U.S. Department of Homeland Security

U.S. Immigration and Customs Enforcement (ICE)
Office of Civil Rights Compliance (OCRC)
Equal Employment Opportunity Division (EEO)

Equal Employment Support Services

Statement of Work

January 29, 2025

Table of Contents

Statement of Work for EEO Services

1. BACKGROUND

The **Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE)** is the United States government's principal agency leading our nation's efforts to strengthen border security and prevent the illegal movement of people, goods, and funds into, within, and out of the United States. The agency's broad investigative authorities are directly related to our country's ongoing efforts to combat terrorism at home and abroad.

ICE includes a workforce numbering approximately 20,000 including deportation officers, special agents, analysts, and professional staff. ICE's programs are administered by 5 Directorates and Staff Offices, including members of the U.S. Public Health Service.

The Office of Civil Rights Compliance (OCRC), Complaints and Resolution Division's (EEO) mission is to work to achieve a workplace free from discrimination and harassment where every employee is valued for his/her unique contribution toward achieving the goals of ICE.

OCRC's mission is to (1) promote and ensure equal employment opportunity (EEO) for all employees, former employees, and applicants for employment and foster an agency culture and environment free from discrimination; (2) work in partnership with management and employees to create and implement innovative effective affirmative employment programs and dispute resolution processes; and (3) ensure full utilization of a diverse workforce in carrying out the Agency's mission and provide quality and timely services to its customers.

OCRC-EEO provides EEO services for ICE, through both in-house and contract providers. EEO routinely contracts for EEO services to include: traditional counseling services and report preparation during the pre-complaint stage of the EEO complaint process; mediation or alternative dispute resolution (ADR) services, including scheduling, processing, and resolution attempts; formal complaint processing, including investigation of discrimination complaints and preparation of Reports of Investigation, preparation of letters of acceptance/dismissal and preparation of draft procedural dismissals or final agency decisions, and compliance monitoring services, including responding to and implementing EEOC Orders, Judgements, and Settlement Agreements.

2. SCOPE

The contractor must be able to provide scalable EEO services to address the volume of pre-complaints, formal complaints, and compliance monitoring actions that are expected. The Contractor must provide certified EEO counselors and investigators to conduct the following:

- Pre-complaint services, including timely traditional counseling of EEO complaints and alternative dispute resolution (ADR) services; preparation of quality EEO counselor's reports, notices of the right to file, contact summaries for ADR cases, and Agency requested streamlined pre-complaint processes.

- Formal complaint services, including the timely preparation of draft accept/dismiss letters, the timely and quality submission of investigative plans, the timely and thorough investigations of the accepted issues, the timely and quality submission of draft and final reports of investigation (ROI) and the preparation of timely and quality draft procedural dismissals or final agency decisions (FAD), and Agency requested streamlined formal complaint processes.
- Compliance monitoring services, including responding to, managing, and implementing EEOC Orders, Judgements, and Settlement Agreements.

All services provided must be in conformance with the Equal Employment Opportunity Commission's (EEOC's) regulations set forth at 29 CFR part 1614,EEOC Management Directive-110 (MD-110), and Agency documented streamlined processes.

3. QUALIFICATIONS AND EXPERIENCE

The Contractor's, EEO Counselors, EEO Investigators and FAD Writers must possess the following requisite training, experience, knowledge, and skills to perform the required EEO services.

- EEO Counselors and Investigators must receive 32 hours of initial training and 8 hours of refresher training each fiscal year thereafter as described in the EEO MD-110.

- ADR service providers must meet the certification and/or licensing requirements, if required, for the state in which the ADR services are provided. Additionally, ADR Practitioners must meet and comply with the requirements contained in 29 C.F.R. § 1614.102(b)(3) and EEOC Management Directive 110, Chapter 3, Section B (c).

- FAD Writers must have completed at least 5-10 cases/decisions; have a minimum of 2 years of Federal EEO Investigative or FAD Writing experience; and/or legal analysis experience and have the appropriate certification.

The Contractor must ensure that its staff has the required professional certifications in advance of the assignment and maintains the required professional certifications throughout the period of performance for the contract services. The Contractor must retain documentation of such records and must provide a copy of the certificates and resumes of the staff members to EEO prior to case assignments. The Government will not pay expenses for sub-contractors to meet the professional certification requirement.

In accordance with FAR 37.114(c), the Contractor and its employees must always identify themselves as Contractor personnel when dealing with Government employees or the public in the performance of the services under their contract. All documents or reports produced by a Contractor must also be suitably marked as contractor products.

4. PLACE OF PERFORMANCE

OCRC manages its mission through a virtual (remote) work environment. All services shall be performed by the Contractor in a virtual or remote work environment. In the event work needs to be performed in person, a temporary workspace can be requested and provided at our headquarters location, 500 12th Street SW, Washington, DC.

5. HOURS AND DAYS OF OPERATIONS:

Contractor employees shall generally perform all work between the hours of 7:00 a.m. and 6:00 EST p.m., Monday – Friday except for federal holidays listed below and any other day designated by Federal Statute, Executive Order, or Presidential proclamation. A 40-hour work week is required, and no overtime is anticipated on this task.

Federal Holidays

New Year's Day, January 1
Martin Luther King's Birthday, the third Monday in January
Washington's Birthday, the third Monday in February
Memorial Day, the last Monday in May
Juneteenth, June 19
Independence Day, July 4
Labor Day, the first Monday in September
Columbus Day, the second Monday in October
Veteran's Day, November 11
Thanksgiving Day, the fourth Thursday in November
Christmas Day, December 25.

