as requested.

4. Service Provider – Non-Personal Services

DHS retains the authority to make all decisions regarding the DHS mission, and the execution or interpretation of laws of the United States. Contactor Services defined are not considered to be inherently Governmental in nature, as defined by Federal Acquisition Regulation (FAR) Subpart 7.5. This is a Non-Personal services contract as defined by FAR Subpart 37.101. Contractor personnel rendering services under this order are not subject to direct, day to day supervision or control by Government personnel. The Contractor will be responsible for the supervision of the Contractor employees at all duty locations. The Contractor is expected to work independently to accomplish the requirements of this order. The Contractor must generate reports and other deliverables as specified in the Statement of Objectives. The government will neither supervise contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances will the government assign tasks or prepare work schedules for individual contractor employees. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services. If the Contractor believes that any actions constitute or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the Contracting Officer (CO) immediately.

While it is the Contractor's responsibility to supervise its personnel, The United States Government, DHS and U.S. Immigration and Customs Enforcement will require and ensure all contractor personnel have received the requisite Privacy training, and any other training deemed necessary to satisfy the mission and requirements of the United States Government. The delivery of said training will be determined by the United States Government, but may include online training via a link provided by

the United States Government to contract employees, via government furnished equipment, virtual training, and/or in person training

5. Task Objectives:

5.1. Vulnerability Assessments

- Evaluate and conduct Tier 1 vulnerability assessments using proprietary and publicly available electronic information associated or regarding designated ICE Senior Leaders to identify threats, the exploitation of Protection Plans, and other risk factors. This assessment will be provided within five (5) business days from the award the contract.
- Evaluate and conduct Tier 2 vulnerability assessments using proprietary and publicly available electronic information associated or regarding threats to the general ICE population and facilities, as well as threats and/or disruptions to ICE operations. This assessment will be provided within five (5) business days of a request from ICE OPR.
- Evaluate and conduct Tier 3 vulnerability assessments using proprietary and publicly available electronic information associated or regarding designated ICE personnel, facilities and operations. These assessments will be provided on an ADHOC basis as requested by ICE OPR.
- Assessments and/or searches shall involve real-time aggregating open source information using unique identifiers for related association, enhanced data analytics, and analytic reporting on sentiment and other related factors.
- Assessments will include queries to determine what personally identifiable information is publicly available about those in categories Tier 1, 2 and 3 (Phone numbers, addresses, relatives, etc.).
- Conduct analytics by utilizing social and behavioral sciences to multiple data sets to locate dangerous individuals posing a possible threat to categories Tier 1, 2 and 3.
- Conduct real-time Deep Web and Dark Web searches to identify possible threats against categories Tier 1, 2 and 3.
- Conduct open source searches using key-terms and geolocation properties relative or associated with categories Tier 1, 2 and 3.
- Immediately notify ICE OPR via electronic means of imminent threats.
- Supply ADHOC vulnerability assessments as requested by ICE OPR.
- Supply assessments of locations and facilities as requested by ICE OPR.

5.2. Proactive Threat Monitoring & Report Requirements

- Provide a secure and proactive threat monitoring program that contains automatic alerts.
- Provide monitoring and analysis of behavioral and social media sentiment (i.e. positive, neutral, and negative) based on a time of day, a week, a month-long period.
- Upon system outages, capability to immediately complete searches to recover any lost or potentially lost threat information.
- Provide ADHOC searches and reporting when notified by ICE OPR.
- Provide secondary and/or follow-on real-time strategic monitoring of previous adverse findings.

