Privacy Impact Assessment

for the

Public-Private Sector Analytic Exchange Program (AEP)

DHS Reference No. DHS/I&A/PIA-001

July 30, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) acts as an Executive Agent for the Public-Private Sector Analytic Exchange Program ("AEP" or "the Program") on behalf of the Office of the Director of National Intelligence (ODNI). The purpose of the AEP is to provide intelligence community (IC) and federal, state, local, tribal, and territorial (FSLTT) intelligence analysts the opportunity to engage with volunteer private sector analysts to better understand select national security and homeland security issues. All participants are selected through a competitive application process. AEP participants work to create unclassified joint analytic deliverables of interest to both the private sector and the U.S. Government.[1] I&A is publishing this privacy impact assessment (PIA) because I&A collects personally identifiable information from individuals applying to, and selected for, the AEP in order to verify their U.S. citizenship, facilitate entry into federal buildings, facilitate reimbursement of their travel expenses, and enable access to federally-maintained information technology platforms used to facilitate public-private collaboration.

Overview

The AEP is an interagency program created by the ODNI pursuant to Intelligence Community Directive (ICD) 205,[2] which established policy for Analytic Outreach as an essential factor in the production of intelligence analysis. Analytic Outreach is the overt and deliberate engagement by an IC analytic component with individuals or organizations outside the IC to explore ideas and alternative perspectives, gain insights, or generate new knowledge. In furtherance of the goals and policies of ICD 205, the DNI (Director of National Intelligence) established the AEP via Memorandum for Distribution No. ES 2015-00524, August 24, 2014, to provide a mechanism for engagement and collaboration with the private sector in order to conduct analytical outreach and provide recommendations on how to improve upon IC priorities and further other homeland and/or national security goals.

One of I&A's existing missions is to engage with the private sector. Because of this, I&A's membership in the IC, its relationship with private sector entities, and its historical involvement in similar programs, the DNI Memorandum designated I&A to (1) serve as the Executive Agent of the AEP and develop and maintain any services of common concern related thereto on behalf of the IC; (2) develop policies, procedures, and guidelines implementing the AEP; (3) advise the DNI on resources, funding, and other requirements and processes related to the AEP; and (4) ensure that the AEP complies with all applicable laws, regulations, and policies. ODNI and DHS entered

[1] For more information about the AEP and a sampling of deliverables from the program from years past, *see* https://www.dhs.gov/private-sector-engagement and https://www.dhs.gov/aep-deliverables.
[2] Intelligence Community Directive Number 205 (ICD 205) (July 2008), *available at* https://www.dni.gov/files/documents/ICD/ICD_205.pdf.

into a Memorandum of Agreement on August 24, 2015, to establish their respective roles and responsibilities related to the AEP.

The Secretary of Homeland Security subsequently established the AEP Committee by charter pursuant to ICD 205, Executive Order 12333, as amended, and the Homeland Security Act of 2002 (Pub. L. 107-296, 6 U.S.C. 101 *et seq*.), as amended. Pursuant to Section 871(a) of the Homeland Security Act, the Secretary exempted the AEP Committee from the requirements enumerated in the Federal Advisory Committee Act (FACA) (Pub. L. 92-463, 5 U.S.C.A. App. 2). The AEP Committee serves as the principle mechanism by which I&A implements the AEP on behalf of the Secretary and DNI. It provides the forum in which FSLTT and private sector personnel will engage and collaborate on matters and issues affecting national security. This charter was most recently renewed on March 18, 2020.

The Director of I&A's Partner Engagement Office, within the Field Operations Division (FOD), serves as the Chairman of the AEP Committee, which is composed of up to 100 individuals from the IC and FSLTT partners, as well as up to 100 private sector representatives from critical infrastructure sectors. The Chief of I&A Partner Engagement Office, Private Sector Engagement (PSE) serves as the Vice Chairman of the AEP Committee. The chief of the I&A Private Sector Engagement (PSE) Branch within the I&A Partnership Office serves in the capacity of a FACA Designated Federal Officer. These I&A personnel, in their capacities as Committee Chairmen and Vice Chairmen, are responsible for:

- Overseeing the application, selection, and participation processes for the AEP Committee and AEP Subcommittee members, including all security and counterintelligence vetting and screening procedures;
- Convening all AEP Committee meetings, including established time, locations, participation, and agendas;
- Establishing meetings with AEP Subcommittee leadership members, and discussing all other personnel and membership matters therein;
- Identifying, in coordination and consultation with the Undersecretary for Intelligence and Analysis (USIA) or other IC elements, the subject matter, focus, goals, and scope of the AEP Committee and Subcommittees;
- Coordinating and consulting with the Office of General Counsel – Intelligence Law Division (OGC-ILD) prior to dissemination of all AEP Committee and/or AEP Subcommittee recommendations, policy advice, analytical assessments, reports, and other deliverables outside of the AEP Committee;
- Renewing the AEP Charter (or any superseding documentation) every two years, in consultation with OGC-ILD, and, as appropriate, making recommendations to amend

or alter said documentation;

- Developing and maintaining measurements of progress and all other relevant metrics related to the AEP Committee;
- Performing any other relevant administrative functions, as appropriate; and
- Publishing to the general public, to the extent reasonably practicable, all processes, procedures, agendas (including the agendas of the opening and concluding summits of the AEP), and reports (including final subcommittee reports) described in the AEP charter.

In addition, the FACA Designated Federal Officer is responsible for:

- Creating and/or approving, as well as implementing, AEP Committee governance and operational rules, standards, guidelines, procedures, and policies; and
- Terminating any committee or subcommittee meetings that exceed the scope of the AEP Charter.

It is pursuant to the above enumerated functions that I&A collects, uses, shares, and retains personally identifiable information of AEP applicants and participants. The annual application process begins when the I&A AEP staff disseminate the application window announcement, which remains open for a minimum of four to six weeks. The announcement includes the program overview, application form, topic descriptions, supervisor endorsement form, and a request for a resume. Applicants must provide contact information, answer essay questions, and select prioritized topics, as well as provide a separate resume. The applicants' supervisors must also provide their contact information, a yes/no selection for endorsement, and may choose to provide additional information. All applications are received into the AEP Submissions inbox. AEP staff perform an initial review of all application packages and save them onto the AEP shared drive, on the unclassified DHS-wide computer system, using the file naming convention of Last Name, First Name, and whether the document is an Application, Endorsement, or Resume. All applicant information is additionally entered into an Application Tracker on the same shared drive, which is simply a spreadsheet used to maintain a consolidated list of all documents received and identify topics selected by applicants.

Once the AEP staff have assembled a selection panel (which consists of senior I&A and ODNI personnel from their respective Partner Engagement offices), AEP staff then provide those panel members with binders including physical copies of all completed application packages and summary sheets of applicants by group for review. The summary sheets are a modified version of the application tracker, reflecting verification of the documents received, topics selected, individual's name, and company. Two completed binders, one each for public sector and private sector applications, are provided to each selection board member (from both DHS and ODNI) prior

to the time of the selection panel so that they have sufficient time to review the application package. Once the panel has made their selections, AEP staff document the information, and the selection board members return the application binders to the AEP staff to destroy, by shredding, all hard copies. The records are updated with the panel results.

All applicants are notified of their status via email. Private sector provisional selectees subsequently receive a notice of provisional acceptance, subject to additional vetting as outlined below. The public sector provisional selectees receive a notice of acceptance. Non-selectees receive a notice of denial, and their applications remain on file for that cycle for two months. If selected participants are not available to participate in the program, due to life circumstances, the AEP staff will review the resumes of non-selectees to extend this opportunity to another applicant. All applications are saved on the shared drive on the unclassified network.