6. CONFLICT OF INTEREST

If for any reason the agency or the Contractor determines that the Contractor and/or an employee of the Contractor faces a potential, perceived, or real conflict of interest, immediate notification shall be made by contractor and/or agency. all work shall cease until a determination is made by the agency on how to proceed.

7. COUNSELING OF PRE-COMPLAINTS

Scope.

The purpose of the EEO Counseling inquiry is to obtain information regarding the claim(s), address jurisdictional questions, and respond to the Aggrieved Person's (AP) requested remedy. The EEO Counselor should interview persons who can provide information that is relevant to the claim(s), settlement, and jurisdictional questions. The EEO counseling inquiry is not an "investigation" nor is it intended to resolve disputed facts, rather, it is simply gathering information necessary for the EEO Counselor to assist the parties in resolving the

matter at the lowest level. The EEO Counselor must control the inquiry at all times and seek guidance and assistance from the Contractor, or ICE as needed.

Assignment

a. The Contractor shall assign an EEO Counselor to a matter within **two (2)** business days of receipt of the assignment.
b. The EEO Counselor shall contact the AP within 2 days of assignment to schedule the initial interview. The initial interview with the AP should be conducted as soon as possible after receiving assignment but no later than 5 days of assignment. Unusual circumstances that may prevent conducting the interview immediately, e.g., illness or emergency leave must be brought to the attention of ICE.

The responsibility for EEO Counseling is as follows:

a. The EEO Counselor will interview all witnesses, including the responsible management official (RMO), within 20 days of the initial contact.
b. The EEO Counselor should write-up each interview after completion and incorporate the information into the EEO Counselor's Report.
c. The EEO Counselor should review and summarize all documents relevant to the claim(s) and incorporate the information into the EEO Counselor's Report.
d. If the EEO Counselor believes the inquiry is deficient procedurally, or in content or scope, he/she should immediately notify the agency.

Initial Counseling Interview

a. During the initial interview, the EEO Counselor will complete the following tasks, obtain the AP's signature on all necessary paperwork, and answer any questions (s)he may have about the pre-complaint process. See EEO MD-110, Chapter 2, Section III and 29 C.F.R. § 1614.105.

    1. Advise the AP of his/her rights and responsibilities under 29 C.F.R. § 1614 Explain the Agency's ADR program and explain that they must elect whether to seek pre-complaint resolution through ADR or through the traditional pre-complaint process. The EEO Counselor shall inform the AP about the differences between the two processes.
    2. Determine the claim(s) and bases raised by the AP.
    3. Determine if there are issues relating to the timeliness of the initial contact or other jurisdictional questions and obtain information relating to this issue.

4. Advise the AP of his/her right to file a formal discrimination complaint if attempts to resolve the dispute through EEO counseling or ADR fail to resolve the dispute.
5. Ask what the AP desires from the supervisory chain to resolve the complaint.
6. Explain the right to anonymity during pre-complaint counseling only, the right to a representative of his/her choosing, and his/her obligation to inform the EEO office, immediately of the name, address, and phone number of a representative if one is chosen after the initial interview.
7. Explain the role of the EEO Counselor and advise the AP that the EEO Counselor will complete his/her inquiry and conduct a Final Interview within 30 calendar days of the initial contact unless the AP has agreed in writing to an extension of the counseling period, or to participate in the ADR process.
8. If the pre-complaint will follow a streamlined process, the EEO Counselor shall follow the Agency's streamlined processes.

Requests to Extend the Pre-Complaint Period Beyond 30 Days

By the **25th day** after initial contact, if the EEO Counselor has not completed the counseling process, the EEO Counselor shall contact EEO to discuss the circumstances of the case and to request the authority to seek an extension from the AP.

EEO may consider whether a request for an extension can be sought based on exigent circumstances such as illness, emergency leave, or extended travel of the AP or a primary witness.

a. An AP may agree in writing to postpone the Final Interview and extend the period for pre-complaint counseling for up to or less than **60** additional calendar days from the date of the initial contact.
b. The requisite Extension Form shall be used to obtain the request in writing.
c. If the AP is unwilling to grant additional time, the EEO Counselor must complete the counseling process and issue the Notice of Right to File Formal along with DHS Form 3090 (Individual Complaint of Employment Discrimination) within 25 days from the date of initial contact. The EEO Counselor should immediately submit the EEO Counselor's Report, and all paperwork gathered during counseling for review.

Settlement

The EEO Counselor shall attempt to facilitate a settlement of the pre-complaint. If the AP and the Agency agree to an informal resolution of the dispute during the course of the EEO counseling inquiry, the terms of the settlement shall be reduced to writing, in DRAFT, using the approved settlement template and sent to EEO for final review and approval.

a. The EEO Counselor must document the settlement in writing if one is achieved.

b. The EEO Counselor must coordinate with and solicit guidance and advice from EEO regarding any proposed settlement.
c. EEO Counselors cannot execute settlement of pre-complaints without first communicating with EEO.
d. All settlements must be reviewed by EEO and approved by the respective Settlement Official prior to execution.
e. EEO will be responsible for securing all necessary signatures on the agreement, disseminating copies of the agreement to the parties, implementing and monitoring compliance with the terms of the settlement.
f. Once a settlement agreement has been executed, the EEO Counselor will submit all paperwork generated during the pre-complaint process to EEO and close out the case within three **(3)** business days of the agreement being signed.

Withdrawal

If the AP elects to withdraw the pre-complaint, the withdrawal must be obtained in writing on the requisite Withdrawal Form. Once a pre-complaint has been withdrawn, the EEO Counselor will submit all paperwork generated during the pre-complaint process to EEO and close out the case within 2 days of receipt of the withdrawal form.