- Capability to save search criteria post obtaining adverse results, ADHOC queries, or for future queries.
- Ensure searches and/or inquires on information and alerting procedures never reveal ICE's affiliation.
- Contractor will analyze individual(s) and/or organization(s) making threats. Analysis should include: 1). Previous social media activity which would indicate any additional threats to ICE; 2). Information which would indicate the individual(s) and/or the organization(s) making threats have a proclivity for violence; and 3). Information indicating a potential for carrying out a threat (such as postings depicting weapons, acts of violence, refences to acts of violence, to include empathy or affiliation with a group which has violent tendencies; references to violent acts; affections with violent acts; eluding to violent acts, etc.).
- Monitor and analyze all social media activities (including foreign/dark web/deep web social media networks) in REAL-TIME.
- Conduct correlation of users' social media accounts.
- Provides psychological profiles.
- Geo-locate individuals beyond standard geo-tagging. The government defines geo-locating as the ability to provide a specific location of the subject/threat actor.
- Identify any person or group who has previously identified as having made a threat and individual(s) whose language that would potentially lead to violence directed towards ICE, Facilities, and employees has reached a level of concern.
- Identify whether a user has deleted messages and provide content from deleted accounts and/or deleted messages.
- Capability to identify threats by location.
- Provide detailed daily, weekly, monthly and end of year/contract reporting, and ADHOC reporting on results with mitigating recommendations in Adobe PDF or Microsoft Office format.
- Provide ADHOC reports as requested by ICE OPR with the capability to adjust date ranges and identify threats by those made against ICE Senior Leaders, ICE employees, and facilities, as well as threat type.
- All daily, weekly, monthly and end of year/contract reports will be provided even when there is no reportable activity.
- All reports will include threat information in narrative form, including analytical summaries of identified threats and assessments.
- All reports will contain statistical data in narrative form and will be depicted in graphs (bar charts, pie charts, etc.).
- Statistical data provided in the reports should include information such as: 1). Total number of negative references to ICE found in social media during monitoring; 2). Total number of threats against Senior Leaders; 3). Total number of threats against ICE employees; 4). Total number of threats against ICE facilities/operations; 5). Trend analysis, such as the increase/decrease of threats for each of these categories during the requested period; and 6). Total number of threats by type.
- Daily reports will contain a running total as to the number of social media provided by the vendor. Each daily report will break this number down by the daily number of social media posts provided for review by day and a running total for fiscal year to date (Beginning October 1st of one year and ending September 30th of the following year).

- Daily reports will further break down the number of posts provided by platform (Reddit, YouTube, Facebook, News, X and other platforms). This breakdown will be included for the individual daily report and fiscal year running totals.
- Reports will identify ICE Senior Leaders, ICE employees and facilities that have been repeatedly targeted.
- Reports will provide all relevant information for threats identified by the contractor. This information shall include: 1). Screen renderings of threatening social media posts; 2). The real and social media identity of the threat originator; 2). Time, date and online platform through which the threat was made; and 3). Location and/or the identity of the ICE Senior Leader, ICE employee or facility identified in the threat.
- Facial Recognition capabilities that could take a photograph of a subject and search the internet to find all relevant information associated with the subject that will help identify any individual making a threat and help cross reference the individual across multiple platforms.
- At the request of OPR, the contractor needs to be able to adjust for the addition and removal of each Tier category from the monitoring list.
- Link analysis indicating individual may be associated with other potential threats/threat actors (narrative, charts & graphs).
- If threatening information is identified and in a foreign language, the contractor will provide the threat as it appears and provide a translation of the threat in English.
- Monitoring capabilities need to include the ability to proactively search for any threatening information and/or information which would suggest a potential disruption in ICE operations by location.
- Ability to determine which websites were accessed by users prior to making a threat.

5.3. Data Sources (Required, but not limited to)

- Open Source Information Portals
- Available Proprietary Sources
- Deep Web Content
- Dark Web Content
- IRC/Chat
- Message Boards
- Online Broadcasting Websites
- Public Email Groups and Discussion Forums
- Social Media Sites
- USEnet Data
- Web Blogs
- World Wide Web
- Public Records (Court records, police reports, DMV records, news reports, etc.)

