Performance Work Statement

For

DHS-wide Background Investigative Services

February 26, 2021

CHANGE CONTROL LOG

VERSION	DATE	CHANGE
Initial Release	2/26/2021	Updates to Applicable Documents 5.24 and 5.25

Table of Contents

Performance Work Statement (PWS)

Background Investigative Services

1. BACKGROUND

The primary mission of the U.S. Department of Homeland Security (DHS) is to lead the unified national effort to secure the country and preserve our freedoms. The Department was created to secure our country against those who seek to disrupt the American way of life.

Components within the Department of Homeland Security (DHS), are responsible for: the protection of the security of the American people and homeland by vigilantly enforcing the nation's immigration and customs laws; protecting our Nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.; apprehending individuals attempting to enter the U.S. illegally; stemming the flow of drugs and other contraband; protecting our agricultural and economic interests from harmful pests and diseases; protecting American businesses from theft of their intellectual property; regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws.

DHS Component Personnel Security organizations promote public trust and confidence in this mission by ensuring organizational integrity is maintained through a multi-layered approach utilizing security inspections and investigations. The integrity and efficiency of the program is promoted by making risk-based decision in evaluating applicants, employees, and contractors in according with all Federal regulations, policies, and guidelines.

DHS Component Personnel Security organizations are responsible for overseeing the Personnel Security and Suitability program; to include managing background investigations to determine suitability and fitness for employment, and eligibility to occupy national security positions and access National Security Information (NSI).

This Performance Work Statement (PWS) establishes the scope of the requirement to procure non-personal services for conducting various background investigations resulting in Reports of Investigation (ROI) on Federal, Contractor, and State & Local applicants for suitability/fitness/eligibility determinations for employment, continued employment, and authorization to have access to NSI.

2. SCOPE

The contractor shall provide all personnel, materials, services, and other items necessary to perform non-personal services in support of processing personnel security actions for Entry-On-Duty (EOD), fitness determinations, suitability and/or eligibility for access to NSI. Specifically, adhering to established processes.

This requirement is to procure non-personal services for the conduct of background investigations culminating in the delivery of Reports of Investigation (ROIs) in support of

DHS. These investigations often involve details of an individual's life and must be conducted with tact and discretion. The collection, use, storage, and dissemination of information provided by the Government to the Contractor to facilitate the performance of work under this Blanket Purchase Agreement (BPA), as well as, information collected by the Contractor as part of the investigations performed under this BPA are designated For Official Use Only (FOUO) only and are governed by the Privacy Act of 1974. The location of services to be performed will be nationwide, including U.S. territories.

The requirements detailed in this Performance Work Statement (PWS) describe the work to be performed in direct support of the DHS investigation program. All costs associated with the resulting contract actions will be considered case based to include program management and administrative support services.

3. PLACE OF PERFORMANCE

The Contractor shall be capable of conducting investigative services with coverage in all fifty (50) states, and U.S. territories at their established contract rate for each investigation type; this includes Puerto Rico, the U.S. Virgin Islands, Mariana Islands, Guam, Commonwealths, and other U.S. Trust Territories and Outlying Areas. The contractor must be capable of conducting investigative leads in the various languages spoken in these areas.

3.1 Administrative Office

The Contractor shall provide and maintain an administrative office for the management and performance of all aspects of the BPA, other than field investigative work. The Contractor shall have designated areas within the Contractor's facility where DHS general and investigative case data is stored, processed, handled, or secured as "DHS cleared spaces." DHS cleared spaces must be segregated from non-DHS spaces and secured via access control measures (keycard, pin code, door locks, etc.). Only personnel that have been approved by DHS to handle and process DHS general and investigative work, with a favorably adjudicated Tier 5 (T5) investigation or equivalent, may have un-escorted access to DHS cleared spaces. The Contractor shall have its facility operational within thirty (30) calendar days after BPA award.

3.2 Off-Site Locations

Prior to Contractor staff working off-site, the Contractor must ensure that their policies and procedures include the safeguarding of DHS's documents and information. Positions and/or job titles designated to work off-site shall also be included in the policies and procedures.

DHS reserves the right to inspect any off-site location at any time without prior notification.

- Administrative Contractor Staff - May only process or handle DHS general and investigative data within DHS cleared spaces in the Contractor's facility, or at approved off-site locations, to include home offices.

- Contract Field Investigators - Not limited to DHS cleared spaces or approved off-site locations.

4. PERIOD OF PERFORMANCE

The period of performance for the BPAs shall be for five (5) years. In accordance with FAR

Part 8.405-3 (d) awarded BPAs may extend beyond the current term of their GSA Schedule contract, so long as there are option periods in their GSA Schedule contract that, if exercised, will cover the BPA's period of performance.

5. APPLICABLE DOCUMENTS

The following regulations and policies (or the specific parts noted) are applicable to this PWS; however, this list is not all-inclusive.

5.1 Title 50 United States Code (USC) 435b. Located at: https://www.govinfo.gov/content/pkg/USCODE-2009-title50/pdf/USCODE-2009-title50-chap15-subchapVI-sec435b.pdf

5.2 5 U.S.C. 552a Privacy Act of 1974. Located at: https://www.govinfo.gov/content/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf

5.3 Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011 or its successor. Located at: https://www.govinfo.gov/content/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf

5.4 Executive Order 13764, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters, January 17, 2017 or its successors, Located at https://www.govinfo.gov/content/pkg/FR-2017-01-23/pdf/2017-01623.pdf

5.5 Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, January 16, 2009 or its successors. Located at: https://www.govinfo.gov/content/pkg/WCPD-2009-01-19/pdf/WCPD-2009-01-19-Pg87.pdf

5.6 Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008, or its successor. Located at: https://fas.org/irp/offdocs/eo/eo-13467.htm

5.7 Executive Order 12333, United States Intelligence Activities, December 4, 1981, as amended, or its successor. Located at: https://www.archives.gov/federal-register/codification/executive-order/12333.html

5.8 Executive Order 12968, Access to Classified Information, August 2, 1995, as amended; or its successor. Located at: https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf

5.9 Executive Order 10577, Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service, November 23, 1954, as amended or its successor. Located at: https://www.archives.gov/federal-register/codification/executive-order/10577.html

5.10 Title 5 Code of Federal Regulations (CFR) Part 731, or its successor. Located at: https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title05/5cfr731_main_02.tpl

5.11 Title 5 CFR Part 1400, or its successors. Located at: https://www.ecfr.gov/cgi-bin/text-idx?SID=ea8d9b7f129b58c4b512ea9d68a44761&mc=true&node=pt5.3.1400&rgn=div5%23se5.3.1400_1201#sp5.3.1400.c

5.12 Public Law 108-458, *Intelligence Reform and Terrorism Prevention Act of 2004 and its successor documents.* Located at: https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf

5.13 U.S. Office of Personnel Management (OPM), Suitability Executive Agent & the Director of National Intelligence (DNI), Security Executive Agent, Federal Investigative Standards, December 2012, or its successor. Uploaded to SharePoint folder

5.14 Memorandum of Understanding between U.S. Office of Personnel Management and U.S. Department of Homeland Security for Delegated Investigative Authority dated 27 August 2020 or its successor.

5.15 Performance Accountability Council memorandum, Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards, December 6, 2012.

5.16 The July 2007 U.S. Office of Personnel Management's Investigator's Handbook, or its successor publication.

5.17 Department of Homeland Security (DHS) Handbook for Safeguarding Sensitive PII. Located at : https://www.dhs.gov/publication/dhs-handbook-safeguarding-sensitive-pii#

5.18 U.S. Office of Personnel Management, Guidance for Moving between OPM Investigative Products, dated November 21, 2011. Located at: https://www.dcsa.mil/Portals/91/Documents/pv/GovHRSec/FINs/FY12/fin-12-01.pdf

5.19 U.S. Office of Personnel Management Memorandum, Aligning OPM Investigative Levels with Reform Concepts, dated 24 August 2010. Located at: https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2010/aligning-opm-investigative-levels.pdf

5.20 18 USC 701 Official Badges, Identification Cards, Other Insignia *http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap33-sec701.pdf*

5.21 Federal Acquisition Regulation (FAR) *http://www.acquisition.gov/far/*

5.22 National Industrial Security Program Operating Manual (NISPOM) *http://www.fas.org/sgp/library/nispom.htm*

5.23 Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 et seq.

5.24 DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017, or most current version http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf

5.25 DHS 4300A Sensitive Systems Handbook, Version 12.0, November 15, 2015, or most current version https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook

5.26 CBP HB 1400-05D Information Systems Security Policies and Procedures Handbook is available only to current contractors supplying a quote for this solicitation via e-mail transmission. All other vendors must request a viewing of the document.

5.27 Critical Infrastructure Information Act of 2002 http://www.dhs.gov/xlibrary/assets/CII_Act.pdf

5.28 Federal Information Security Management Act (FISMA) https://www.dhs.gov/federal-information-security-management-act-fisma

5.29 49CFR Part 1520, Sensitive Security Information (SSI) http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=2f5eda45365c9204319d13e64defaf36&tpl=/ecfrbrowse/Title49/49cfr1520_main_02.tpl

5.30 Federal Information Processing Standard (FIPS) http://csrc.nist.gov/publications/PubsFIPS.html

5.31 OMB Circular A-130 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

5.32 50 U.S.C. 3341-Security Clearances

5.33 http://www.gpo.gov/fdsys/granule/USCODE-2009-title50/USCODE-2009-title50-chap15-subchapVI-sec435b/content-detail.html

5.34 DHS Management Directive 11042.1 (Safeguarding Sensitive but Unclassified Information) https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf

5.35 DHS Background Investigator's Report Writing Guide

6. GENERAL REQUIREMENTS

The Contractor shall perform non-personal services to deliver various types of background investigation reports on Federal, contract, and State & Local applicants and reinvestigation reports on existing personnel on a nationwide basis, including US territories and protectorates.

The Contractor shall be responsible for the appropriate scoping, scheduling and delivery of all required coverage elements for all investigation types (with the exception of Tier 1) in support of the following types of Background Investigations (BI) as identified by the President; the December 2012 Federal Investigative Standards (FIS), or successor thereto, the U.S. Office of Personnel Management (OPM) and/or the Director of National Intelligence (ODNI).

The Contractor is required to follow the DHS Background Investigator's Report Writing Guide and associated DHS Investigation Guidance Documents (hereinafter referred to as the Writing Guide), the July 23, 2007 version of the Office of Personnel Management (OPM) Investigator's Handbook or future versions (hereinafter referred to as the Handbook), and the 2012 ODNI Federal Investigative Standards (hereinafter referred to as the FIS) or future versions unless otherwise stated in this PWS. The Handbook is intended for use by all persons conducting investigations under the authority of OPM or its designee and is a controlled document. The Handbook is for only the Contractor personnel supporting this BPA, and not for further dissemination. Contractors shall be responsible for the control of this document. Any future updates to the Handbook and/or the FIS, will be provided to the Contractor(s) by the Government. Directions provided in the Writing Guide and Transmittals shall take precedence over information provided in the Handbook and the FIS.

Investigative types are subject to change as they will be superseded by the investigative requirements as defined in the Federal Investigative Standards (FIS) Tiered Investigative Model and the July 2007 OPM Investigator's Handbook, Chapter 3:

- Tier 5
- Tier 5R
- Tier 4
- Tier 4R
- Tier 3

- Tier 3R
- Tier 2
- Tier 2R
- Additional Lead Activity (ADL)

In 2018, The Director of National Intelligence (ODNI) National Counterintelligence and Security Center (NCSC), announced **Trusted Workforce 2.0** which establishes a new set of policy standards in its approach to vetting the workforce. With the establishment of Workforce 2.0 the investigative requirements are subject to change.

6.1. Delivery types may apply to any investigation type listed in this PWS:

- Expedited Delivery = 14 days
- Standard Delivery = 35 days
- Extended Delivery = 60 days

6.2. Additional requirements consist of the following:

- Upgrade
  The Government reserves the right to upgrade any investigation within one (1) year of the initial transmission of the completed ROI. If a Component upgrades a previously scheduled and completed investigation, the Contractor will only be allowed to bill for the difference between the original case price and the current price for the upgraded case type.

- Reopen
  The Government reserves the right to reopen any investigation within one (1) year of the initial transmission of the completed ROI. The Contractor cannot invoice at a cost greater than the case price in which the ROI was originally scheduled. If the Component requests that an investigation be reopened for developed information the Contractor could not have reasonably discovered during the course of their investigation, the Component will identify the required leads and pay the Contractor the agreed Additional Lead (ADL) price.

- Additional Lead Activity (ADL)
  Additional lead activity shall be performed at the written request of the Component COR and/or Component POC when the Government determines that additional information is required in order to complete the adjudication of the ROI.

    - ADL - Individual Subject Interview
    - ADL - Individual Subject Re-Contact
    - ADL - Individual Telephonic Subject Re-Contact
    - ADL - Individual Source Interview
    - ADL - Individual Telephonic Source Interview
    - ADL - Individual Record Check
    - ADL - Individual Telephonic/Fax/Online Record Check

7. SPECIFIC REQUIREMENTS

7.1 Case Assignment

Assignment of a case to the Contractor is considered to have occurred when the following information; at minimum, is received:

- Case number
- Subject Information
- Investigation Type
- Delivery Type
- Date of Last Investigation (Reinvestigations Only)
- Case Materials

7.1.1 Transmitting Case Materials to Contractor:

a) Secure Transmission of Documents
Documents are delivered electronically via the contractor's established Secure Internet Portal (SIP).

b) Secure Email Transmission of Documents
If required for contingency purposes, documents will be delivered electronically via secured email, with the attached documents password protected and in accordance with Section 13.2.2.