EEO Counselor's Report

The EEO Counselor is responsible for submitting a final copy of the EEO Counselor's Report along with all paperwork gathered during the counseling process to EEO within 3 days of conducting the Final Interview/issuing the Notice of Right to File Formal.

a. The counseling shall be conducted in accordance with the EEO regulations set forth at 29 CFR § 1614.105; MD-110, Chapter 2; and EEOC's "A Guide to Effective EEO Counseling." The contactor shall provide as a part of the Final EEO Counselor's Report information detailing the specific claim(s) raised during EEO counseling. Each claim shall show:

   a) The bases of discrimination alleged for the claim.
   b) The specific act taken by management which gave rise to the claim.
   c) The specific date or timeframe during which the alleged discrimination occurred.
   d) The identification of the management official(s) involved in the act(s) alleged in the claim.

b. The EEO Counselor's Report shall reflect that the Counselor notified the Aggrieved Party that only matters covered in EEO counseling can be raised in a formal ICE EEO complaint unless the matter occurs after the EEO counseling session has ended.

c. Unless otherwise specified, the contractor shall submit a copy of the final EEO Counselor's Report to the Aggrieved Party, a copy to the Aggrieved Party's

representative, where one has been designated and the original and a copy of the Counselor's Report to the EEO, within **three (3)** days of the final interview and issuance of the Notice of Right to File a Formal complaint or within five days of the signing of a Settlement Agreement.

d. Special Protocols.

1. When a Counselor requires an interview with a member of the Senior Executive Service, including Directorate and Staff Office Heads or their direct reports, the Counselor will first contact EEO. EEO will facilitate the scheduling of the initial interviews.

2. Counselors must take all necessary precautions to safeguard PII or other sensitive information including law enforcement investigative documents, techniques or procedures, and all equipment used during the conduct of the investigation.

8. ALTERNATIVE DISPUTE RESOLUTION FOR EEO MATTERS

The Commission's regulations at 29 C.F.R. § 1614.102 (b)(2) require agencies to establish or make available an EEO ADR program. The EEO ADR program must be available during the pre-complaint process and the formal complaint process. The Commission regulations extend the counseling period when EEO ADR is used. See 29 C.F.R. § 1614.105(f).

a. When requested, the contractor will provide ADR services. ADR service providers must meet the certification and/or licensing requirements, if required, for the state in which the ADR services are provided.

b. ADR Practitioners must meet and comply with the requirements contained in 29 C.F.R. § 1614.102(b)(3) and EEOC Management Directive 110, Chapter 3, Section B (c).

c. The Contractor is required to adhere to the Model Standards of Conduct for Mediators promulgated by the Society of Professionals in Dispute Resolution, the American Arbitration Association, and the American Bar Association.

d. Mediations will be conducted virtually unless special circumstances warrant a different arrangement.

e. The mediator will objectively listen to the claims affecting the complainant and the Agency and engagement in alternative methods of dispute resolution, as appropriate, (e.g., mediation, fact finding, ombudsman meeting, dispute panels, and facilitated discussion.

f. The Contractor shall advise the principal parties of the time and place for the ADR meeting(s). The Contractor shall conduct meetings, jointly or separately, and shall explore with the parties' various options for resolving the dispute. Meetings shall be

conducted during normal duty hours of the principal parties. The Contractor shall also mediate like, or related issues raised during the ADR process, after coordination and negotiation of price(s) with the ICE PM.

g. Initial Meeting: The Contractor shall, before beginning ADR and throughout the process, review with the parties the ADR process, respective responsibilities of the dispute resolution professional and the parties, affirm the party's willingness to participate in the process, and fully explain EEO procedures and guidelines relating to ADR.

h. Identification of Issue(s) and Basis(es): The Contractor shall encourage and elicit sufficient information from the parties to ensure that the issue(s) is clearly defined.

i. Agreement: If the allegation(s) is resolved and full or partial agreement is reached on the substance of the dispute, the Contractor shall prepare the proposed agreement in writing. However, before resolving any complaint or entering into any settlement agreement, ICE ADR Policy and Delegation of Authority requires that the Settlement Official must consult the Office of the Principal Legal Advisor (OPLA), Labor and Employment Law Division, for guidance and legal review. If a personnel action (e.g., reassignment, transfer, disciplinary action) is involved, the Settlement Official and OPLA will consult with the Office of Human Capital (OHC) for its guidance and administrative support, as appropriate.

j. Settlement: Terms agreed during the mediation will be presented to EEO prior to obtaining additional approvals. Draft terms of the agreement will be provided via email to EEO, which will then prepare the Negotiated Settlement Agreement for both parties to sign.

k. The Contractor shall send an electronic copy of the signed agreement to EEO. EEO shall provide an original agreement to the complainant.

l. Closure: When it becomes apparent to the Contractor that resolution will not be reached, the Contractor shall inform the parties that their efforts to settle the dispute have been unsuccessful and shall close the ADR process. The Contractor shall maintain confidentiality in the process unless required to by law.

m. Information Exchange: The Contractor shall determine whether the parties need to share information about the dispute. This exchange of information shall be coordinated, and its scope limited by the Contractor, and may be accomplished through exchanges of information across the negotiating table by way of stipulations as to the facts, or as determined by the Contractor. The contractor will only mediate the accepted claims, not other information. When the facts are not in dispute (because the parties are familiar with each other's version of the facts and they agree on the facts), the facts are not complicated, or only the interests of the parties need to be addressed, the Contractor may determine that an exchange of information shall not be necessary.

n. When performing ADR, the Contractor will:

1. Obtain written consent agreement from the parties to participate in the ADR process.
2. Obtain the letter of authorization and other relevant documents as determined by EEO.
3. Obtain authorization on method(s) of ADR to accomplish resolution.
4. Offer reasonable accommodation and inform EEO of any accommodations that may be requested by persons with disabilities.
5. Coordinate and negotiate cost(s) for the resolution of like and related issues raised after receipt of the task order by Contractor.
6. Make available agency officials who will be able to respond to questions and who have authority to resolve the dispute.

o. Confidentiality: All information revealed during the ADR process is confidential. The Contractor shall advise the parties to the resolution attempt of their obligation to resist disclosures of information about the contents and outcomes of the ADR process. The Contractor in connection with the ADR function shall not utilize electronic devices used for recordings or transcripts of ADR proceedings or conferences. Notes taken during the mediation will be taken and destroyed by the Contractor.

p. The contractor agrees to schedule and conduct ADR within the timeframes contained in the task order.