5.4. Open Social Media Sources (Required, but not limited to)

- Twitter
- Facebook
- Foursquare
- Instagram
- Snapchat
- LinkedIn
- Pinterest
- Applicable Foreign Social Media Sites
- WordPress
- StumbleUpon
- Tagged
- YouTube
- Tumblr
- Vine Camera
- Bitly
- Flickr

6. Deliverables:

Acceptance by the Government of satisfactory products/services will be made once all the terms and conditions of the contract are fulfilled including the following delivery requirements:

Deliverable	Task	Frequency	Receivers
Tier 1 - Report on findings	All	Daily (NLT 11:00 AM EST)	Gov't POC
Tier 2 - Report on findings	All	Daily (NLT 11:00 AM EST)	Gov't POC
Tier 3 - Report on findings	All	Daily (NLT 11:00 AM EST)	Gov't POC
In-depth Monthly Vulnerability Assessment	All	Monthly (by the 1st calendar day of each month)	Gov't POC
Continuous monitoring and alerting on imminent threats (via electronic notification 24/7).	All	Immediately	Gov't POC
ADHOC Report	All	As needed	Gov't POC
Courtesy Invoice	All	Monthly (NLT the 15th calendar day of each Month)	COR

6.1. Deliverables Continued – Tiers 1, 2, 3 Reports
The Contractor shall provide a daily report of identified threats. The Contractor shall curate all findings into two sections:

1. Threat Intelligence: This section shall include a daily risk assessment based on the day's threat activity; a summary of post volume and change from previous period to provide contextual intelligence; a summary of key insights and identified threats, including the user platform, and language of the threat.
2. Social Media Overview: This section shall include a daily risk assessment based on the day's threat activity; a summary of post volume and change from previous period to provide contextual intelligence; a summary of key insights and identified threats, including the user platform, and language of the threat.

Each report shall include screenshots of threatening posts and a summary of active hyperlinks to the source material. Each finding reports shall be delivered to ICE daily by 11:00 AM EST.

6.2 Deliverables Continued – Ad Hoc Reporting
The Contractor shall develop and provide ICE Ad Hoc reports with actionable intelligence on identified threats within 24 hour period. Once a threat is identified, the Contractor shall review a user's available open source and social media activity to aid location of the associated individual.

The Ad Hoc reports shall be generated based on ICE guidance and request.

1. The Contractor shall provide public records details on the individual, as available. These details include, but are not limited to: Full legal name, date of birth, any aliases, Social Security Number (SSN), probable address(es), any relevant recent address(es), phone numbers, e-mail, work affiliations, vehicle registration information, and any criminal legal history, The Contractor shall also provide a summary of the methodology used to determine the subjects identity.
2. The Contractor shall provide all available identifying information to aid ICE in identification in complete information is unavailable. These details can include, but are not limited to: photograph, partial legal name, partial date of birth, possible city, possible work affiliations, possible school or university affiliation, and any identified possible family members or associates.

6.3 Deliverables Continued – Monthly Vulnerability Assessment
The Contractor shall provide a monthly Vulnerability Assessment on all key identified ICE Personnel to mitigate threats to high-risk personnel. The Monthly Vulnerability Assessment shall provide a comprehensive understanding of an executive's online exposure on social media, open source public record aggregators, and other open sources so ICE personnel can limit such exposure and remove vulnerable information adversaries could use to target ICE personnel.

The contractor can collect, analyze, and report on the full collection of openly available information on an identified individual and his immediate family, including spouse and children, in the Monthly Vulnerability Assessment.

All Monthly Vulnerability Assessments shall include:

1. An executive summary of key findings and identified threats.
2. An overview of the executive's social media presence collected of all social media platforms and open sources. The overview details the social media presence of the executive and includes the publicly available information used to connect the executive to his or her immediate family, including spouse and children, on social media and/or in open sources. Screenshots and hyperlinks (where available) of all relevant findings shall be included.
3. A summary of the open source presence of the executive's immediate family, including spouse and children. This summary details the analysis of open source public records for identifying information such as relatives, address, and phone number; social media; and open sources for key identifying and/or contextual details on a person's pattern of life.
4. An overview of any relevant open source a Deep Web and Dark Web exposure identified during research which adversaries could use to target ICE personnel or their families.
5. A comprehensive listing of all identified open source exposures. This listing shall include, but not limited to; type (public records, social media, or open source), an indication of whether the site is active as of the assessment; the URL; details of the available information; details of any links to the executive under review and/or their immediate family; and details of any addresses or phone numbers listed on the source.

7. Government Furnished Information and Support

ICE will provide a list of entity (ies) that require Threat Mitigation and Monitoring Service.