7.1.2 The day the transmission of the documents occurs would be considered Day 0 for the purpose of calculating due dates specified by the delivery types (See Section 7.5.1)

7.1.3 Delivery instructions for case materials will be provided upon issuance of each Component's Call/ Task Order.

7.2 Conducting Investigations and Investigative Requirements

The Contractor shall only complete the items required for the specific background investigation type in accordance with the current federal investigation standards and any successors thereto.

7.2.1 Initial Contact

Contractor Personnel must make an attempt to contact the subject of the investigation within 3 business days from the vendor receive date (See Section 7.5.1):

a) Proof of these attempts should be maintained by the Contractor and available to the Component upon request.

b) The initial contact will provide the following:

- Notify Subject that their background investigation has been assigned to (provide name of Contract Field Investigator (CFI) telephone number and Investigator's credential number) and they should expect a telephone call for the purpose of scheduling an interview.

- Determine any change in the Subject's current residence or employment.
- Establish Subject's status as an applicant or employee.
- Provide instructions to contact the CFI in the event he/she should withdraw from employment consideration, resign or be terminated, prior to the interview taking place.

c) Subjects will not be queried regarding investigative issues during initial contact.

7.2.2 Records Checks

Centralized automated systems or databases used to conduct record checks in lieu of direct sources may only be used to satisfy investigative requirements if listed in the OPM Handbook, or if the Contractor has obtained pre-approval by the Component. In all instances, an in-person contact must be attempted before conducting other contact means or using an online alternative.

a) Originating Reporting Identifier (ORI)

An ORI number is provided to each vendor solely for use under this BPA in order to conduct Local Agency Checks (LACs) and shall not be considered the property of the Contractor, shall not be used for any purpose other than the conduct of investigation tasked to the Contractor under this BPA, and the Contractor shall cease and desist in the use of the ORI number at any time when instructed to do so by the Contracting Officer, DHS COR or at the end or termination of the BPA.

7.2.3 Leads

a) Inquiry Leads

Guidelines for completing inquiry leads are as defined in the OPM Handbook, 2.1.3.11. If no response to an inquiry is received, the Contractor is to attempt to conduct Personal Coverage or a Records Check to obtain coverage from the same source.

b) Overseas Leads

The Contractor is to conduct collateral verification of the overseas activity as directed in the Writing guide and OPM Handbook. The contact information for developed overseas leads does not need to be provided in advance and can be reported in the ROI.

An overseas source that cannot be identified as required, does not require notification to the Component but shall be documented in the final ROI as directed by the OPM Handbook. Investigators must attempt collateral verification of overseas leads through stateside records and reference interviews. The ROIs must reflect efforts to verify overseas activities.

c) Incomplete Leads

If coverage of an investigation is not complete for any reason, the ROI will provide a detailed explanation of all attempts to fulfill the coverage requirement. This reporting requirement includes unsuccessful attempts for all scoped and developed leads and does not waive the requirement to obtain or verify the lead through other sources.

7.2.4 Subject Interview

a) In-Person Interviews

All Subject interviews (initial and re-contact) conducted throughout the investigative process will be conducted in-person and in a private and professional setting such as office space, a public library or police station, not in a public space, such as a restaurant or coffee house.

Subject interviews of current DHS employees shall be conducted at the Employee's work site unless otherwise approved by a COR and/or the Component POC. Investigators shall inform employees to make his/her Supervisor aware of the interview and request the employee secure a private space for the interview.

Subject interviews will not be conducted at residences without prior permission from the Component and are on a case by case basis.

b) Telephonic Interviews

In the rare occurrence that the Subject interview cannot be made in-person, the contractor can conduct a telephonic interview; however, it requires pre-approval by the Component.

All investigators are cautioned regarding inappropriate use of the telephone to conduct investigative leads. An Investigator's Note must be included in the ROI indicating the interview was conducted telephonically.

For all investigations, interviews may be conducted telephonically as outlined in Section 7.2.5 of this PWS and does not require approval by the Component.

c) Developed Derogatory

If any issue(s) or derogatory information is developed/encountered at any point during the Subject Interview, the Investigator will establish the reason the Subject failed to provide that information on the security forms or during the interview and will obtain all details and resolve all discrepancies and inconsistencies regarding the issue.

If any issue or derogatory information is developed at any point during the conduct of an investigation, the investigator will establish the reason the subject failed to provide that information on the security forms or during the interview.

The Investigator will obtain all details and resolve all discrepancies and inconsistencies regarding issues.

Telephonic contact with the Subject to resolve issues is prohibited. The investigator shall schedule an in-person Re-Contact Interview to obtain information from the Subject to resolve the issue(s). In the rare occurrence that re-contact with the Subject cannot be made in-person, the Contractor must contact the COR and/or the component POC to request approval prior to conducting the Subject re-contact telephonically. The investigator must include an Investigator's Note detailing the telephonic contact.

7.2.5 Source Interview

a) In-person Source Interview

Source interviews (initial and re-contact) conducted throughout the investigative process should be conducted in-person and in a private and professional setting such as office space, a public library or police station, not in a public space, such as a restaurant or coffee house.

b) Telephonic Source

In order for a personal source testimony to be obtained via telephone, the case must be favorable or only contain minor issues; with "minor issues" defined as any issue that does not trigger the requirements of a flag, as described in the Expandable Focus Investigation (EFI) model of the Federal Investigative Standards (FIS).

Once the Contractor determines the case is favorable or only contains minor issues, a source telephone testimony may be conducted when one of the following conditions are present:

- The source interview requires significant travel to accomplish (remoteness).
- The item is for a single source testimony and there is no other pending work in that location.
- The source is the last field item pending on the case.
- The source is located in a different geographical area and the interview must be re-assigned to another field office.

If a testimony is obtained via telephone the ROI must include a corresponding Investigator's Note to explain the reason for the telephonic interview, clearly indicating which criterion listed above was met on the case.

c) Developed Derogatory

If any issue(s) or derogatory information is developed/encountered at any point during the investigation, the CFI will establish the reason the Subject failed to provide that information on the security forms or during the interview and will obtain all details and resolve all discrepancies and inconsistencies regarding the issue.

The Contractor shall provide a written report of all serious derogatory or significant information obtained during the course of a background investigation to the Component COR and/or Component POC within 24 hours of discovery. Serious derogatory or significant information is considered to be that, which may warrant cancellation, discontinuance or delay of an investigation, (i.e.: Subject's death; Subject is no longer interested in employment; a recent arrest; incarceration; Subject's unavailability as a result of hospitalization and /or recovery period). This report must be electronic and include the Subject's full name, assigned case number and a brief description of the date discovered, significant or derogatory information, and source of the information.

7.2.6 Interpretive Services

In the event a Subject or Source requires interpretive services to complete a lead, the Contractor is responsible for securing and paying for the required services. The interpreter must be certified to perform the required services.

7.2.7 Investigator Case Notes

Investigator Case Notes must be retained with all other case related documents. The use of a standardized Case Note Sheet (CNS) for each Contractor is required and must be utilized by all Contract Field Investigators (CFI) and Contract Investigative Technicians (CIT) that conduct a lead or write-off an attempted lead for cases.

a) Each CNS must include at a minimum the following information:

- Lead Type
- Case Number
- Subject's Full Name
- Investigator Credential Number
- Date Lead Conduct (or attempted for write-offs)
- Method Lead Conducted
- Evidence of Privacy Act (PA)/Unsworn Declaration/Recommendation Provided
- Name/Title/Contact Info for Reference or Record Provider to include email address
- Name of Agency/Company/Educational Institution where lead was conducted

At a minimum, the CNS must be used as a cover sheet for the written notes taken by the Investigator. The CNS can be used by CFIs and CITs as their case

notes if there is sufficient space for handwritten notes taken during interviews or record checks.

b) All pages of case notes following the CNS for a completed or written-off lead must include the following information:

- Case Number
- Date Lead Conducted
- Subject's Last Name
- Investigator's Credential Number
- Lead Type/Last Name of Reference or Name of Record Check Agency
- All Pages numbered (beginning with the CNS) for example (1 of 4, 2 of 4, 3 of 4, and 4 of 4)

If the Investigation is based on a SF-85P - A notation must be made on the CNS as to whether a source recommends the Subject for a "Position of Trust" with the U.S. Government.

If the Investigation is based on a SF-86 - A notation must be made on the CNS as to whether a source recommends the Subject for a "Position impacting National Security" with the U.S. Government.

Contractor shall not consolidate investigative information from multiple Subjects or sources on the same page of notes. Notes for all applicable sources, must be legible and maintained by Case Number and last name of the Subject. Investigator notes shall remain available for retrieval/inspection and maintained in a safe, secure manner, not accessible to any individual who does not have a need-to-know. Upon case completion, investigators are to forward all case papers to the Contractor.

7.3 Report of Investigation

The investigation will culminate in a Report of Investigation (ROI) that shall be prepared in accordance with the Writing Guide, Investigator's Handbook and Transmittals.

7.3.1 Complete ROIs:

a) The Contractor shall prepare each ROI in typewritten form with the proper syntax and shall be generally free of any typographical errors.

b) The Contractor shall utilize an approved high-impact writing style.

c) The Contractor shall include all items completed by the CFIs and CITs during the course of the investigation in the completed ROI.

d) The Contractor shall include with the completed ROI all adjudicatively significant supporting documentation (e.g., bankruptcy papers, dismissals from employment, credit report, police records, court documents, proof of

citizenship, etc.). In the event the Contractor is unable to obtain such documents, the ROI shall contain a statement to this affect and reason(s).

e) The Investigator's Handbook will be used as the basis for report writing; however, direction provided by the Writing Guide, which addresses new and different topics and expands upon the Handbook. If guidance is required, the DHS COR will provide final direction.

f) The Contractor will have thirty (30) days to implement any new forms/formats to the ROI. All revised forms/formats must be approved in advance by the DHS COR.

7.3.2 Deficient ROIs

a) A deficient ROI is a report that does not fully address the current investigative requirements outlined in the Investigator's Handbook and in the Federal Investigative Standards (FIS) or its successors thereto.

b) Inspection of the ROI shall be performed by the Component within **365 days** of receipt from the Contractor. The Component will review investigations completed by the Contractor for quality. The Components' review effort will range from a sampling to a 100% review of all transmitted cases.

c) If the ROI does not meet the investigative requirements outlined in the Investigator's Handbook and/or the FIS, it will be rejected.

d) Some reasons include, but are not limited to the following:

- Scope of ROI does not provide appropriate coverage for the investigative type.
- Evidence and supporting documentation have not been provided to support ROI.
- References have not been checked, both those provided by the subject and those developed through other leads.
- Developed Issues that were not previously revealed by the subject have not been researched and investigated.
- Listed Issues that have not been investigated and fully resolved.
- Closure of issues has not been completed, providing corroboration that an issue of concern either does or does not exist.
- Use of centralized index databases or other than in person records, without prior approval of the component POC.

- If the deficiency is found after the 365th day retention period, the Government will provide the vendor with all required documentation.

e) The Government reserves the right to require the Contractor to correct deficient ROIs.

f) The Government reserves the right to require the Contractor to re-conduct investigative leads when other factors in the investigation indicate that additional information should have been obtained and/or investigative issues are not fully resolved.

g) The Government will notify the Contractor via email of the deficient area(s). Corrected/updated copies will be furnished at no additional expense to the Government. The Contractor shall put forth its best effort to resolve issues and deliver such ROIs within five (5) business days.

7.3.3 Deficient ROI Resolution

In the event the Government identifies a deficient ROI the following can be provided to resolve the deficiency(s):

a) Information found within the investigator notes, (and does not require additional investigative effort), a corrected ROI in its entirety will need to be submitted.

b) Requires additional record reviews, a re-contact of reference(s) or a re-contact of Subject, a supplemental ROI containing only the missing or additional information will be submitted to the component (the reason that the new investigative effort was expended will be reflected in the ROI).

7.3.4 Contractor Dispute of Deficient ROI

When the Contractor disputes a deficient ROI, a rebuttal must be submitted via e-mail to the Component COR and/or POC for review. The rebuttal must specifically stipulate why the vendor believes the ROI is not deficient. The Component will review and consider the rebuttal and make a final determination. The Contractor will be notified of the final decision via e-mail. The Component will be the final authority in determining that investigative products are sufficient to meet standards.

7.3.5 Deficient ROI Ratings

The following rating scale for the quality of the ROIs will be used based upon the sampling of cases reviewed by the Components:

Rating	Percentage of Cases Reviewed Determined to be Deficient
Satisfactory	1-5%
Marginal	5.1-6.5%

Unsatisfactory	6.6% or greater

Note: The ratings above may be utilized by Components for future workload distribution and/ or award of Calls/ Task Orders.

7.4 Delivery of ROIs

The required method of delivery of completed ROIs to the Component is via electronic delivery (E-Delivery). The method will differ for each Component and will be specified at the Calls/ Task Order level. Components may have different systems and the contractor is required to ensure that E-Delivery works with each of the individual systems. Also, e-Delivery must work with Integrated Security Management System (ISMS).

In order to connect to the DHS network, an Interconnection Security Agreement (ISA) will be completed between the Component and the Contractor. An ISA must be approved and implemented before any casework will be assigned to the Contractor by the Component.