109.. INVESTIGATION OF FORMAL DISCRIMINATION COMPLAINTS

Scope

a. The assigned contractor shall conduct investigations for formal EEO complaints filed by a current or former ICE employees or applicants for employment. The Contractor shall assign an EEO Investigator within **three (3)** days of receipt of the assignment. Within 10 days of the assignment, the EEO Investigator shall submit an Investigative Plan (IP) to EEO for review and approval. The EEO Investigator shall submit the draft report of investigation to EEO for review within 60 days after the approval of the IP. Within **60** calendar days of the assignment as specified in the Letter of Authorization; the Contractor shall submit a draft electronic copy of the Report of Investigation to EEO for review. The Contractor shall submit an electronic Final ROI to the Agency within 60 days of the assignment.

Assignment of Complaint

a. EEO shall notify the contractor of each assignment to investigate, via e-mail.
b. Upon receipt of a case assignment, the Contractor must provide the following information to EEO within **five (5)** business days:
    1) name and contact information for the assigned independent contractor.
    2) a price confirmation; and
    3) a request for a Letter of Authorization.

d. The designated Investigator shall, within **two (2)** business days of case assignment, call or email the designated Agency POC to discuss any applicable Collective Bargaining Unit (CBU) Procedures or special requirements pertaining to any of the proposed affiants, including members of the Senior Executive Service. In all cases where a complainant has a representative, the investigator must contact the representative or attorney to coordinate the complainant's interview(s).

Assignment of Investigator

a. The Contractor shall assign an investigator within **(5)** business days of receipt of the assignment, acceptance letter and the Program Manager (PM) issue a Letter of Authorization for the assigned investigator.

b. The PM shall issue a Letter of Authorization (LOA) for up to **60** calendar days upon notification from the assigned contractor in the name of the contractor's assigned investigator. The Investigator is required to provide Complainant/Responding Management Official (RMO)/witnesses with a copy of the LOA. The LOA can be presented via email. The investigator shall provide a copy of the LOA with the initial request for documents.

Agency Point of Contact Person

The investigator will be provided the name of a contact person (POC) within EEO.

Within 5 days, the investigator shall notify the contact person regarding any difficulties with the required actions including all logistical support, i.e., scheduling of interviews, and obtaining documents and data.

Investigative Plan

The investigator shall submit an Investigative Plan (IP) within **five (5)** business days of receiving the Letter of Authorization to the Agency POC. The IP shall contain a list of witnesses, a list of documents needed for the investigation, the scope of the investigation, and the anticipated areas of questioning and questions. EEO shall review and approve the IP The Contractor shall not await approval of the IP and/or delay commencing the investigation pending a review of the IP.

a. Special Protocols.

1. When an Investigator requires an interview with a member of the Senior Executive Service, including Directorate and Staff Office Heads or their direct reports, the Investigator will first contact EEO. EEO will facilitate the scheduling of the initial interviews.

2. Document requests from individuals identified above must be submitted to EEO. EEO will be responsible for the coordination and collection of these documents.

The required documents will be provided to the investigator by the EEO PM.

3. Investigators must take all necessary precautions to safeguard PII or other sensitive information including law enforcement investigative documents, techniques or procedures, and all equipment used during the conduct of the investigation.

Document Requests

The document request should be clearly identified in the investigative plan and submitted in writing to the POC within **five (5)** business days of receiving the Letter of Authorization. The document request should specify a firm deadline, not to exceed **20 business days** for the return of the requested documents. If the investigator encounters difficulties in obtaining documents, the investigator shall immediately inform their EEO POC and the PM to solicit assistance in obtaining the documents. At least two documented attempts should be made to obtain the documents. If the documents have not been received and/or the Agency has not requested additional time; the Contractor shall elevate the issue of delays/non-cooperation to the EEO POC with a copy to the PM.

Scheduling Interviews

Unless prior approval is required before contacting a witness (such as a member of the Senior Executive Service), the Contractor shall contact the Complainant/witnesses directly to schedule interviews.

Affidavits

a. The investigator shall take Complainant's affidavit first.
b. Affidavits should be in question-and-answer format. The investigator is not required to administer an Oath. Instead, the affiant shall sign an affidavit swearing or affirming the truthfulness of their testimony. This affidavit will become an official part of the ROI.

c. Draft affidavits shall be emailed to the affiants and the affiant shall be informed that corrections or additions to the affidavit shall be made directly into the document. The affiant has **four (4) business days** to e-mail back the affidavit with an electronic signature (/s/ Name).

d. If Complainant or any other witness fails to submit their signed affidavit within the specified time frame, a 15-day demand letter should be issued to Complainant or witness advising that the ROI may be submitted without their affidavit. A copy of the 15-day letter should be forwarded to the POC. The investigator should have documentation that the 15-day letter was sent by either (1) certified mail, return receipt requested; or (2) by email with a delivery and read confirmation.

e. Affiants are permitted to make non-substantive revisions to their affidavits. The Investigator should require the affiant to make any necessary revisions electronically and directly into the document (using track changes).

f. Affidavits shall be signed and dated. Electronic signatures are acceptable.