8. Service Provider Furnished Items

8.1. The Contractor shall furnish all other facilities, equipment, and services required in the performance of this contract.

8.2. The Contractor is responsible for taking the actions necessary to protect supplies, material, and equipment and personal property of employees from loss, damage, or theft.

9. Approval Authority

Overall coordination, final approval and authority for this project are the responsibility of the ICE Office of Professional Responsibility. The Contracting Officer will be the administrative point of contact at ICE Office of Acquisition Management – Mission support (MS) for all official correspondence and information concerning this contract. Final acceptability or unacceptability of all deliverables and tasks performed by the Contractor is the responsibility of the OAQ-MS Contracting Officer.

A Contracting Officer's Representative COR will be identified for this effort. The COR will recommend acceptance of the deliverable products, but only after concurrence from Government on-site Subject Matter Experts (SMEs) that deliverables are complete and correct.

10. Period of Performance

Performance Period	Performance Period Dates
Base Period	TBD
Option Period 1	TBD
Option Period 2	TBD
Option Period 3	TBD
Option Period 4	TBD

11. Type of Performance

The contract type will be a Firm Fixed Price Contract.

12. Place of Performance

The Contractor shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, training, and experience. The Contractor shall match personnel skills to the work or task with a minimum of under/over employment of resources. The Contractor shall provide the necessary resources and infrastructure to manage, perform, and administer

the contract. Performance will not be at a government location.

13. Business Relations

The Contractor shall successfully integrate and coordinate all activity needed to execute the requirement. The Contractor shall manage the timeliness, completeness, and quality of problem identification. The Contractor shall provide corrective action plans, proposal submittals and timely identification of issues. The Contractor shall seek to ensure customer satisfaction and professional and ethical behavior of all contractor personnel.

13.1. Quality Control: The Contractor will establish and maintain a complete Quality Control Plan (QCP). This plan will include expected services delivered, contractor procedures for review of delivered services, and other items that may have impact on the performance of this contract. The Contractor will submit their QCP within 15 business days of contract award. When changes are made to the QCP a revised plan will be submitted to the Government.

14. Constraints and Risks

14.1. Obtaining Information from Unrestricted Sources. When conducting social media searches, the Contractor may obtain information from publicly-accessible online sources and facilities under the same conditions they may obtain information from other sources generally open to the public. This principle applies to publicly-accessible sources located in foreign jurisdictions as well as those in the United States.

14.2. Accessing Restricted Sources. When conducting social media searches, the Contractor may not access restricted online sources or facilities.

14.3. Obtaining Identifying Information about Users or Networks. The Contractor may not use software tools, even those generally available as standard operating system software, to circumvent restrictions placed on system users.

14.4. Public Interaction. The Contractor may access publicly-available information only by reviewing posted information and may not interact with the individuals who posted the information.

14.5. Appropriating Online Identity. "Appropriating online identity" occurs when an entity electronically communicates with others by deliberately assuming the known online identity (such as the username) of a real person, without obtaining that person's consent. The Contractor may not use this technique to access information about individuals.

14.6. International Issues. Unless gathering information from online facilities configured for public access, Contractor personnel conducting the required service or deliverables should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever an item or person is located abroad, contractor personnel shall follow ICE's policies and procedures in providing the required service or deliverables.

14.7. PII Safeguards. The contractor will protect personally identifiable information (PII) as required by the Privacy Act and DHS privacy policy.

14.8. Complete ATO and Ongoing security scans and remediation for High Risk Sensitive contracts in accordance with HSAR Deviation 15-01.

15. Contract Management

The Contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement. The Contractor must maintain continuity between the support operations at OPR and the Contractor's corporate offices.

16. Contract Administration

The Contractor shall establish processes and assign appropriate resources to effectively administer the requirement. The Contractor shall respond to government requests for contractual actions in a timely fashion. The Contractor shall have a single point of contact between the government and Contractor personnel assigned to support contracts or task orders. The Contractor shall assign work effort and maintaining proper and accurate time keeping records of personnel assigned to work on the requirement.