7.4.1 Electronic ROI Delivery (E-Delivery):

a) Delivery Time to DHS-ISMS: DHS, which maintains control over ISMS, will establish a time frame, referred to as "the upload window," for the upload of completed ROIs to be delivered to the Government.

b) Every day shall be considered a calendar day.

c) Received Date:
The date utilized as the delivery date will be the date associated with the start of the upload window established by DHS.

- Example: For Monday-Thursday due dates, if the completed ROI is uploaded by the Contractor into ISMS anytime during the 11:00 pm to 4:30 am Eastern upload window, the ROI will be considered delivered as of the date upon which the upload window began.

- Example: For Friday due dates, if the completed ROI is uploaded by the Contractor into ISMS anytime between 11:00 pm Friday and 4:30 am Monday, the ROI will be considered delivered on Friday, at the start of the upload window.

d) Network Outages:
DHS-network outages are outside the control of the Contractor. All ROIs affected by such outages will be treated as delivered on the date associated with the start of an upload, so long as an upload was attempted and failed.

Additionally, late delivery disincentives will not be applied to ROIs which would have been considered to be timely deliveries at the time the upload began.

- The Government shall notify the Contractor of any planned DHS-network outages.

- The Contractor remains responsible for any delivery delays resulting from network outages or issues on the Contractor's side.

- Upload Errors: In the event of an E-Delivery upload rejection by ISMS, based on an administrative error by either the Government or Contractor, a delivery date shall be determined by coordination between the Component COR and Contractor. The final decision is at the sole discretion of the Component COR.

7.4.2 Mailed/Hand Delivered ROI (NETWORK OUTAGES ONLY)

Delivery of a hard copy or CD ROI to the Government is considered to have occurred when the Government takes possession of the ROI.

When closed/completed ROIs are delivered in hard copy, delivery to the Government is based on the UPS/FedEx (or other delivery method) delivery date.

When delivered in CD, each ROI shall be encrypted via 12-character password including uppercase, lowercase, number, and special character. No SPII (such as social security numbers) shall be used as the password. All CD deliveries of ROIs shall include a manifest inside the package listing the contents by case numbers within each shipment. This requirement is in addition to the emailed manifest requirement below.

All hard copy deliveries of ROIs shall include a manifest inside the package listing the contents by case numbers within each shipment. This requirement is in addition to the emailed manifest requirement below.

When delivered in hard copy, the original and all supporting documentation shall be transmitted:

a) Mailing Documents

The preferred method of transmission for all case material is electronic. In the event other means must be utilized to transmit case material, the Contractor shall incur all costs associated with the delivery and receipt of all case materials. The method(s) of delivery shall be approved by the Component prior to implementation or change. Any courier service used must be bonded.

The Contractor shall take precautions to ensure that incoming and outgoing mail and FOUO material are not easily accessible to persons other than those authorized to perform work under this BPA.

Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and

addressee. The sender will double wrap PII when sending it through the mail. The material will be sealed in an envelope, addressed to the authorized recipient, and marked as "FOUO – Privacy Sensitive", and then placed in a second sealed, unmarked envelope addressed to the authorized recipient. For Official Use Only (FOUO) materials may be mailed by U.S. Postal Service First Class (certified) or Priority Mail (with delivery confirmation) or a commercial delivery service such as FedEx or United Parcel Service, pre-approved by the Component.

b) Hand-Delivered Documents

All FOUO material hand carried must be in a sealed envelope or sealed container, i.e., folder, portfolio, and precautions must be taken so the material is not accessible to persons other than authorized Contractor personnel.

7.5 Performance and Pricing

7.5.1 Calculation of Due Dates

Due dates shall be calculated by considering the date of E-Delivery to the Contractor as "Day 0", examples are as follows:

Calculation of Due Dates				
Case Type	Days	Day 0 (E-Delivery)	Day 1	Due Date
Expedited	14	Monday 4/13/20	Tuesday 4/14/20	Tuesday 4/28/20
Standard	35	Monday 4/13/20	Tuesday 4/14/20	Tuesday 5/19/20
Extended	60	Monday 4/13/20	Tuesday 4/14/20	*Monday 6/15/20
Case Type	Days	Day 0 (E-Delivery)	Day 1	Due Date
Expedited	14	Friday 4/10/20	Monday 4/13/20	Monday 4/27/20
Standard	35	Friday 4/10/20	Monday 4/13/20	Monday 5/18/20
Extended	60	Friday 4/10/20	Monday 4/13/20	Friday 6/12/20

Note: If Day 0 falls on a Friday, Day 1 will be the following Monday. If the ROI due date falls on a weekend or holiday it is due the next business day.

7.5.2 Incentives & Disincentives

Unless otherwise waived by the Government, the Contractor shall apply the appropriate percentage based on the delivery timeframe established for a specific delivery type.

a) Incentives:

- ROI's delivered within the specified incentive timeframe for each delivery type are eligible for an incentive.
- A deficient ROI is not eligible to incur any incentives. If the case was previously invoiced and incurred an incentive, the Contractor will credit the amount of the incentive on the next invoice.

b) Disincentives:

- ROI's delivered outside of specified timeframe for each delivery type shall incur a disincentive.

Incentive/Disincentive Table				
Delivery Type	**Delivered on day 1-10**	**Delivered on day 11-14**	**Delivered on day 15-20**	**Delivered after day 21**
Expedited Delivery 14 Days	Base Price + 10% incentive	Base Price	Base Price – 10% disincentive	Base Price – 25% disincentive
Delivery Type	**Delivered on day 1-25**	**Delivered on day 26 -35**	**Delivered on day 36 -45**	**Delivered after day 46**
Standard Delivery 35 Days	Base Price + 10% incentive	Base Price	Base Price – 10% disincentive	Base Price – 25% disincentive
Delivery Type	**Delivered on day 1-50**	**Delivered on day 51 -60**	**Delivered on Day 61 - 75**	**Delivered after day 76**
Extended Delivery 60 Days	Base Price + 10% incentive	Base Price	Base Price – 10% disincentive	Base Price – 25% disincentive

7.5.3 Notification of Late Delivery:

a) When the Contractor anticipates late delivery of any ROI, the Contractor shall provide the Component COR individual notifications stating the reason for delay and anticipated (revised) delivery date. Notifications shall be provided electronically, as soon as the Contractor becomes aware of an anticipated late delivery and before the Government's due date. This notification requirement applies whether or not the Contractor intends to request a waiver of the disincentive for late delivery.

b) ROI's delivered after the specified due date in accordance with Section 7.5.1, above shall be considered late. The Government has established the above disincentives to be applied to the late delivery of a ROI.

7.5.4 Untimely ROI Ratings

The following rating scale for the timeliness of the ROIs will be used based upon the

sampling of cases reviewed by the Components:

Rating	Percentage of Cases Reviewed Determined to be Timely
Satisfactory	1-25%
Marginal	25.1-50%
Unsatisfactory	50.1% or greater

Note: The ratings above may be utilized by Components for future workload distribution and/ or award of Calls/ Task Orders.

7.5.5 Waivers

During the course of the investigation, issues may be developed or encountered that are out of the contractor's control that will prohibit the Contractor from finalizing the ROI within the base price time frame. The Contractor may ask the Component COR to grant a waiver of disincentive.

For example, the subject of the investigation is unavailable for an extended period of time (i.e., maternity leave, serious medical condition, military deployment, etc.) or a natural disaster has occurred in a particular area (Hurricane Katrina), etc.

The COR will review the request and advise the Contractor whether it meets the requirements for an acceptable delay and will either grant or deny the waiver. A heavy workload area, delay in scoping and/or scheduling to the field is not an acceptable reason to request a waiver.

a) Waiver requests shall be submitted electronically to the COR in the following format:

Waiver Request			
Case Number:	ICE20-011005-XYZ	Subject's Name:	Doe
Case Type:	T5	App/Emp/Con:	Employee
Date Received:	2/28/2020	Agency Due Date:	4/2/2020
3 Day Contact:	2/28/2020	SI Completed:	N/A
ETA:	08/15/2020		
Summary:	SUBJECT was contacted this date and notified of the investigation. However, SUBJECT advised he is currently overseas in Japan with Military CIS and will not return stateside until July 2020. Based on this information, may a waiver of disincentive be granted?		

b) Waiver requests must meet the following guidelines:

- Waiver requests will only be granted if the 3-day contact requirement has been met. (See Section 7.2.1)
- If the Contractor anticipates circumstances continue to exist that would prevent delivery by the revised delivery date, they shall provide new justification and delivery date.
- Waivers requested after the initial delivery dates will not be approved.
- Approval of a waiver by the COR merely waives the Government's right to impose a disincentive percentage for ROIs that are delivered late. The responsibility still falls under the Contractor to provide a completed ROI.
- When a waiver is granted, the Contractor remains responsible for putting forth its best effort to deliver the ROI as expeditiously as possible following resolution of the matter that prevented a timely delivery.
- By requesting a waiver both disincentive and incentive are voided for that ROI.

7.5.6 Cancellation of Investigations

The Government reserves the right to cancel/discontinue any investigation at any time; however, the Contractor shall not cancel/discontinue an investigation or modify the type of investigation to be performed without explicit directions to do so from the COR.

a) Cancellation Request

If information is developed indicating that the investigation may need to be cancelled, the Contractor shall provide the information in the following format to the Component COR within twenty-four (24) hours:

Cancellation Request			
Case Number:	CBP20-001105-XYZ	Subject's Name:	Doe
Case Type:	T4	App/Emp/Con:	Contractor
Date Received:	1/27/2020	Agency Due Date:	3/27/2020
3-Day Contact:	1/30/2020	SI Completed:	N/A
Summary:	On February 24, 2020, Investigator Smith spoke to Subject to set up Subject Interview and Subject said he was no longer interested being investigated. Subject has not responded to Investigator Smith's request for a cancellation letter.		

b) Cancellation Pricing

Pricing for the cancellation of investigations is based upon the date the Contractor

was instructed by the Government to cancel.

Cancellations which occur after a case is already late will be paid using the pricing for Late Delivery as indicated in Section 7.5.2 Incentives & Disincentives.

c) Any time a cancellation occurs, and the ROI has been completed prior to the cancellation notice, 100% of the delivery base price will be authorized. In those instances, the completed ROI must be delivered to the government within 24 hours.

Cancellation Table			
Delivery Type	**Cancelled on day 1-3**	**Cancelled on day 4-9**	**Cancelled after day 10**
Expedited Delivery 14 Days	5% of Base Price	50% of Base Price	100% of Base Price
Delivery Type	**Cancelled on day 1-5**	**Cancelled on day 06-29**	**Cancelled after day 30**
Standard Delivery 35 Days	5% of Base Price	50% of Base Price	100% of Base Price
Delivery Type	**Cancelled on day 1-10**	**Cancelled on day 11-49**	**Cancelled after day 50**
Extended Delivery 60 Days	5% of Base Price	50% of Base Price	100% of Base Price

7.5.7 Reopened Investigations

The component reserves the right to reopen any investigation within one (1) year after initial cancellation.

a) Calculation of number of days
In order to calculate the total number of days, add the number of days the Contractor performed work on the initial investigation; and the number of days that work was performed after the investigation was reopened.

b) Below example is for a 35-Day Case:

Original Investigation (Number of days the Contractor preformed work before cancelled)	Reopened Investigation (Additional days of work performed after being reopened)	Total number of days worked
30	15	45

c) Pricing of Reopened Investigations
The total numbers of days required to complete and submit the investigation to the component will be utilized for pricing purposes.
Incentives and disincentives will apply to reopened cases as they do for regular investigations.

The DHS component will not pay the Contractor more than the base case price plus incentive for any reopened investigation.

7.5.8 Records Management

Information in which the collection, storage, use, or disclosure of is governed by the Privacy Act of 1974 (5 U.S.C. 552a), shall be treated in the same manner as FOUO information.

a) Records Retention

All documents associated with casework (to include case notes) must be retained for 365 days from the final date of delivery of the ROI to the Government or date of cancellation for cancelled cases. The 365-day retention will allow for audits to be conducted for purposes of quality control.

The Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.

The Contractor shall not create or maintain any records containing any Government Agency data that are not specifically tied to or authorized by the contract.

The Contractor may convert any paper notes into an electronic file once the case is closed if the Contractor can ensure all paper notes are in a readable/printable format and all documentation/notes are accounted for. Upon case completion, investigators are to forward all case papers to the Contractor (See 7.4.2 for mailing precautions).

The Contractor is prohibited from retaining Component case data and materials in excess of three hundred and sixty-five (365) days unless expressly requested to do so by the Component.

b) Destruction

After the required three hundred and sixty-five (365) day retention period, all case papers (electronic and paper) and investigator notes (electronic and paper) must be destroyed in accordance with National Industrial Security Program Operating Manual (DOD 5220.22-M, Feb 2006/ Incorporating Change 2, May 18, 2016) Chapter 5, Section 7 (Methods of Destruction),

Destruction of the ROI, all other materials and associated case notes, both electronic and hard copy must occur on day 366 (or the first business day thereafter) and be documented by and with certification of destruction that details the cases destroyed/deleted by case number and the official(s)/employee(s) responsible for the destruction/deletion. Certification shall be submitted to the Government with the Monthly Progress Report.

The Contractor is responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701, Destruction of documents, and must be IAW with NISPOM; Safeguarding of Sensitive Information (Mar 2015) and Information Technology Security and Privacy Training (Mar 2015) clauses. Additionally, various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether or not the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or Department employee or contractor.