Witnesses

a. Either in the initial conversation with Complainant or at the end of Complainant's interview, the Investigator shall ask the Complainant for a list of witnesses they want interviewed, including a proffer of their testimony. The Complainant's witness list will be included as an Exhibit in the ROI. A Memorandum to the File should be included to reflect any reasons why the investigator determined not to interview some or all of the listed witnesses.

b. Testimony may be obtained, and the investigation may be completed using all the available methods contained within MD-110.

c. The Investigator is responsible for identifying all relevant witnesses whether identified by Complainant or not.

Rebuttal

a. Complainant shall be given a rebuttal opportunity. Complainant can either (1) prepare a rebuttal to management's statements for inclusion in the ROI; or (2) reserve the right to rebut management's statements only, upon receipt and review of the entire Report of Investigation. If Complainant seeks to reserve his/her rights, the Investigator shall obtain a signed and dated Reservation of Rights memorandum for the file.

b. If Complainant elects to provide a rebuttal, the Investigator shall provide Complainant with copies of the RMOs signed affidavits. The Investigator shall inform Complainant of the purpose of the rebuttal and that the rebuttal should not restate information provided in the original affidavit. If the investigator anticipates a lengthy rebuttal or one which restates the affidavit, the Investigator may (1) interview Complainant for rebuttal purposes; (2) provide Complainant with a summary of management's defenses; and (3) draft a rebuttal for Complainant's signature based on the interview conducted.

c. The ROI shall contain a brief summary of relevant portions of Complainant's rebuttal statement.

Terminology

a. Complainant should be referred to as "Complainant" and not "the Complainant".

b. RMO is "Responsible Management Official" and not "Responding Management Official."

c. Witness should be identified by their respective roles: Agency Witness, Complainant Witness, and/or Expert Witness.

Non-Cooperation/15-Day Demand Letter

a. If the Complainant or a witness is uncooperative, the investigator will immediately notify the Contractor POC and the PM. Non-cooperation includes witnesses (including Complainant) who are reluctant to participate; indicate that work responsibilities or absence from the workplace will delay their participation; are non-responsive to request for their affidavit; and/or who delay the return of their affidavits. Non-cooperation further includes the failure to return or delay in returning requested documents.

b. The Contractor shall immediately notify the Agency POC and PM of any delays experienced. The Agency shall assist in resolving any delays. The Contractor shall make at least **two (2)** documented attempts to compel cooperation. The Contractor shall evaluate concerns of non-cooperation to the PM for assistance.

c. After **two (2)** documented attempts to obtain cooperation, the Contractor shall issue the 10-Day Demand letter. This 15-day Demand letter applies to the Complainant, RMOs, Witnesses and the Agency when the Contractor has timely made the requisite documented attempts to obtain testimony and documents.

Extensions

a. Investigations shall be completed within **75 days** of the assignment made. The contractor shall forward all requests for an extension of the Letter of Authorization in writing to the Contractor POC with a copy to the PM.

b. A request by the Contractor to extend an investigation beyond the period stipulated in the LOA must be submitted in writing to the POC at least **ten (10)** days before the due date for the ROI.

c. The requests shall contain the specific reason(s) why the investigator could not complete the investigation within the specified time frame. All attempts to obtain testimony and requested documents shall be fully documented. A one-time, **10 calendar day** extension may be considered, unless there are unusual circumstances warranting a longer extension.

Delay of Work

a. If the performance of work is delayed or interrupted by failure of the Agency or complainant to act within a reasonable time (5 business days of the investigator's initial contact or requested deadline), the investigator must immediately advise the POC and EEO Investigation's Program Manager (PM). When a witness refuses to cooperate, the investigator must immediately contact the POC. The POC will attempt to resolve the delay or advise the investigator on how to proceed. The investigator must document the file regarding all attempts to gain responses to his/her requests from the witnesses. The

investigator shall utilize the 15-day letter in obtaining affidavits and documents after at least two attempts to secure the information.

b. If the performance of work is delayed or interrupted by failure of the investigator to act within the time frames specified in the award, the POC must notify the Contractor, or if the matter comes to the attention of the Contractor, they will notify the POC as soon as possible. If the Agency and Contractor are unable to resolve any outstanding issues, the investigator must be replaced with a qualified investigator. If the delay of work cannot be resolved the PM has the right to cancel the order. In the event the PM cancels the order, the Contractor must return the case(s) to the POC within 2 business days of notification.

Privacy Act

In order to be in compliance with the Privacy Act, investigators shall not disclose Privacy Act protected information of a witness with any other witness. This includes, but is not limited to, social security numbers, dates of birth, home addresses, phone numbers, medical information, salary information or any other information protected by the Privacy Act. If the investigator is unsure about what information they may release they should contact their Contractor POC or EEO PM.