16.1. Monthly Invoices: The Contractor shall provide monthly invoices to the ICE Invoice Consolidation Office, CO, and COR for services completed within that calendar month. Invoices will separate and note costs per CLIN (Tier Level) for the billed Period of Performance (POP). POP dates for each monthly invoice shall begin with the first and end on the last date of that month.

16.1.1. Invoices shall be submitted no later than the 15th calendar day of the following month. Should the 15th calendar day of the month fall on a Federal holiday or weekend, the invoice shall be delivered to the COR the following business day.

16.1.2. When using Standard Form 1034, Public Voucher for Purchases and Services Other Than Personal, the inclusive dates of delivery of services must only be for the period for which the incurred costs are being claimed.

16.1.3. These invoice requirements are in addition to, not in place of, any invoice submission instructions provided by the CO at the time of award.

17. Auditing

The United States Government, DHS and U.S. Immigration and Customs Enforcement reserves the right to audit the contractor’s equipment, tool and/or platform, as well as any equipment provided by the United States Government to the contractor for the purposes of ensuring the contract is being performed in a manner that is consistent with the contract, with Privacy regulations, and any other regulation enforced by the United States Government. This can include allegations made against contract employees and the contractor in the performance of this contract. The timing and frequency

of these audits will be determined by the United States Government, DHS and U.S. Immigration and Customs Enforcement, but will more than likely occur on a monthly, quarterly and yearly basis.

18. Acronym List

CO	Contracting Officer
COR	Contracting Officer's Representative
DHS	Department of Homeland Security
HRI	High Risk Indicators
ICE	Immigration and Customs Enforcement
OPR	Office of Professional Responsibility
PSU	Personnel Security Unit
SME	Subject Matter Expert
SOO	Statement of Objectives
SOW	Statement of Work
POP	Period of Performance

19. Federal Law Enforcement Sensitive

The data provided or processed within the ICE Office of Professional Responsibility shall be considered federal law enforcement sensitive, and, therefore, cannot be used to solicit or benefit other work by the Contractor. All records received, created, used, and maintained by the Contractor for this effort shall be protected as sensitive data, in accordance with government laws, to include the Federal Acquisition Regulation (FAR), Part 24, Protection of Privacy and Freedom of Information, and shall be returned and provided to the government upon contract completion. All reports created by the vendor shall be labeled "Law Enforcement Sensitive" at the top and bottom of each page in red.

All data created for government use and delivered to or falling under the legal control of the government are federal records and shall be managed in accordance with records management legislation as codified at 44 U.S.C. Chapters 21, 29, 31, and 33, the Freedom of Information Act (5 U.S.C. 552), and the Privacy Act (5 U.S.C. 552a), and shall be scheduled for disposition in accordance with 36 CFR 1228.

All contractor employees for this effort will also be required to sign a nondisclosure statement, Acknowledgement and Agreement Handling Sensitive Government Data and Other Government Property, and are subject to the security requirements of the SOW/SOO. This form will be signed prior to beginning work for this effort.

20. Security Requirements (Updated October 2024)

20.1 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 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 Fitness determination by OPR PSD. Contract employees are processed under DHS Instruction 121-01-007-001, Revision 2, dated August 10, 2024, Personnel Security, Suitability and Fitness Program, dated June 14, 2017, 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 are nominated by a Contracting Officer Representative (COR) for consideration to support this contract via submission of the DHS Form 11000-25 and ICE Supplement to the DHS Form 11000-25 to the PSD. This contract shall submit the following security vetting documentation to OPR PSD, through the COR, within 10 days of notification of initiation of an Electronic Application (eAPP), or successor thereto, in the National Background Investigative Services (NBIS) automated on-line system:

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

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

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

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

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

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

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

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under 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 was favorably adjudicated within 5 years and not to exceed 7 years, meets the contract risk level requirement, and applicant has not had a break in service of more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01)

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

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

Only U.S. citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007-001. 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.

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

REQUIRED REPORTS

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

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

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

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

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

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

SECURITY MANAGEMENT

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

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

INFORMATION TECHNOLOGY SECURITY

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

Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, regardless 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 (ITS) or by contacting ICE.ADSEC@ice.dhs.gov. Contractor employees with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

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