As such, the Contractor shall have and provide upon request an information security protection plan commensurate with DHS 4300A Sensitive Systems Policy and the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Component, and on information systems used or operated Component, or by a contractor or other organization on behalf of the Component.

Destruction of FOUO material shall be accomplished by or in the presence of Contractor personnel authorized to perform work under this BPA. When destruction is accomplished by a subcontractor approved by the Contracting Officer, the FOUO material shall not be left unattended by the Contractor until it is destroyed, or control is assumed by authorized destruction facility personnel. All removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements. This effort does not involve information collected, stored, and disposed of which is classified above the FOUO level (i.e., CONFIDENTIAL, SECRET, TOP SECRET).

c) The information security protection plan will address but not be limited to:

- Accounting for the distribution, sharing, and copies of collected PII within the Contractor's facilities and IT environment(s), to ensure all PII is able to be located, identified, and destroyed.

- Retention and destruction practices of the collected PII for the minimum amount of time necessary to fulfill the purpose(s) identified or as required by this contract;

- Disposing of, destroying, erasing, and/or anonymizing the PII, regardless of the method of storage, in a manner that prevents loss, theft, misuse, or unauthorized access;

- Ensure secure deletion or destruction of PII (including originals, copies, backups and archived records) in accordance with DHS 4300A Sensitive Systems Policy.

8. TRANSITION

8.1 Transition Plan: Phase-In Period

The Phase-In period will begin upon BPA award and continue for a period of up to 6 months. The Transition Plan shall detail all information required by DHS and DHS Components as outlined in the PWS below.

There shall be no Background Investigation Services rendered during the phase-in period until the following transition activities are completed:

8.1.2 Transition Activities

Following notification of the BPA award, the Contractor shall undertake the necessary preparations for commencement of performance. These preparations include, but are in no way limited to, the following activities:

- Ensuring the vendor has the capability to electronically submit ROIs or case information.

  Vendors utilizing a case management system will ensure compliance with ITAR 4.5.3.5 – Security Review Terms and Conditions 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.

- Providing the ATO documentation, final Security Assessment Report (SAR), current remediation plan and Plan of Action and Milestone (POA&M) report and any other relevant documentation.

- Establishing communication procedures with Component/POC, identifying key transition issues/milestones and minimizing impacts on continuity of operations.

- Providing a list of all employees; CFIs and CITs (non-credentialed and credentialed) the Contractor intends to use to perform background investigative work under this contract. The list must include full name, social security number (SSN), date of birth (DOB), place of birth (POB), the date of their last favorably adjudicated (T5 level) background investigation.

- Prepare and submit training plans for review by the DHS Inspection POC prior to implementation. Training plans, at a minimum, must address the following:

  - OPM Handbook Review and Familiarization
  - FIS Review and Familiarization
  - National Training Standards promulgated by the Director of National Intelligence (ODNI)Field Mentoring, Field Evaluation, and Certification
  - Safeguarding PII and Appropriate Use of Email
  - Quality Control
  - IT Security Awareness Training
  - Privacy Training

- Provide resumes for all Key Personnel (see Section 9.2)

8.2 Transition Plan: Phase - Out Period

If the Contractor is unsuccessful in any subsequent Government solicitation for Background Investigations Services or the BPA is terminated for any reason, the Contractor shall, during the last month of this contract, provide all reasonable support to the Government and the successor contractor to ensure an orderly transition and minimize any impact on the mission.

The Contractor shall retain full responsibility for all Background Investigative Services ordered under their Calls/ Task Order(s).

The Contractor shall certify in writing the destruction (See Section 7.5.7) of all data and any other Government Furnished Information (GFI) at the request of the COR.

8.3 On-ramping

DHS reserves the right to on-ramp additional Contractors in support of this multi-award Blanket Purchase Agreement. Consideration for and the actual on ramping process shall take place prior to an ordering period, making newly added Contractors available for all fair opportunity competitions initiated at/after the commencement of the next ordering period.

The total number of Contractors supporting the multi-award BPA may fluctuate due to any number of reasons including, but not limited to:

a.) Competition levels on task orders, or
b.) Mergers and acquisitions, or
c.) Development and growth in investigator capacity, or
d.) The evolution of in-scope background investigative service processes and procedures

It is in the Government's best interest that there remain an adequate number of Contractors eligible to compete for task orders in order to consistently meet the Government's background investigation service requirements.

The CO, in collaboration with the COR, will determine whether it would be in the Government's best interest to initiate on-ramping procedures in an attempt to recognize additional Contractors, subject to the following conditions:

a.) A notice is published on GSA EBuy, and
b.) A solicitation is issued under current Federal procurement law, and
c.) The solicitation identifies the total anticipated number of new contracts that the CO and COR intend to award, and
d.) Any vendor that meets the eligibility requirements set forth in the solicitation may submit a proposal, and
e.) The award decision under the solicitation is based, in large part, upon the same evaluation factors as the original solicitation, with only revisions made to enhance the effectiveness and efficiencies of the source selection process, and
f.) An vendor's proposal shall meet all the minimum requirement criteria of the original solicitation

A best value determination shall be made in accordance with the established source selection guide in support of the initial awards associated with this requirement. The ordering period for any new awards shall commence at the time an ordering period starts and run concurrently with the existing ordering period for all other Contractors.

Any incumbent BPA contractor will not be required to, nor will they be eligible, TO re-compete for a contract award. The Government will not consider unsolicited proposals.

Newly awarded BPA contractors shall only be eligible to submit a proposal in response to any task order solicitation and receive calls/ task order awards with the same rights and obligations as any other contractor upon receipt of a BPA contract award and the commencement of the subsequent
ordering period with which they were on-ramped.

8.4 Off-ramping

The DHS CO reserves the unilateral right to off-ramp Contractors at any point during the awarded performance period based upon an analysis of the Contractors' performance history and an evaluation of the overall value and benefit to the Government. In making that determination, the CO may utilize performance surveys or CPARS. Contractors that are off-ramped shall be allowed to complete active calls/ task orders at the time of the off-ramping. Off-ramping does not remove or impede upon the Government's right to terminate the contract in accordance with the FAR. The DHS CO may take any other action which may be permitted under the terms and conditions of the awarded contract

9. PERSONNEL REQUIREMENTS

9.1 General

The Government reserves the right to review the qualifications of personnel working under this contract. It reserves the right to refuse to allow any person to perform under this

contract when the retention of the individual would not be in the best interest of the Government's operations or the performance of the contract.

Current Federal employees present a conflict of interest and are not eligible to perform work under this PWS.

All Contractor personnel with immediate family or a cohabitant (as defined in the Federal Investigative Standards) who are employed by DHS or a DHS component must disclose this fact to the Government when a request for approval to conduct work under this PWS is submitted to the DHS Credentialing POC and DHS COR for review and approval. This notification must include the government employee's name, the agency they are employed with, their title at this agency, and the nature of their relationship to the Contractor personnel. The DHS Credentialing POC and DHS COR will make a conflict of interest determination and provide a response to the Contractor. If there is a change in the government employee's employment status or relationship status at any time during the performance of this BPA, the Contractor personnel must notify the Program Manager (PM) within two (2) business days of this change. The PM must in turn notify the DHS COR and DHS Credentialing POC within two (2) business days of when they became aware of the change in status of the employment or relationship.

The Contractor will be responsible for all expenses incurred for initial and/or periodic investigations of its employees. The Contractor will also be responsible to ensure that all personnel maintain a current favorably adjudicated T5 or T5R background investigation at all times during work on this BPA. The only exception to this requirement is outlined in section 9.5 (Preliminary Approvals).

The Contractor must have at least one employee who holds a Top Secret clearance granted by Defense Counterintelligence and Security Agency (DCSA) available on an as needed basis. DHS Components will not grant security clearances to any Contractor personnel.

9.2 Key Personnel

All personnel positions specified below are considered Key Personnel positions because they are essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract, as appropriate:

- Program Manager
- Deputy Program Manager
- Quality Assurance Officer
- Investigative Training Coordinator

9.2.1 Key Personnel Removal/Replacement:

All requests for approval of changes hereunder must be in writing, via email, and provide a detailed explanation of circumstances necessitating the proposed change and to enable the CO and COR, to evaluate the qualifications of the new candidate.

A resume should accompany the request and will be submitted no less than fourteen (14) calendar days before the change becomes effective. An exception will be considered if the replacement is due to performance issues whereas the contractor may not be capable of providing such lead notice.

The Contractor shall submit sufficient information to support the proposed action. The Contractor shall include a written justification for replacement and provide the name and qualifications of any proposed personnel substitute(s).

All proposed substitutes shall meet the requirements of this PWS. The Contractor shall not remove or replace personnel until the Contracting Officer approves the change.

Resumes for individuals filling "Key Personnel" positions, and any subsequent replacement of vacating "Key Personnel", must be provided to the COR for review and approval prior to commencing work under the PWS.

9.2.2 Program Manager (PM)

The Contractor must designate a person as the PM for the DHS Background Investigation BPA, in writing, to the Contracting Officer and the COR.

a) PM Requirements:

- PM shall always be available to communicate directly with the CO or COR regarding the performance of the PWS and associated Call/ Task Order.
- Sufficient corporate authority to direct, execute and control the performance of all work required under this BPA.
- Act as the central point of contact with the Government for all program-wide technical issues.
- Represents the contractor at all post-award meetings
- Responsible for the overall coordination and implementation of the contract.
- Responsible for all issue resolution, program management, and other administrative support including providing comprehensive support for the contract.
- Ability to analyze problems to identify significant factors, gather pertinent data, and recognize solutions;
- Ability to plan and organize work;
- Ability to communicate effectively orally and in writing.

The Program Manager must meet both the minimum experience and education requirements for at least one of the options below:

Program Manager	
Experience	**Education**
Option #1	
At minimum: Have at least seven (7) years of combined personnel security and investigative experience at the state or federal level; In addition, at least seven (7) years of program management experience that demonstrates the ability to direct, execute, and control the performance of all work under this BPA;	**At minimum:** Bachelor's degree from an accredited college or university
Option #2	
At minimum: At least fourteen (14) years of combined personnel security and investigative experience at the state or federal level; In addition, at least ten (10) years of program management experience that demonstrates the ability to direct, execute, and control the performance of all work under this BPA;	**At minimum:** Associates Degree from an accredited college or university

9.2.3 Deputy Program Manager (DPM)

Contractor must designate a person as the DPM, in writing, to the Contracting Officer and the COR. The DPM shall be available to communicate directly with the CO or COR regarding the performance of the Call/ Task Order.

a) DPM Personnel Requirements:

- Act as the central point of contact with the Government for all Task Order level technical issues.
- Represents the contractor at all post-award meetings
- Responsible for the overall coordination and implementation of the Call/ Task Order.
- Ability to analyze problems to identify significant factors, gather pertinent data, and recognize solutions;

- Ability to plan and organize work;
- Ability to communicate effectively orally and in writing.

The Deputy Program Manager must meet both the minimum experience and education requirements for one of the options below:

Deputy Program Manager	
Experience	**Education**
Option #1	
At minimum: Have at least five (5) years of combined personnel security and investigative experience at the state or federal level; In addition, management experience that demonstrates the ability to direct, execute, and control the performance of all work under this BPA with detailed knowledge of daily operations;	**At minimum:** Bachelor's degree from an accredited college or university
Option #2	
At minimum: At least seven (7) years of combined personnel security and investigative experience at the state or federal level; In addition, management experience that demonstrates the ability to direct, execute, and control the performance of all work under this BPA with detailed knowledge of daily operations;	**At minimum:** Associates Degree from an accredited college or university

A waiver for the experience and education requirements of the DPM could be provided to the Component CO/COR regarding a specific Call/Task Order.

9.2.4 Quality Assurance Officer (QAO)

The Contractor must designate a person for the QAO for the DHS Background Investigation BPA. The QAO is responsible for implementing the requirements of the DHS Quality Control Contact Program, ensuring the two-tier review of investigations is accomplished to meet Federal Investigative Standards and DHS guidance (Section 5.0), and administering the overall Quality Control Program.

It is preferred, though not required, that the QAO have a background in integrity, compliance, and ethics related to personnel security.

a) QAO Personnel Requirements:

- Demonstrate knowledge of background investigations policies and procedures,
- Experience in Project/Process Management, to include successful coordination of a project from concept to implementation and controls,
- Knowledge of metrics as a performance driver and trend indicator,
- Quality Assurance experience to include understanding of competitive landscape, industry best practices, products and systems, and analytics to drive operational excellence.

Quality Assurance Officer (QAO)	
Experience	**Education**
At minimum: Six (6) or more years of experience in the personnel security investigations or background investigations industry	**At minimum:** Bachelor's degree from an accredited college or university

9.2.5 Investigative Training Coordinator (ITC)

The Contractor must designate a person as the ITC for the DHS Background Investigation BPA. The purpose of the ITC includes, but is not limited to:

a) ITC Personnel Requirements:

- Establishing/maintaining CFI/CIT personnel training in support of the Component's BI program;
- Demonstrate knowledge of background investigations policies and procedures.
- Establish/maintain a program to train personnel who are involved in conducting investigations, scoping, assigning, controlling, reviewing, approving, and performing quality control and assurance functions;
- Providing investigators with guidance on investigative and ROI issues and maintaining quality standards;
- Providing advice and guidance to investigative and staff personnel on FIS and Component requirements.
- Plan, develop, and implement training programs and supplemental guidance for classroom or web-based instruction platforms concerning the conduct of background investigations.