Report of Investigation (ROI) Format and Submission

a. ICE uses the MD-110 format for Reports of Investigation. A Memorandum to the File shall be included to explain any missing information to include missing and/or unsigned affidavits and missing documents. The exhibit Index shall reference all exhibits either alphabetically (Exhibit A) or numerically (Exhibit 1).

b. All dates should be written out: August 27, 2007, not 8/27/07. Where age is a basis, the date of birth and witness's age shall be provided.

c. It is expected that the contractor firm will perform a thorough review of the ROI before submitting it to the EEO. The Contractor shall submit **one (1)** un-sanitized and one (1) sanitized electronic copy of the ROI to the EEO. The sanitized copy shall include the redaction of all social security numbers, salary information, dates of birth, home addresses, and home/cell phone numbers pertaining to any witness. All Privacy Act protected information shall be redacted from all copies of the ROI prior to submitting them to the EEO.

d. The ROI will not contain any reference to the validity or merits of a complaint, nor shall it render any legal opinions or analysis with regard to the Complainant's claims. The ROI should be factual in nature based on the information provided during the course of the investigation.

e. After providing notice to the complainant, in accordance with MD-110, Ch. 5 (A,3), the agency may unilaterally extend the time period or any period of extension for no more than thirty (30) days where it must sanitize a complaint file that may contain information

classified pursuant to Executive Order 12356 or successor orders as secret in the interest of national defense or foreign policy. 29 C.F.R. § 1614.108(e).

Sufficiency of ROI

a. The ROI will be reviewed by EEO for sufficiency. If the ROI is deemed to be deficient, the Contractor will be notified immediately. EEO has **10** days to notify the contractor of any deficiencies in the ROI. Deficiencies may include obtaining additional documents, interviewing additional appropriate witnesses, and interviewing witnesses already interviewed in order to ensure their affidavits are complete.

b. The ROI may be returned to the Contractor for additional work, including a request to correct any errors and/or to perform a supplemental investigation. The ROI must include an accurate summary of statements made in the affidavits and summary of relevant documents. The ROI summary shall not include any information not supported by affidavits, documents and/or Memoranda to the File.

c. The ROI will not contain any reference to the validity or credence of the complaint, nor shall it render any "legal opinions" with regard to Complainant's claims. The ROI will be factual in nature based on the information provided during the course of the investigation.

d. If the ROI is returned for additional work and/or to rectify any deficiencies cited, the Contractor shall have 10 days to cure any deficiencies. The contractor shall have an agreed upon time, generally, no more than 30 days if a supplemental investigation is required.

Amendments/New Basis

a. It is the responsibility of the Complainant to notify EEO of any new claims. If the Complainant notifies the Investigator of a new claim, the Investigator must advise the Complainant to notify EEO in writing, of any new claims. EEO will provide the investigator with a copy of the amended acceptance letter if the new claims are accepted. Under no circumstances shall the Investigator investigate any claims without approval and authorization from the Agency and the PM.

b. Unless otherwise specified, the Investigator used in the original complaint shall investigate the amended claims. The Contractor shall notify the PM as to how far the investigation has progressed to determine whether the ongoing investigation can include the new claims or whether a supplemental investigation is needed.

c. If the Agency amends the complaint after the investigation accepted by the Contractor after the Investigator has commenced interviews with the Complainant, management officials, the PM shall grant additional time as specified to complete the investigation.

d. If the Agency adds an amended issue or consolidated complaint to the investigation accepted by the Contractor after the Investigator has commenced interviews with the Complainant, management officials, and has substantially completed the investigation, the PM shall negotiate an additional compensation with the Contractor up to the cost of a new or supplemental investigation. An investigation is considered substantially completed when (1) all interviews have been conducted and signed affidavits have been obtained; (2) all documents have been requested and obtained; and (3) the ROI summary has been drafted, in the process of being drafted, in production, or in route to the Agency.

e. Complainants are permitted to raise a new basis at any stage of the investigative process. The investigator should inform the Complainant to notify EEO if there are new basis/bases. If the investigation is near completion, the Contractor must contact the PM to discuss any additional investigation cost in obtaining documentation relevant to the new basis/bases. The Agency will review the Complainant's request to add a basis and determine whether a letter of amendment is required.

Witnesses No Longer with the Agency

a. If a witness has retired or left federal service, the investigator must contact the POC to obtain contact information. The investigator must attempt to contact the witness to ascertain whether the witness is willing to testify.

b. If the witness declines to testify, the investigator must document the witnesses' decision in the ROI, citing the exhibit containing the dates and method of contact. If a witness has left the agency but remains in the federal service, they are required to cooperate.

10. DRAFT PROCEDURAL DISMISSALS

Scope

The assigned contractor shall complete the preparation of a draft procedural dismissal (full or partials) or draft Final Agency Decision within 30 days of receipt of the pre-complaint administrative file or **30 days** of its receipt of the Report of Investigation and the administrative file. The contractor shall submit the draft electronically to EEO.

Analyses for Draft Procedural Dismissals or Draft Final Agency Decisions

The Contractor shall prepare a draft procedural dismissal or draft FAD which discusses and analyzes all claims presented in the pre-complaint or formal complaint. The analysis shall consist of a presentation of facts, and recommended findings and conclusions. The analysis shall be clear, concise, logical, well-reasoned, well documented, and fully supported. It should include all procedural and substantive issues presented and generally, should conform to the following:

- Introduction – This section will provide the complainant's name, title, grade, organizational unit, basis(es), issue(s) and nature of the complaint.

- Background – This section will provide a procedural history of the complaint.
- Claim(s) – This section will state the claim(s) as accepted in the formal complaint and that will be addressed in the FAD analysis.
- Analysis – This section will consist of a discussion of the applicable judicial and administrative case law governing the identified claim(s).
- Burden of Proof – This section will delineate the relevant and appropriate standards for the burden of proof based on the facts and circumstances for each complaint.
- Evidence – This section will provide an application of the case law to the facts of the case, i.e., evidence of a prima facie case, the Agency's articulated non-discriminatory reason for its action(s), and evidence of pretext.

Submitting the Draft Procedural Dismissal or Draft FAD

a. The Contractor shall deliver a draft procedural dismissal within 15 days, or draft FAD within **30 calendar days**, or as otherwise specified to the task order. EEO shall review the draft procedural dismissal or draft FAD and may return it for any revisions. If required, the Contractor shall return the revised FAD via email within five days of receipt for final approval.

b. The Contractor's recommended findings and conclusions are not binding on the Agency.