Investigative Training Coordinator (ITC)

Experience	Education
At minimum: Six (6) or more years of experience in the personnel security investigations or background investigations field and demonstrate general knowledge of background investigations policies and procedures.	**At minimum:** Bachelor's degree from an accredited college or university

9.3 Non-Key "Investigative Personnel"

The term "Investigative Personnel" when used in this performance work statement, refers to both Contract Investigative Technicians (CIT) and Contract Field Investigator (CFI). Components will not incur costs, nor be responsible for initial or periodic reinvestigations of Contractor personnel.

Investigative personnel must have the following education, experience and training to perform in the labor categories designated:

- Contract Field Investigator (CFI)
- Contract Investigation Technician (CIT)

9.3.1 Contract Field Investigator (CFI) Qualifications/Experience: The contractor shall provide qualified Field Investigators in support of contract performance. The government reserves the right to require the contractor to provide verification and/or certify all CFI qualifications/experience within 24 hours upon request.

a) CFI Duties include:

- Conducting source/reference interviews (i.e., developed, listed, employment, education, medical, neighbor, cohabitant, ex-spouse, etc.) as required by the FIS.
- Conducting Subject Interviews to include executing release forms as applicable as required by the FIS.
- Producing clear, concise, unbiased, technically and factually accurate ROIs noting all information relevant to DHS reporting requirements.

Contract Field Investigator (CFI)	
Experience	**Education**
Option# 1	

At minimum: 3 years of general experience (i.e. military, local, state or federal law enforcement or investigative functions) within the last 5 years and Completion of "New Investigator" and DHS-Specific Training.	**At minimum:** High School diploma or equivalent
Option #2	
At minimum: 1 year of specialized Federal background investigative experience within the last five (5) years and DHS-Specific Training.	**At minimum:** High School diploma or equivalent
Option #3	
At minimum: Completion of "New Investigator" and DHS-Specific Training	**At minimum:** Bachelor's degree from an accredited college or university

a) Proof of experience and completion of training must be provided, upon request. All requirements must be met prior to the individual being issued credentials and performing investigative work under this BPA.

b) Upon issuance of DHS credential, the CFI must complete the Non-Disclosure Agreement, DHS Form 11000-6. A copy of the form must be retained by the Contractor.

9.3.2 Contractor Investigation Technician (CIT): The contractor shall provide qualified Contractor Investigation Technicians (CIT) in support of contract performance. The government reserves the right to require the contractor to provide verification and/or certify all CIT qualifications/experience within twenty-four (24) hours upon request.

a) CIT Duties include:

- Conducting record reviews
- Conducting interviews of record custodians as required to obtain information.

Contractor Investigation Technician (CIT)	
Experience	**Education**
Option #1	

At minimum: 3 years of general experience (i.e. military, local, state or federal law enforcement, investigative, or personnel security functions) within the last 5 years and DHS Specific training.	**At minimum:** High School diploma or equivalent
Option #2	
At minimum: 1 year of specialized experience as an administrative professional within the last 5 years and DHS Specific training.	**At minimum:** Associates degree from an accredited college or university

a) Upon issuance of DHS credential, the CIT must complete the Non-Disclosure Agreement, DHS Form 11000-6. A copy of the form must be retained by the Contractor.

9.4 Non-Investigative Personnel Approval Requirements

Non-investigative personnel supporting this BPA must have a current favorably adjudicated T5 or T5R investigation, the only exception applies to preliminary approvals as outlined in 9.5. Upon approval, non-investigative/non-credentialed personnel must complete the Non-Disclosure Agreement, DHS Form 11000-6. A copy of the form must be retained by the Contractor.

9.4.1 Upon final approval of a favorably adjudicated investigation the Contractor will provide the DHS Credentialing POC with the following for verification:

- Full name,
- Social Security Number (SSN),
- Date of Birth (DOB),
- Place of Birth (POB),
- Date and type of the last favorable background investigation,
- Brief job description.

a) Any new/rehire employee starting work on the BPA must meet the same requirements as above.

9.5 Preliminary Approvals

On a preliminary basis, CFI, CIT, and non-investigative/non-credentialed staff may be submitted for a pre-clear to start working in support of the BPA provided they are currently undergoing the required Background Investigation. The Contractor may submit a DHS credential request for CFIs, CITs and requests for non-investigative/non-credentialed

staff who have been granted an interim Secret National Security clearance where such interim clearance includes at a minimum:

- A verifiable open T5 background investigation not open in excess of 18 months or 545 days,
- A favorable review by Defense Counterintelligence and Security Agency (DCSA) of the CI candidate's SF-86 "Questionnaire for National Security Positions,"
- A completed favorable National Agency Check and
- A verifiable "Interim Secret" National Security clearance issued by DCSA.

9.5.1 All personnel submitted for DHS credentials under the pre-clear procedure must meet all other requirements to hold DHS credentials as described in this PWS (to include training, experience and field mentoring). Field Mentoring must be completed within ninety (90) days of pre-clear approval. Failure to complete the Field Mentoring process in a timely manner will result in the retrieval of the DHS credentials.

9.5.2 If the Contractor receives notification of derogatory information during the course of the background investigation, the DHS Credentialing POC must be notified within twenty-four (24) hours of the date that the Contractor receives notification of derogatory information. Failure to notify the DHS Credentialing POC of derogatory information in a timely manner may result in the suspension or removal of the Contractor's ability to utilize the pre-clear procedure.

9.5.3 Any individual that has not had a favorably adjudicated T5/T5R investigation within eighteen (18) months (545 days) will be required to return the credentials to the sponsoring Contract Company until a favorable adjudication has been made. Non-investigative/Non-credentialed staff will lose the ability to conduct work until a favorable adjudication has been made. It is the responsibility of the Contractor to track this information, and failure to track this eighteen (18) months (545 days) requirement in a timely manner may result in the Contractor not being able to submit candidates for approval using the pre-clear process.

9.5.4 Tracking of the final adjudication status (favorable or unfavorable) is the responsibility of the Contractor. The Contractor must notify the DHS Credentialing POC of final adjudication (favorable or unfavorable) within forty-eight (48) hours from the date that the Contractor receives the final adjudication date.

9.6 Training

9.6.1 The Contractor shall adhere to all applicable statutes, executive orders, regulations, policies, and supplemental guidance issued by the DHS COR.

9.6.2 The Contractor shall retain all supporting training documentation and make these records available to the Government within 24 hours upon request.

9.6.3 The Government will provide the training materials referenced below to the Contractor. The Contractor shall provide copies of employee training certificates at the request of the Government. Names of all personnel and their training completion dates shall be included in each monthly report.

a) All Personnel Required Training
The Contractor shall provide initial and annual refresher training as identified below for ALL personnel supporting this effort. Notification of all training shall be included in the monthly status report.

- Cyber Security Awareness Training (CSAT)
Contractor shall provide training for all employees and sub-Contractors that have access to Sensitive PII as well as the creation, use, dissemination and / or destruction of Sensitive PII, at the outset of the sub-Contractor's / employee's work on the contract and every year thereafter. The training shall include procedures on how to properly handle Sensitive PII, to include security requirements for transporting and transmission Sensitive PII information, reporting requirements for a suspected breach or loss of Sensitive PII information and the use and prohibitions of email for DHS background investigations. The Federal Information Security Management Act (FISMA) requires all individuals accessing Government information, regardless of their employment status, be they Federal or contract type employees, to take the annual CSAT course.

- All Contractor employees are required to take Privacy at DHS
Protecting Personal Information training course. These courses shall be obtained from the DHS Inspection POC. The Contractor shall maintain copies of certificates as a record of compliance.

- DHS Records Management Training
All Contractor employees are required to complete DHS Basic Records Management training course annually. The Contractor shall provide training to all personnel who will have access to paper or electronic records relating to the investigations or ROIs created under this BPA.

- NISPOM Training
The Contractor shall provide initial and annual refresher security training and briefings commensurate with their clearance level as required by National Industrial Security Program Operating Manual (DOD 5220.22-M, Feb 2006/ Incorporating Change 2, May 18, 2016) Chapter 3-1.

b) Contract Field Investigator (CFI) and Contract Investigation Technician (CIT) Specific Training

The Contractor shall provide training for all Field Investigators (CFIs and CITs) and ensure all training is conducted in compliance with the National Training Standards-Background Investigator Training Standards and must provide documentation attesting that all FIs proposed to perform work under the contract have met the training requirements prior to performing any work under this contract and subsequently attest to any refresher training throughout the period of performance.

The Contractor shall also provide all Background Investigators with forty (40) hours of approved DHS specific training, which may include training on the following:

- Writing Guide (including high impact writing)
- Report of Investigations (ROI) template
- Instruction for Interview of Subject

Contractor training courses will comply with the Background Investigator Skill Standards and Core Competencies promulgated with the ODNI/OPM Memo "*Approval and Implementation of Performance Accountability Council Background Investigator Training Schedule*", dated August 20, 2012.

Contractors must demonstrate that the content and methodology of any training for background investigators supports compliance with the Skill Standards and Core competencies. Contractors must ensure that the basic background investigator training (New Investigator Training) includes a portion of this training to be conducted in-person to allow for the observations of background investigators' interview techniques for interviewing both Subjects and Sources of investigations.

Certify background investigators based on actual demonstrated field skills (e.g., ability to independently conduct records checks, reference interview, Subject interview) and not merely by a set hourly requirement.

Satisfy certification in critical investigative elements by field training officers/mentors/officials/etc.

Always requires final approval of field mentoring certification by the DHS Credentialing POC.

The Contractor is responsible for the appropriate vetting, training and certification of all CFI's, CITs and the collateral personnel involved in any critical function of

the background investigation process. This includes personnel conducting review, analysis, compilation, scoping, scheduling, quality assessment or integrity assessment of the CFI's work product.

Contract Field Investigator training shall include, but is not limited to, the defined Federal Investigative Standards, identification of applicable Executive Orders, Security Executive Agent Directives, Intelligence Community Directives (ICDs) and governing policies, methodology, issue resolution, interviewing techniques, but also the background investigator core competencies (technical competence, planning/case management, autonomy, interpersonal, oral and written communication skills, and technical application).

The Contractor shall comply with Government requests to review any or all CFI or CIT training certifications, CFI or CIT qualification records, cases, procedures, curriculum, methods, testing materials and test results.

The Contractor shall retain all training related information for the lifecycle of the contract. This includes course descriptions, rosters (to include course title and CFI or CIT name), dates of training, results, transcripts (to include remedial training), and assessment tools. Retained records shall be available for a Government audit.

9.6.4 Contractor shall ensure that all CFI have received basic background investigator training in accordance with National Training Standards.

9.7 Professional Conduct

All persons performing work under the contract are held to the highest ethical standards.

9.7.1 Contractor personnel must adhere to the Standards of Conduct as specified in the OPM Investigator's Handbook or its successor publication.

- The Contractor will ensure that each CFI and CIT performing under this delegation certifies that his or her conduct will conform to the expectations for professionalism and ethical conduct as specified in the OPM Investigator's Handbook or its successor publication.

9.7.2 Misconduct & Misrepresentation

Contractor personnel are not government employees and at no time shall any contractor personnel represent themselves verbally or in writing as government employees.

a) Any action or misconduct by a contractor employee, subcontractor, consultant or other persons performing work under this contract that might adversely affect the following:

- The integrity of an investigative product.
- The Government's access to source information.
- A Subject or Source's rights under the Privacy Act of 1974 (5 U.S.C. 552a)
- The security of investigative material or Government equipment or facilities.
- The individual's basic suitability to perform work under this contract.

b) If any action or misconduct is discovered by the contractor, the contractor will advise the DHS COR, Component POC and/ or COR of the following:

- Offending individual's identity.
- Position held by the individual.
- Nature of the alleged negligence or misconduct.
- Identification of all investigations on which the individual performed work or which might otherwise be affected by the individual's negligence or misconduct.

c) The Contractor will reimburse the Government for any costs incurred due to negligence or misconduct by a Contractor's employee(s), subcontractor(s), consultant(s), or other Contractor's personnel.

d) In the event of negligence or misconduct, the Component may immediately suspend or revoke the Contractor's or its representatives' access to government facilities and/or general access to perform work under this contract.

e) The Government shall not be liable for actions of contract personnel performing work under this BPA. If a CFI acts outside the limits of this BPA or national security policies and procedures, the Contractor will hold the Government harmless and indemnify the Government for any legal actions and costs brought against the Government. The Contractor will be liable for their own employees' or subcontractor's.

9.7.3 Contract Employee's Arrests and/or Convictions

All persons performing any work under this contract are required to report to the contractor's Facility Security Officer (FSO) all arrests and/or convictions for criminal or alleged criminal acts, whether such acts occur during the performance of work, under the contract, or otherwise.

9.7.4 Allegations of Ghost Writing

For incidents involving allegations of falsification (ghost writing) on the part of a CFI, the Contractor shall conduct a full audit of all leads reported (successfully completed or written-off) by the CFI within the last 180 days.

This audit must include exhaustive efforts to contact each reference and record provider associated with the lead reported by the CFI within the last 180 days (of initial allegation) to attempt to verify the accuracy of the information reported by the CFI for each reported lead.

a) The results of this audit must be provided to the Component COR and Component POC in a report, which shall include the following:

- Case Number
- Subject's Last Name
- Lead Type
- Date Lead Reported per ROI
- Reference/Record Provider's Name
- Date of Audit Contact with Reference/Record Provider
- Result of Audit Contact (Favorable/Unfavorable)
- If Unfavorable, information provided
- Comments
- Name of Contractor personnel that conducted the audit for the lead
- Written statement from CI or Non-Credentialed Personnel involved

b) Based on the information provided by the Contractor's audit, additional information may be requested by the DHS Credentialing POC, Component COR and/or Component POC to address any identified falsification of investigations.

9.7.5 Incidents and Incident Report

All incidents of contract personnel negligence, misconduct or investigation compromise of which the contractor becomes aware shall be reported to the DHS COR, Component COR and Component POC immediately upon discovery or receipt of information by the contractor, unless otherwise set forth in this contract.

a) When directed to do so by the DHS COR, Component COR and/or Component POC, the contractor shall investigate the alleged negligence, misconduct or investigation compromise and prepare an Incident Report reflecting its findings concerning the alleged contract personnel negligence, misconduct or investigation compromise.

b) The Incident Report shall be submitted to the DHS COR, Component COR and Component POC within no more than five (5) calendar days of the date upon which the contractor became aware of the negligence, misconduct or investigation compromise.

c) The report shall be provided on the contractor's official letterhead electronically and include at a minimum the following:

- Name of the investigative or other contract personnel involved.
- Credential numbers of all investigative personnel involved.
- If applicable, the name and case number of the subject of the investigation that the contract personnel were working on at the time the negligence, misconduct or investigation compromise occurred or was discovered.
- Date, time, and location of the incident.
- Full details of the incident obtained through interviews of the parties involved, all witnesses to the incident, and/or copies of any police reports regarding or describing the incident, if applicable.
- Names, and telephone numbers (work, home, cellular, etc.) of all persons involved in or witnessing the incident.
- CFIs/CITs/Employee's Response/Correspondences.
- Contractor's analysis of the incident and any actions taken by the contractor regarding the incident (e.g., removal of the offending personnel from contract work).
- Any additional actions the contractor proposes to take. If the conduct involved inaccurate or false reporting of investigative information, the contractor shall describe how the matter came to its attention and provide a list of all investigations known to the contractor to be affected by inaccuracy or falsity.

9.7.6 Supplemental Report

The Contractor shall provide a supplemental report describing any follow-up actions taken as instructed by the DHS COR, Component COR, and/or Component POC regarding incidents of negligence, misconduct or investigation compromise.

9.7.7 Removal of Personnel

The Contractor will notify the Component COR, Component POC and DHS Credentialing POC immediately of personnel working on the BPA that were removed from other Government contracts for misconduct, misuse of Government credentials and/or any other inappropriate behavior.

9.8 Identification of Contractor Employees

9.8.1 All Contractor personnel are required to identify themselves as Contract employees to avoid creating an impression to the public, agency officials, or Congress that such Contractor personnel are Government officials.

This can occur during meeting attendance, through written (letter or email) correspondence or verbal discussions (in person or telephonic), when making

presentations, or in other situations where their Contractor status is not obvious to third parties.

a) The Contractor employee(s) shall:

- Not by word or deed give the impression or appearance of being a Government employee.

- Clearly identify themselves as Contractor employees in telephone conversations and in all written and electronic correspondence.

9.8.2 The Contracting Officer will make the final determination of compliance with regulations with regards to proper identification of Contractor employees.

10. GOVERNMENT FURNISHED PROPERTY/CREDENTIAL

All CFIs and CITs will be required to possess DHS credentials to perform investigative duties under this BPA.

10.1 Vendors will be provided guidance for the processing, handling, and issuance of all DHS credentials, as well as the processing of non-credentialed contract personnel who support this BPA. This includes the following:

- all requests for new credentials
- all requests for new non-credentialed personnel to support the BPA
- requests for sharing and transferring of existing credentials
- credential-related incidents
- separations and returns of credentials
- inventory of credentials.

10.2 Investigative personnel shall meet the requirements to hold DHS credentials as described in this PWS. The Government reserves the right to review the qualifications of any investigative personnel performing work under this BPA. The Government further reserves the right to refuse to allow any person to work under this BPA for any reason deemed appropriate by the Government. Current Federal employees present a conflict of interest and are not eligible to perform work under this PWS.

10.3 The Government may review the qualifications of individuals submitted by the Contract Company, to be "approved" to work the contract. The Government will then determine if an individual is "approved" or "not approved" to conduct work on the contract, as outlined in the PWS.

10.4 Credential requests for new CFIs and CITs may be submitted to the DHS Credential POC after successful completion of DHS approved training and prior to completion of the field certification.

Field certification cannot be accomplished until the DHS Background Investigator

credential has been received by the CFI. Notification of field certification will be provided to the DHS Credentialing POC upon completion.

- DHS Approved Training - Any new investigator must have investigator training which is compliant with National Training Standards as determined by DHS and such training must include forty (40) hours of approved DHS-specific training.

- Field Certification - Must be completed prior to independently conducting background investigations. Field Mentoring must be completed within ninety (90) days of DHS issuing the credential. Failure to complete the Field Mentoring process in a timely manner will result in the retrieval of the credentials. Credential requests that include a waiver request for field certification (mentoring) may be submitted to DHS after successful completion of the initial forty (40) hours of DHS approved training. Contractors may request a provisional DHS determination regarding approval for CFIs prior to completion of required training.

10.5 All investigative leads conducted shall be reported reflecting the DHS credential number of the person who conducted the investigative lead(s). Investigative personnel shall not perform any investigative duties until credentials are issued.

10.6 At the written direction of the Contracting Officer (CO), the DHS COR or the Credentialing POC, the Contractor shall immediately remove any person from the performance of work under this BPA and shall immediately retrieve the credentials, if any, issued to a person removed from the BPA.

10.7 DHS Credentials shall be used only for conducting personnel security investigative work tasked by DHS under this BPA, or as otherwise specifically approved by the DHS COR or DHS Credentialing POC. The Contractor shall immediately confiscate credentials used by investigative personnel for other than official business and shall immediately notify the DHS COR and the DHS Credentialing POC of the unauthorized use. Any investigative personnel using credentials for a purpose other than one authorized under this BPA may be banned from further performance of work under this BPA. The Contractor understands and agrees that if it knows, disregards, or has active participation in the use of investigative personnel credentials for any purpose other than the performance of work under this BPA, this shall be considered a violation of the law and a risk to the national security of the United States, and may be cause for default under this BPA. Use of, or allowing the use of, a DHS credential for other than official duties may be considered sufficient cause for criminal sanctions in accordance with 18 USC Section 701.

10.8 The Contractor agrees to reimburse the Government for costs resulting from the misuse of investigative personnel credentials by the Contractor, its heirs and successors, the Contractor's employees, subcontractors, consultants, or others. The Contractor is liable for any and all costs of the Government in recovering investigative personnel credentials in the event that the Contractor is unable to do so, including but not limited to any and all litigation and court costs reasonably associated with the Government's recovery efforts and costs associated with the recovery of credentials by federal, state, or local law enforcement

agencies.

10.9 For issuance of a credential, an approved contractor will be required to travel to a DHS PIV Card Issuance Facility (PCIF). The cost for creation of the initial credentials will be incurred by DHS. DHS will not assume any of the associated costs (i.e. travel to the location and time).

11. QUALITY CONTROL

11.1 Quality Control Process

The contractor shall establish and maintain policies and procedures to ensure the quality, timeliness, productivity and performance of all contract requirements. The Government will conduct onsite Performance and Compliance Inspections focused on policies and procedures that support the quality and timeliness of delivered products. Additionally, elements of program management will be evaluated through various means, such as review of policies, review of administrative and managerial processes, investigative practices, audits, observations of employees while conducting work and review of the Quality Control Contact Program.

The Government will conduct the onsite Performance and Compliance Inspections to include unannounced onsite inspection of the Contractor, subcontractor, consultant, and other facilities and computer systems where contract work is performed.

11.1.2 Onsite Performance and Compliance Inspection

During Performance and Compliance Inspections, the DHS Inspection Team will examine the effectiveness of the Contractor's program and evaluate PWS compliance within the following inspection categories: Physical Security, Case Retention, Quality Control, Information Security, Personnel Security, Credential Management, and the Contractor's Training Program. Critical factors of the PWS within each inspection category are evaluated and assigned individual ratings. A subsequent (combined factor) rating is assigned to each inspection category. Inspection category ratings are then combined and evaluated to determine the overall combined Performance and Compliance Inspection rating. Noted deficiencies which represent non-compliance with the PWS are identified as "Findings."

There are three types of factor, category and combined ratings to identify the results of onsite Performance and Compliance Inspections:

- **Satisfactory:** The contractor specific task, area, operation or facility being evaluated meets the DHS PWS requirements and objectives. Any finding(s) is/are minor in nature and are easily correctable. Any consequences of the finding(s) would be negligible in affecting the associated DHS mission and in the protection of DHS assets controlled by the program.

- **Marginal:** The contractor specific task, area, operation or facility being evaluated only partially meets the DHS PWS requirements and objectives. The finding(s) is/are moderate in nature and may require the contractor to dedicate sufficient time and resources to address the deficiencies through management reviews, policy changes, and/or additional employee education and training. The consequences of the finding(s) could affect the associated DHS mission or the protection of DHS assets controlled by the program.

- **Unsatisfactory:** The contractor specific task, area, operation or facility being evaluated does not meet DHS PWS requirements and objectives. The finding(s) is/are serious in nature and will require the contractor to comprehensively address the deficiencies through immediate management reviews, policy changes, and/or additional employee education and training. The consequences of the finding(s) would severely affect the associated DHS mission or the protection of DHS assets controlled by the program.

Note: An overall combined Performance and Compliance Inspection rating of Unsatisfactory will result in an immediate workflow stoppage for the Contractor until sufficient corrective action plans have been developed and implemented by the Contractor, and approved by the Government. The Contractor's program will then be reevaluated by the DHS Inspection Team to determine subsequent compliance with the DHS PWS before future work can be assigned.

11.1.3 Resolution of Findings and Corrective Action Plan (CAP)

Any inspection findings should be resolved and corrected in a timely manner by the Contractor. These should include correction of direct and root causes to preclude recurrence of the findings and to ensure ongoing compliance with DHS PWS requirements. Corrective action plans (CAP) with meaningful, measurable completion milestones are the primary means of resolving findings. When an inspection contains findings, the inspected Contractor will submit a response identifying anticipated corrective actions for each finding to the DHS Inspection Team no later than 15 calendar days after formal receipt of the final inspection report.

Findings cannot be considered closed until associated corrective actions have been verified as completed. A commitment by Contractor representatives to implement a corrective action does not automatically constitute completion of that corrective action. The severity and impact of the finding(s) will be the predominate factor for determining if a follow-up site visit is required to properly evaluate and rate the subsequent corrective action.

This inspection report is considered a living document. The first report received by the Contractor, post-inspection, will be an "Interim" report. When corrective actions have been implemented and validated, the topical area and/or overall combined Performance and

Compliance rating(s) will be recalculated to account for the corrective action(s). The DHS Inspection Team and DHS COR will submit to the contractor a memorandum and a "Final" report documenting the revised ratings resulting from any implemented corrective actions.

11.2 Quality Control Contact (QCC) Program

The Contractor shall administer a Quality Control Contact Program that has been approved by the DHS Inspection POC. The QCC Program ensures that Contractor Investigative personnel are performing their duties in an ethical and professional manner. Information gathered from the responses to the QCC will be used to identify any potential problems or shortcomings of an investigator and to assist in arranging training and counseling for those in need. The QCC program will be used to evaluate competence and to reinforce the importance of integrity and accurate reporting. The DHS Inspection POC is responsible for overseeing the QCC Program for the DHS investigative workforce. The QCC program will emanate from the Contract Company and the Contract Company will record, and make available to the DHS Inspection POC on a monthly basis, metrics reflecting the results of the QCC program. These metrics must be searchable by DHS credential number and provided in the format described in this PWS. This monthly report will be provided to the DHS Inspection POC.