11. NOTIFICATION OF SIGNIFICANT EVENTS

a. The Contractor shall notify EEO immediately of any noteworthy events occurring during the course of an assignment. Significant events include but are not limited to signed consents to extend; non-cooperation; issuance of Notice of Right to File a Formal Complaint; Withdrawals; Reservation of Rights; and/or extended illnesses or absences of witnesses.

b. Upon the determination of a significant event, the Contractor shall notify EEO with an email outlining the significant event and attaching any document/notification pertaining to the significant event. The Contractor should not wait until the completion of a case before notifying EEO of a significant event.

COMPLIANCE MONITORING

The Contractor may be required to provide services to assist in monitoring the implementation of EEOC Orders, Judgements, or Settlement Agreements. If required, the work will be done consistent with a document outlining the expectations for such work.

12. BI - WEEKLY STATUS REPORTS ON COUSELING

a. The Contractor must submit a bi-weekly status report to the Agency POC and PM every other Friday, until the Notice of Right to File a Formal Complaint has been issued.

b. If a case is still open beyond the 30-day counseling period, the status report shall include a statement as to when a Consent to Extend the Counseling Period was obtained and the reason for the delay.

13. MONTHLY STATUS REPORTS ON INVESTIGATIONS AND FADS

a. The Contractor must submit a monthly status report to the POC and PM the 5th of each month.
b. If a case is still open beyond the assigned due date, the status report shall include a statement as to whether the case was amended; whether an extension was granted and/or obtained and by which date the contractor anticipates submitting the final work product.

14. DELIVERY SCHEDULE

Deliverable Schedule and Performance Threshold			
Location	Deliverable	Frequency	Performance Threshold
Page 4	Counseling of Pre-Complaints	Due within 20 days after initial contact	Acceptance 100% of deliverable
Page 6	Withdrawal Notification	Due within 2 days of receipt	Acceptance 100% of deliverable
Page 7	EEO Counselor's Report	Due within 3 days of final interview/issuing the Notice of Right to file formal	Final version 95% error free and contains all identified data
Page 7	Settlement Agreement ADR, EEO Counselor's Report	Due within 5 days of signing	Final version and all required documents provided, Acceptance 100%
Page 9	Alternative Dispute Resolution Authorization		
Page 10	Assignment of Complaint	Due within 5 days business days	Acceptance 100% of deliverable
Page 10	Assignment of Investigator	Due within 3 days of receipt of the assignment	Acceptance 100% of deliverable
Page 10	Letter of Authorization Email Request	Due within 5 business days	Acceptance 100% of deliverable
Page 10	Call or email designated Agency POC	Due within 2 business days	Acceptance 100% of deliverable
Page 11	Investigative Plan	Due within 10 days after assignment	Acceptance 100% of deliverable

Page 11	Draft Investigator Report of Investigation (ROI)	Due within 60 days of the assignment	Draft version 80% error free and contains all identified data
Page 11	Final Report of Investigation (ROI)	Due within 60 days of the assignment	Final version 95% error free and contains all identified data
Page 17	Draft procedure dismissal	Due within 15 days	Acceptance 100% of deliverable
Page 17	Draft Final Agency Decision (FAD)	Due within 30 calendar days	Draft version 80% error free and contains all identified data
Page 19	Status Report on Counseling	Due bi-weekly until the status changes to RTF or Formal Complaint	Acceptance 100% of deliverable

15. LATE SUBMISSIONS

Habitual lateness beyond 40 days may result in Termination for Cause in accordance with the provisions of FAR 8.406-4, Termination for causes and FAR 12.403(c).

16. DEFICIENCIES

a. If the Agency determines that a final work product is deficient in quality to include the absence of information essential to the issues; the report, summary or analysis is inadequate; and/or documents are not properly organized; the Agency will return the case file to the Contractor to remedy the deficiency.

b. If the case is returned for revisions, the Contractor will be subject to the following schedule regarding consideration to the Government for the untimely completion of revisions and return of the case file:

Time to Complete Revisions
Fifteen (15) calendar days
Thirty (30) calendar days beyond due date
Forty-five (45) calendar days beyond due date
Sixty (60) calendar days beyond due date
Beyond sixty-one (61) days

17. TERMINATION OR INTERRUPTION OF THE INVESTIGATION:

a. The Complainant and the Agency may elect to engage in alternative dispute resolution (ADR) during the course of the investigation of a complaint, or Complainant may

withdraw the complaint, file a civil action or the case may otherwise terminate or interrupt.

b. If a case is terminated or interrupted, the Contractor will be so notified to suspend, continue and/or end the investigation. The Agency shall compensate the Contractor for the documented time spent, conducting the investigation to the point where the Contractor was provided notification.

c. In the event an investigation is interrupted because of withdrawal, settlement or cancellation, the Contractor will receive written notice from the POC. The Contractor must then tab all information received from the Agency and any other information gathered, and return the information to the Agency, within 10 calendars days of notification.

d. If the case is interrupted or cancelled, the invoice must accurately reflect the stage at which the cancellation of interruption occurred.

Phase of Investigation at time of Interruption
Planning phase/ initial stage of investigation (Within 15 Calendar days of receipt of case)
During the Investigation (Within 16-45 Calendar days)
After 45 Calendar Days.