The QCC report for a given month will reflect data from qualifying leads completed in the month beginning three calendar months prior to the date the report is due. For example, the QCC report submitted for April of 2022 (the reporting month) would reflect QCC data for qualifying leads completed in January of 2022 (the data month). The QCC report will be submitted in the format provided with this PWS, to include the following categories:

a) **Monthly QC Contact Totals** – In this category, the contractor will provide overall QCC statistics for the data month. The contractor will provide the number of CFIs and CITs completing qualifying leads, the number of qualifying leads completed, the number of QC contacts attempted for qualifying leads completed, the number of successful QC responses for qualifying leads completed, and the number of QC responses with issues for qualifying leads completed.

a) **Monthly QC Contacts per CFI/CIT** – In this category, the contractor will provide QCC statistics for each investigator. The contractor will provide the last name, first name, and DHS background investigator credential number for all CFIs and CITs that completed a qualifying lead in the data month. For each CFI and CIT in that data month; the contractor will provide the number of qualifying leads completed, the number of QC contacts attempted for qualifying leads completed, the number of successful QC responses for qualifying leads completed, and the number of QC responses with issues for qualifying leads completed. A comment section is provided for each CFI or CIT. This comment section should be used to indicate if a check-ride

is required, if a check-ride waiver has been requested, or if an issue has been reported.

b) **Monthly Mailed QC Contact Totals** – In this category, the contractor will provide statistics for QC contacts attempted via mail for qualifying leads completed in the data month. The contractor will provide the number of QC contacts attempted by mail, the number of successful and unsuccessful QC responses received by mail, and the number QC responses received by mail with issues. Any QC attempts that were unsuccessful due to issues with the mailing process (not deliverable as addressed, no such number, etc) will be reported in this category using the format provided.

c) **Monthly Telephonic QC Contact Totals** – In this category, the contractor will provide statistics for QC contacts attempted via telephone for qualifying leads completed in the data month. The contractor will provide the number of QC contacts attempted by telephone, the number of successful and unsuccessful QC responses conducted by telephone, and the number QC responses conducted by telephone with issues.

d) **Complaints/Derogatory Responses** – In this category, the contractor will provide statistics regarding QC contact responses for qualifying leads completed in the data month that reflected complaints, issues, and derogatory responses. The contractor will provide the last name, first name, and DHS background investigator credential number for all CFIs and CITs that were noted to have issues. The date the QC response was received, the method of the QC Contact, the case number of the investigation where the issue occurred, and a short description of the complaint must be included in this category. The contractor must also provide the name of QC POC who is addressing the issue, and what actions were taken to resolve it.

e) **QC Check Rides** – In this category, the contractor will provide statistics regarding any QC check rides that were required due to a CFI or CIT failing to receive the minimum required successful QC responses for qualifying leads completed in the data month. The contractor will provide the last name, first name, and DHS background investigator credential number for all CFIs and CITs that required a QC check ride; as well as the date of the QC check ride, the DHS component case number for the leads used to complete the QC check ride, the name and DHS background credential number of the senior investigator who observed the QC check ride, as well as any observations made by the senior investigator.

This is a cumulative report; each month's QCC report should include the data submitted in previous monthly QCC reports. This should continue until 12 months of QCC data are reflected on the QCC report; at which time data from the oldest data month must be removed and replaced with data from the current data month.

In the event that a QCC reflects personnel negligence, misconduct or investigation compromise of which the contractor becomes aware shall be reported to the DHS COR, Component COR and Component POC immediately upon discovery or receipt of information by the contractor, unless otherwise set forth in this contract. The Contractor will immediately investigate the matter. The Contractor will report the results of the investigation in accordance with the reporting requirements outlined in this PWS.

Based on responses from the QCC program, the Government reserves the right to have a CFI or CIT removed from any further work on this contract. Based on responses from the QCC program, Contractors will ensure adequate training is provided to investigators identified as needing additional or remedial training.

11.3 Frequency and Selection

A Quality Control Contact is used to query a source as to the conduct, integrity, and professionalism of the investigator who interviewed them in the course of a background investigation completed under this PWS. A Quality Control Contact must query the source regarding the following applicable elements of the interview:

- Did the investigator introduce themselves as contract investigator conducting a background investigation for DHS or a DHS component?
- Was the interview conducted in-person or via telephone?
- Did the investigator present their DHS background investigator credentials?
- Did the investigator explain the purpose of the investigation?
- Did the investigator explain the requirements of the Federal Privacy Act of 1974?
- Did the investigator appropriately question the source regarding the subject's honesty, integrity, trustworthiness, financial responsibility and personal conduct?
- Did the investigator appropriately question the source regarding their knowledge of any criminal conduct, alcohol abuse, or illegal drug use by the subject?
- Did the investigator ask the source if he/she recommended the subject?
- Did the investigator present themselves in a professional manner, to include their grooming and attire?

As part of the Quality Control Contact Program, the Contractor is required to make a minimum number of QC Contact attempts per investigator per month and is required to receive a minimum number of successful QC contact responses per investigator per month.

a) The Contractor must conduct at least four QC contact attempts for every CFI or CIT completing qualifying leads in a data month. For any investigator that completes fewer than four qualifying leads in a data month, the Contractor must conduct QC contact attempts on 100% of the qualifying leads completed by that investigator.

b) Attempts will be made to identify sources that were originally interviewed no more than 30 days prior to the QC contact attempt. The Contractor should not wait for final case closure to begin selecting sources for QC contact attempts.

c) The requirements for successful QC responses per investigator will be assessed based on the number of qualifying leads completed by each CFI or CIT in a data month.

d) The Contractor must receive a successful QC response for at least 10% of the qualifying leads completed by each investigator in a data month. This requirement applies to any CFI or CIT that completes four or more qualifying leads in a data month. The table below illustrates the number of successful QC responses necessary to meet this requirement:

NUMBER OF QUALIFYING LEADS COMPLETED BY INVESTIGATOR IN DATA MONTH	NUMBER OF SUCCESSFUL QC RESPONSES REQUIRED FOR DATA MONTH
1-3	0
4-10	1
11-20	2
21-30	3
31-40	4
41-50	5

Note: This table is an example for CFIs completing between one and 50 qualifying leads. The requirement continues following this pattern for CFIs completing 51 or more qualifying leads in a data month. As it is not possible to receive a partial successful QC response; if 10% of qualifying leads results in a fractional number, the requirement for successful QC responses will be rounded up to the next whole number.

This requirement applies to each investigator individually; the Contractor may not use a surplus of successful QC responses for one investigator to address a deficiency in successful QC responses for another investigator.

e) For active CFIs and CITs completing three or less qualifying leads during the reporting month; this does not relieve the Contractor of the requirement to conduct the minimum monthly QC contact attempts.

f) Any active CFI or CIT that does not receive the minimum required successful QC responses for the data month must undergo a documented QC check ride with a qualified DHS credentialed supervisor or senior/experienced DHS credentialed investigator and the results must be provided to the DHS Inspection POC. The qualified credentialed supervisor or senior/experienced credentialed investigator during this QC check ride must witness, at a minimum, one reference interview and one subject interview. If a SI is not available for a QC check ride, three additional reference interviews may be conducted in lieu of the SI for a total of four reference interviews, to meet the QC check ride requirement. A QC check ride must be completed and reported to the DHS Inspection POC within thirty (30) days of a CFI being identified as failing to meet the monthly successful QC response requirement.

g) CFI or CITs identified as requiring a QC check ride should have a note reflecting this in the comments column of the data month where they fail to meet the QCC requirements. The results of this QC check ride must be reported in the QC Check Ride tab of the following month's report. Attempts to meet the successful QC response requirement should be documented for any investigator who requires a check ride. The DHS Inspection POC may grant a waiver on a case-by-case basis for CIs s requiring a check ride where the documented attempts are considered exhaustive. Any CI who fails to meet the QCC requirements for a given month (as identified in the monthly QCC report) may not complete work on any DHS Calls/ Task order for any DHS component until they complete the required QC check ride or the DHS Inspection POC has approved a waiver request for that month.

h) Waiver requests must be submitted via email to the DHS Inspection POC concurrently with the monthly QCC report. A single waiver request email may include waiver request information for multiple investigators. The following information must be included for each investigator: Qualifying Leads Completed, Quality Control Contacts Attempted, and the rationale for the waiver that clearly details the exhaustive efforts made to obtain the minimum requirements. As much detail as possible should be provided to support the waiver request. Any investigator with a waiver request must also be reported in the monthly QCC Report, to include an indication in the Comments column that a waiver has been requested for that investigator.

i) Qualifying leads for QCC include:

- Neighborhood reference interviews
- Military reference interviews
- Employment reference interviews
- Education reference interviews
- Listed reference interviews
- Developed reference interviews
- Interviews of references who provided derogatory information
- Interviews conducted via telephone

Qualifying leads include work completed by an investigator for all DHS components. Record checks are not qualifying leads as part of the QCC program. While the Contractor is encouraged and free to conduct their own QCC on record checks, they are not required to be reported to the DHS Inspection POC as part of the QCC Program requirements of this PWS.

j) Leads acceptable for a QC check ride include:

- Neighborhood reference interviews
- Military reference interviews
- Employment reference interviews

- Education reference interviews
- Listed reference interviews
- Developed reference interviews
- Interviews of references who provided derogatory information
- Former spouse interviews
- Confidential source interviews
- Subject Interviews

Leads acceptable for a QC check ride include work completed for all DHS components. Neither record checks nor interviews conducted via telephone may be used for a QC check ride.

11.4 Quality Control of Report of Investigations

The Contractor is responsible for developing and implementing Quality Control processes and procedures for all ROIs. Before the Contractor submits any ROI as part of a call/task order with a component, the Contractor shall conduct a thorough two-tiered review involving two or more separate parties (persons). This review will verify all investigative leads required for the investigation type have been conducted in accordance with the Federal Investigative Standards, Handbook, and the Guide. The plan must incorporate two tiers of review that involve two separate parties (persons) reviewing all ROI's before they are submitted to the component agencies.

11.5 Standards and Evaluation Check Ride

The Government reserves the right to require all investigative personnel to submit to a Standards and Evaluation Check ride. The Government will accomplish such Evaluation check ride by requesting a list of scheduled leads (records checks, source interviews, and subject interviews) and arranging to have personnel join Contractor investigative personnel at the location of the lead, or by Government personnel accompanying contract investigative personnel. DHS will use standards as referenced in the Handbook, Guide, and this PWS to evaluate contract investigator personnel.

12. DELIVERABLES

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

The Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation created as part of this contract. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

The Contractor shall provide the following deliverables to the authorized Government Official. The Government Official may reject or require correction of any deficiencies found in the deliverables. In the event of a rejected deliverable, the Contractor will be notified in writing by

the Government Official of the specific reasons for rejections. The following table specifies the deliverables for this requirement:

Table 12.1

Referenced Deliverables				
PWS Reference	**Title**	**Timeline**	**Delivery**	**Acceptable Quality Level (AQL)**
6.0, 7.5	ROI - Expedited	Due within 14 Days	E-Delivery to requesting Component	Accurate, complete, received on time.
6.0, 7.5	ROI- Standard	Due within 35 Days	E-Delivery to requesting Component	Accurate, complete, received on time.
6.0, 7.5	ROI - Extended	Due within 60 Days	E-Delivery to requesting Component	Accurate, complete, received on time.
6.0	ADL	Due within 35 days	E-Delivery to requesting Component	Accurate, complete, received on time.
7.2.4 (c)	Serious Derogatory Information Notification	Due within 24 hours of discovery	Email to Component COR and/or POC	Accurate, complete, received on time.
7.5.7 (b)	Certificate of Destruction	Due within Monthly Report	Email to Component COR	Accurate, Received on time
7.5.7 (c)	Information Security Protection Plan	Upon request	Email to requesting Component	Accurate and complete
8.0	Transition Plan	Draft due within 7 calendar days after BPA award Final version due within 7 calendar days after government's	Email to DHS COR	Received on time

		review of Draft.		
8.0	Training Plan	Draft due with Transition Plan Due within 5 days of any substantial changes to Training Plans	Email draft to DHS COR (with Transition Plan) Email substantial changes to DHS Inspection POC	Accurate, complete, received on time
9.6.2	Training Documentation	Due within 24 hours upon request	Email to DHS Credentialing POC	100% compliance. Received on time
9.7.5	Incident Report	Due within 5 days after incident	Emailed to DHS COR, Component COR and/or Component POC,	Accurate, complete, received on time
11.1.3	Corrective Action Plan (CAP)	Due within 15 calendar days after formal receipt of the Final Inspection Report	Email to DHS Inspection POC	Accurate, complete, received on time
11.2	Monthly QCC Report	Due by the 7th calendar day of each Month.	Emailed to DHS Inspection POC	Accurate, complete, received on time.
11.2	Various Standard Operating Procedures	Upon Request	PDF	Complete

Note: Unless otherwise specified, "days" refers to calendar days.

Table 12.2

Administrative Deliverables				
Title	**Timeline**	**Delivery**	**Acceptable Quality Level (AQL)**	**Description**

<table>
<tr><td>Monthly Invoice</td><td>Due by the 7th calendar day of each Month</td><td>Electronic, Excel, Encrypted To the Component COR</td><td>Accurate, complete, received on time</td><td colspan="2">The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive government information, such as personally identifiable information (PII), created, obtained, or provided during the performance of the contract.

The invoice must contain the following:

Vendor Name
Invoice Number
Investigation Case Number
Investigation Type
SLIN
Delivery Type
Investigation Status
Subject Last Name
Investigation Base Price
Date Case Opened
Date Case Completed

Investigation Incentive/Disincentive Percent
Investigation Incentive/Disincentive Amount
Date Case Cancelled
Cancellation Reduced Percent
Cancellation Reduced Amount
Credit Indicator
Credit Amount
Total Billed Amount
Exception Indicator
Number of Days</td></tr>
<tr><td>Post Award Conference (Kick-off Meeting) Minutes</td><td>Draft due within 7 calendar days after meeting

Final version due within 5 calendar days of government's review of Draft.</td><td>Draft – Word
Final – PDF

Emailed to the Component COR and CO/CS</td><td>Draft – received on time.

Final Version - Accurate, complete, received on time.</td><td colspan="2">The purpose of the Post Award Conference is to aid both Government and Contractor personnel to achieve a clear and mutual understanding of all contract, management, and technical requirements and to identify and resolve potential problems.</td></tr>
<tr><td>SIP Username and Password</td><td>Upon request</td><td>Electronic to requesting Component</td><td>Accurate</td><td colspan="2">The Contractor shall provide access to the respective Government personnel via established Username and Password for the SIP. Levels of access will be discussed and agreed to upon award.</td></tr>
<tr><td>Monthly Report</td><td>Due by the 7th calendar day of each Month.</td><td>Email to Requesting Component POC</td><td>Accurate, complete, received on time</td><td colspan="2">The coverage period for this report is from the first of every month to the last day of the month. Details associated with the electronic submission of the Monthly Reports format will be provided to the Contractor.</td></tr>
<tr><td>Monthly Credential Database Update Report</td><td>Due by the 7th calendar day of each Month.</td><td>Email to DHS Credentialing POC</td><td>Accurate, complete, received on time</td><td colspan="2">The Contractor will provide a monthly report of credential related information. A template will be provided to the Contractor.</td></tr>
</table>

Daily Manifest Report	Daily	Email to Requesting Component POC	Accurate, complete, received on time	The Contractor will provide a daily list of cases. A template will be provided to the Contractor.
180 Day Investigator Report	Due by the 7th calendar day of each Month.	Email to DHS Credentialing POC	Accurate, complete, received on time	The Contractor will provide a report listing personnel possessing DHS background investigator credentials who have not been assigned work for a period of 180 calendar days or more with any DHS component under this PWS or associated call/ task order. The Contractor must verify that any personnel who appear on this report maintain possession of their DHS background investigator credential. The Contractor must verify that personnel maintain possession of their credential on a monthly basis for as long as the personnel appear on this report. A template will be provided indicating how this information should be reported.

Note: Unless otherwise specified, "days" refers to calendar days.

13. SECURITY

13.1 Contractor's Facility

Secure Storage

The Contractor shall ensure that DHS investigative data is stored in a manner that precludes comingling with data from other non-DHS entities. The Contractor shall ensure that DHS investigative data can be identified, segregated, retrieved, deleted and/or sanitized upon request of DHS.

The Contractor shall provide proof of the ability to provide secure storage for investigative and training materials per standards set out in the DHS Handbook for SPII at the time of award. The protection and disclosure of information collected or provided under this BPA is also governed by the requirements of the Privacy Act of 1974, as amended (5 U.S.C. 552a), DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

Prior to the commencement of work, and during the term of the BPA, the Government reserves the right to inspect, and approve the Contractor's facility and to require the Contractor to complete all necessary security documents. Inspection shall be in accordance with National Industrial Security Program Operating Manual (DOD 5220.22-M, Feb 2006/ Incorporating Change 2, May 18, 2016) Chapter 5, Section 7 for the receipt and/or collection of, handling, storage, dissemination, disposal, and destruction of classified material, information designated as "FOUO," and information subject to the Privacy Act of 1974 requirements as amended (5 U.S.C. 552a).

In addition, the Government may conduct site visits, announced/unannounced at the Contractor's facility to determine compliance with this Performance Work Statement and applicable clauses. During these site visits, the Contractor is required to make the following position personnel

available during the inspections: Management personnel, Case Controllers, Case Schedulers, Case Reviewers, Investigators, Investigative Technicians, Program Manager, Credential Managers, Trainers, Information Technology and Information Technology Security personnel and any other personnel identified by DHS before the arrival of the inspection team at the Contractors facility. The contractor shall be prepared to accommodate an information technology security assessment including, but not limited to, a system penetration test. Any system test results and data, to include vendor packet capture and audit logs, will be collected and retained by the Government for more in-depth analysis in secured and isolated Government labs.

Contractor employees visiting Government facilities shall wear an identification badge that, at minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (DOD 5220.22-M, Feb 2006/ Incorporating Change 2, May 18, 2016) Chapter 2, Section 1 (Facility Clearance) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Counterintelligence and Security Agency. If the Contractor has access to classified information, it will abide by the requirements set by the agency.

The contractor shall ensure all investigative, reinvestigate, and adjudicative requirements are met in accordance with the National Industrial Security Program Operating Manual (DOD 5220.22-M, Feb 2006/ Incorporating Change 2, May 18, 2016) Chapter 2, Section 2. The Contractor will be responsible for ensuring that all personnel have been favorably adjudicated following completion of an appropriate Tier 5 (T5) level background investigation or equivalent and such reinvestigations as may be required prior to and during any work performed on this BPA.

Upon award of the BPA, the Contractor will provide DHS COR with a list of all proposed employees to support this BPA. The list must include full name, social security number (SSN), date of birth (DOB), place of birth (POB), the date of their last favorably adjudicated (T5 level) background investigation. A DHS Component will then provide instructions for the completion of any additional security related documents. The same procedure shall be followed prior to any new/rehire employee performing work on this BPA.

No person shall be allowed to begin work on this contract and/or access sensitive information without receiving clearance verification from the Facility Security Officer (FSO). DHS further retains the right to deem an applicant as ineligible due to an insufficient background investigation or when derogatory information is received and evaluated under a Continuous Evaluation Program. Any action taken by DHS does not relieve the Contractor from required reporting of derogatory information as outlined under the National Industrial Security Program Operating Manual (DOD 5220.22-M, Feb 2006/ Incorporating Change 2, May 18, 2016) Chapter 1-3.

The Government reserves the right to refuse to allow any person to work under this BPA for any reason deemed appropriate by the Government.

The Contractor shall notify the COR of the removal of any person from the performance of work under this PWS. Removal does not relieve the Contractor of the responsibility to continue providing the services required under this PWS.

Any information made available to the Contractor by the Government or its customers shall be used only for the purpose of carrying out the provisions of this BPA and is proprietary. This information shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the BPA.

In the performance of this PWS the Contractor assumes responsibility for the protection of the confidentiality of Government records.

During the course of this agreement, the Contractor will ensure the security of the system data to include secure communication and storage. 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 (SBU) Information.

In the event PII or sensitive program related information (including investigative results) is lost, stolen, misplaced, or inadvertently disclosed, the Contractor must report the matter to the COR within one hour.

In the event of disclosure of PII information, the Contractor will coordinate with the Government in notifying affected persons. The Contractor shall assume all liability for actions resulting from the loss or compromise of personal information provided by applicants, employees or Contractors, when such loss is the responsibility of the Contractor, or any subcontractor performing work on behalf of the Contractor, or an investigator employed by the Contractor. If the government determines the disclosure warrants identity protection services for the affected person(s), the Contractor will be required to purchase identity protection services for the affected person(s).

13.2 Compliance with DHS Security Policy Terms and Conditions

(a) The contractor will abide by all terms and conditions cited in the Clause section including but not limited to: "Safeguarding of Sensitive Information" and "Information Technology Security and Privacy Training" with regard to the use and protection of DHS data under this BPA.

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

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

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

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

(f) Each individual employed under the BPA shall be a citizen of the United States of America. Any exceptions must be approved by the Department of Homeland Security's Chief Security Officer or designee.

13.2.1 Interconnection Security Agreements (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 accredited 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 interconnect service agreements.

ISA's must be approved before any information will be transferred between DHS and the Contractor via the MQ established for electronic transmission of all case related documents.

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

Contractors are fully responsible and accountable for ensuring compliance with all Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST), Special Publication 800 series, Federal Information Processing Standard (FIPS) and related DHS security control requirements (to include configuration guides, hardening guidance, DHS Security Policy, Procedures, and Architectural guidance). The Contractor security procedures shall be the same or greater than those that are provided by DHS Enterprise Data Center(s). Sensitive DHS information, such as privacy and technical data, must be encrypted at rest within non-DHS-facilities.

13.2.2 Encryption Compliance Terms and Conditions

Sensitive DHS information, data, and extracts hosted at non-DHS facilities must be encrypted at rest by using one the following acceptable methods:

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

2. National Security Agency (NSA) Type 2

3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of

13.2.3 Physical and Information Security and Monitoring Terms and Conditions

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

The Contractor will prevent unauthorized physical access to the facility through the deployment of high security lock and key sets, an electronic access control system, and/or an on-site guard force. The facility will be located within the United States and its territories.

13.2.4 Vulnerability Assessments Terms and Conditions

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

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

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

13.2.6 Patch Management Terms and Conditions

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

system (NIDS), Anti-malware, and Firewall) shall be tested by the Contractor prior to deployment in a test environment.

13.2.7 **Supply Chain Risk Management**

The vendor shall assess, avoid, mitigate, accept, or transfer supply chain risks; consistent with requirements contained within Title II of the SECURE Technology Act (titled the "Federal Acquisition Supply Chain Security Act of 2018"), subchapter to Chapter 13 of Title 41 and Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT). The vendor shall, as well as for all subcontractors performing work under this BPA as well as their own service offerings:

a. Assess the supply chain risk posed by the acquisition and use of "covered articles." Covered articles include:
    i. Information technology, including cloud computing services of all types;
    ii. Telecommunications equipment or telecommunications service;
    iii. The processing of information on a Federal or non-Federal information system, subject to the requirements of the Sensitive Information program; and
    iv. All IoT/OT hardware, systems, devices, software, or services that include embedded or incidental information technology.
b. Prioritize supply chain risk assessments based on the criticality of the DHS mission and vendor's system, Component, service, or asset. Provide OIG any and all documentation of Supply Chain and or Chain of Custody on an as requested basis. See https://www.acquisition.gov/gsa-deviation/supply-chain-aug13 and https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force for further details.
c. Provide an initial Supply Chain Assessment Report and if any significant changes in the contract occurs after award to the appropriate DHS point of contact, that includes:
    i. An overview of the supply chain risk management strategy, methodology, and implementation plan used to guide and govern supply chain risk management activities;
    ii. Addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, Components, and software
    iii. A description of how supply chain risk management practices directly impact the life cycle of systems, Components, services, and assets;
    iv. How risks from the supply chain will be identified;
    v. Describes the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this solicitation and associated Calls/ Task Orders;
    vi. What processes and security measures will be adopted to manage these

supply chain risks to the system or system Components; and

vii. How the supply chain risks and associated security measures will be updated and monitored.

viii. A table identifying known supply chain risks, and indicating how the vendor limited, avoided, mitigated, accepted, or transferred any identified risk;

ix. How relevant information was shared with DHS; including classified information;

d. Ensure existing vendor acquisition processes, services, and operations incorporate the results of supply chain risk assessments.

e. Subcontractors.

i. Subcontractors are subject to the same general requirements and standards as prime contractors. Vendors employing subcontractors shall perform due diligence to ensure that these standards are met.

ii. The Government shall be notified when a new vendor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

iii. The vendor shall monitor suppliers and third-parties supporting this contract for potential supply chain concerns as described in Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT). See https://www.acquisition.gov/gsa-deviation/supply-chain-aug13 and https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force for further details.

f. The vendor understands and agrees that the Government retains the right to cancel or terminate the Contract, if the Government determines that continuing this acquisition presents an unacceptable risk to national security.

g. Supply-Chain Transport

i. Vendors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the Component is documented at all times from initial shipping point to final destination, and every transfer of the Component from one custodian to another is fully documented and accountable) for all shipments to fulfill Contract obligations with the Government.

ii. All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the Contract, the period of performance, or one calendar year from the date the activity occurred.

iii. This transit process shall minimize the number of times in route Components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

iv. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

v. The vendor is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government.

vi. The vendor shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

vii. The vendor shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent electronically and will state this solicitation number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

h. Notifications. The vendor shall notify DHS Office of the Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at [redacted]

i. The vendor shall immediately notify the DHS Office of the Chief Security Officer regarding any changes to corporate foreign ownership, control, or influence.

j. For additional details contact the DHS Office of the Chief Security Officer or DHS OCISO National Security Cyber Division directly at [redacted]

k. The vendor shall perform all privileged functions and authorized security-relevant functions that ordinary users are not authorized to perform (e.g. Administration, Development, and Remote Administration) of equipment or services in support of this contract with the ability to affect DHS missions from (a) a U.S. State, and (b) using U.S. Citizens vetted through the personnel security process listed in the Personnel Security Suitability and the Personnel Background Investigation Requirements. The vendor shall ensure the DHS Chief Security Officer (CSO) is apprised of all instances, as well as submits these individuals through the process listed in the Personnel Security Suitability and Personnel Background Investigation Requirements, where the vendor cannot meet this requirement

13.3 Security Plan

13.3.1 Security of Systems Handling Personally Identifiable Information and Privacy Incident Response

The contractor will abide by all terms and conditions cited in the Clause section of

this acquisition including but not limited to: "Safeguarding of Sensitive Information" and "Information Technology Security and Privacy Training" with regard to the use and protection of DHS data under this BPA.

The system security plan shall be implemented at a FIPS 199 High-High-Moderate security level in accordance with the applicable clause.

No DHS data can reside on personally owned laptops used to process DHS investigations. In addition, use of Contractor-owned laptops or other media storage devices to process or store PII and DHS Component data is prohibited under this contract until the Contractor provides, and the Contracting Officer in coordination with CISO approves, written certification by the Contractor that the following requirements are met:

(1) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

(2) The Contractor has developed and implemented a process to ensure that security and other applications software are kept current;

(3) Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;

(4) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements.

(5) The Contractor shall maintain an accurate inventory of devices used in the performance of this PWS.

(6) Contractor has developed and implemented a method to regularly audit laptops and other media storage devices used to process or store PII and DHS data to verify that no DHS or Component case data or materials have been retained in excess of three hundred and sixty-five (365) days (unless expressly requested to do so by the Component).

(7) Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:

(i) Authorized and official use;
(ii) Prohibition against processing, accessing, or storing Sensitive PII on personally owned equipment outside of specified secure applications.
(iii) Prohibition against access by unauthorized users and unauthorized use by authorized users; and

(iv) Protection of Sensitive PII;

(8) All Sensitive PII obtained under this PWS shall be removed from Contractor-owned information technology assets upon termination or expiration of Contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the Contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of Contractor work.