18. INVOICING INSTRUCTIONS

Payment will be processed after approval of the EEO Counselor's Report, final ROI/FAD and invoice receipt. When billing, the contractor must reference the case number, the GSA Schedule special item number (SIN), receipt date and completion date of case, description of services provided to include contract line-item number (CLIN), price and the Task Order reference number. All invoices must have Invoice and case numbers but should not include personal identifiers such as full names. Please ensure all invoices are emailed to Invoice.Consolidation@ice.dhs.gov and copy the Contract Officer/Specialist and CORs listed on the contract.

19. QUALITY REVIEW AND FEEDBACK

a. To ensure the highest quality of EEO contract services at EEO, the PM will keep track of all investigations conducted throughout ICE to ensure timeliness and quality of work.

b. Monthly feedback will be provided to the contractor firm during the fiscal year to keep the contractor firm abreast of any concerns.

c. The Contractor is asked to provide any feedback or suggestions in areas in which EEO can serve to improve the efficiency of investigations.

20. QUALITY CONTROL

The contractor shall establish and maintain a complete Quality Control Plan to ensure the services are performed in accordance with SOW the contractor's proposed technical approach and commonly accepted commercial practices. The contractor shall develop and implement procedures to identify, prevent and ensure non-recurrence of defective services. The government reserves the right to perform inspections on services provided to the extent deemed necessary to protect the government's interests. The contractor must control the quality of the services and deliverables provided in support of this task and maintain substantiating evidence that services conform to contract quality requirements and furnish such information to the government if requested. The contractor shall submit within 30 days after award a Quality Control Plan (QCP) that addresses the monitoring of employees and the tasks performed. The QCP along with any changes/updates must be pre-approved by the COR prior to implementation. The contractor shall provide the draft QCP with the proposal and the final QCP to the COR within 30 days after award.

21. GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND MATERIALS

The government will not be providing property, equipment, and materials.

22 SECURITY REQUIREMENTS

General

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

Preliminary Fitness Determination

ICE will exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for contractor employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination or final Fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination or final Fitness determination by OPR-PSU. Contract

employees are processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or successor thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. (Sexual Abuse and Assault Prevention Standards) implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003)

Background Investigations

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Contractor employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR-PSU, through the Contracting Officer Representative (COR), within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1. Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by the contractor employee in their OPM e-QIP account.

2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by the contractor employee in their OPM e-QIP account.

3. Two (2) SF 87 (Rev. December 2017) Fingerprint Cards. **(Two Original Cards sent via COR to OPR-PSU)**

4. Foreign National Relatives or Associates Statement. (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

6. Optional Form 306 Declaration for Federal Employment (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be

signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

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

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

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

An adequate and current investigation is one where the investigation is not more than five years old, meets the contract risk level requirement, and applicant has not had a break in service of more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01)

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

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

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

Transfers From Other DHS Contracts:

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

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

Continued Eligibility

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

Required Reports

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

The Contractor will report any adverse information coming to their attention concerning contractor employees under the contract to the OPR-PSU, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report

shall include the contractor employees' name and social security number, along with the adverse information being reported.

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

CORs will submit reports to [redacted]

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

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

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

Security Management

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

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

Information Technology Security Clearance

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

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

Information Technology Security Training and Oversight

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

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on PALMS or by contacting [redacted] Department contractor employees, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

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

23 INFORMATION GOVERNANCE AND PRIVACY (IGP)

PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

Limiting Access to Privacy Act and Other Sensitive Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

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

Prior Approval Required to Hire Subcontractors

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

Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.
As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist

by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights

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

Privacy Lead Requirements

If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

25 General Cybersecurity Contract Requirements

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

Compliance with DHS Security Policy Terms and Conditions:

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

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

Security Review Terms and Conditions

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer

Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

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

Security Requirements For Unclassified Information Technology Resources (JUN 2006)

The Contractor shall be responsible for IT security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer (CO), shall be incorporated into the contract as a compliance document.

The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the FISMA of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Examples of tasks that require security provisions include:

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

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

At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

A.5.1 Contractor IT Security Accreditation

Contractor IT Security Accreditation

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (most current version) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

A.6 In accordance with HSAR 3052.204-71 - Contractor Employee Access

Contractor Employee Access (Sep 2012)

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

This definition includes the following categories of information:

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

b) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security

(including the Assistant Secretary for the Transportation Security Administration or his/her designee);

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

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

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

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

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

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

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

A.7 In accordance with ITAR 4.5.3.10 – Contractor Employee Access Clause (use language from HSAR 3052.204-70 and alternates at 3052.204-71).

A.7.1 Alternate I

Contractor IT Resource Access (Sep 2012)

1) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange and complete any nondisclosure agreement furnished by DHS.

2) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

    1) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

3) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

4) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

    a) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

    b) The waiver must be in the best interest of the Government.

    2) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

A.7.2 Alternate II

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

1) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any

exceptions must be approved by the Department's Chief Security Officer or designee.

2) Contractors shall identify in their proposals, the names, and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer

A.8 In accordance with White House Digital Government BYODTK – Privacy Expectations

Privacy Expectations

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

A.9 In accordance with HSAR Class Deviation 15-01, Special Clause, Safeguarding of Sensitive Information (MAR 2015)

Safeguarding of Sensitive Information (MAR 2015)

a) **Applicability.** This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

b) **Definitions**. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet

protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:
(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

c) **Authorities.** The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (most current version), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (most current version), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of

the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring

and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available

at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance.* The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident.

(ii) A description of the types of PII and SPII involved.

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means.

(iv) Steps individuals may take to protect themselves.

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services

shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring.

(ii) Daily customer service.

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period.

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores.

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics.

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate.

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

A.10 In accordance with HSAR Class Deviation 15-01, Special Clause, Information Technology Security and Privacy Training (MAR 2015)

Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract

award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

Privacy Training Requirements.

All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than

October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.