The AEP staff then solicit from the private sector provisional selectees additional personally identifiable information, including full name, date of birth, place of birth, and Social Security number (SSN). As is explained to the provisional selectees, this additional security related information, to include the SSN, is used for several purposes:

- DHS's U.S. Citizenship & Immigration Services (USCIS) verifies U.S. citizenship for private sector participants, which is a requirement for the program, as per the AEP Standard Operating Procedure (SOP);
- DHS's Office of the Chief Security Operations (OCSO) facilitates access to DHS facilities by conducting a background check in the National Crime Information Center (NCIC) database,[3] which is maintained by the Federal Bureau of Investigation (FBI) and which requires the entry of the applicant's SSN;
- Facilitate group access to other federal facilities that require the submission of name, SSN, date of birth, and/or place of birth; and
- Facilitate government-funded travel and direct deposit of reimbursement of participants' travel expenses, including through a government travel management application called Concur.[4]

Separately, private sector provisional selectees must disclose certain types of foreign associations, including:

- Any dual citizenship;

[3] *See* Privacy Impact Assessment for the National Crime Information Center (NCIC), *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.
[4] *See* ConcurGov Privacy Impact Assessment, *available at* https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

- Foreign identification (e.g., passports, visas, licenses, border crossings);
- Recent (within one-year) or Continuous Foreign Contacts (e.g., telephone, email, social media, foreign officials, foreign companies, family ties to a foreign country, foreign acquaintances, foreign exchanges, or foreign organizations);
- Foreign travel (last two years dates/visit locations), indicate official business or personal;
- Foreign affiliation (i.e., U.S.-based foreign organizations, foreign nongovernmental organizations (NGOs), foreign education, foreign employment, receiving foreign support) - (indicate yes or no; if yes, what foreign country?);
- Foreign property (indicate yes or no; if yes, in what country?);
- Foreign bank accounts (indicate yes or no; if yes, in what country?); and
- Sponsorship of foreign nationals (e.g., visas, immigration) (indicate yes or no).

The purpose of collecting information related to foreign associations is to facilitate an inquiry into potential counterintelligence (CI) risks to DHS and ODNI that might result from a particular individual's selection to the AEP. Because the AEP addresses issues that are a priority for the IC and because AEP participants must collaborate closely with U.S. Government personnel, including IC personnel and sometimes even IC personnel in highly sensitive positions, the AEP must ensure that it is not accepting applicants it reasonably believes constitute a CI risk.

The AEP staff provides the information on foreign associations to OCSO, which checks unclassified commercial databases (e.g., Bloomberg, LexisNexis, Dun & Bradstreet), as well as DHS databases that can be used to confirm foreign travel.[5] Additionally, the I&A Counterintelligence Mission Center (CIMC) conducts classified system checks on the selectee's employer, to vet foreign ties.

After OCSO completes its own checks, if OCSO determines that an AEP provisional selectee has significant foreign ties, OCSO then sends the selectee's personally identifiable information to the I&A CIMC. The CIMC conducts classified systems checks on the selectee to vet the foreign ties. The CIMC then either informs the AEP staff that they found no information indicating a CI risk or provides AEP staff a summary response that details the nature of the CI risk a particular conditional selectee poses, the level of that risk, and any information supporting that risk assessment.

[5] More information about OCSO's background check process can be found in DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

AEP staff save the additional information collected from the selectees via DHS Form 11000-13 as a password protected document. AEP staff also convey the information collected to OCSO via emails, in accordance with DHS protocols. USCIS enters the data into their Central Index System (CIS) database[6] in order to verify that the selectee is a U.S. citizen. OCSO also enters the data into the NCIC database in order to determine whether the selectee has any criminal history that would preclude the selectee's access to DHS facilities. Both offices then send an email back to AEP staff that verifies that the private sector participant's U.S. citizenship has been vetted and that no other issues were identified.

AEP staff also convey the selectees' full name, email, and phone number collected on the AEP Application form to the Defense Intelligence Agency (DIA) via an email with a password protected document. This information is used to create an account for the selectee to access the DIA secure collaborative platform known as the "Strategic Analytic Gateway for Expertise" (SAGE).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The legal authority for DHS to act as Executive Agent for the AEP arises from 50 U.S.C. Chapter 15 (the National Security Act of 1947, as amended); Executive Order 12333, as amended; and ICD 205, as well as the Homeland Security Act of 2002 (Pub. L. 107-296, 6 U.S.C. 101 *et seq*.), as amended, which authorized the Secretary of Homeland Security to enter into a Memorandum of Understanding (MOU) with ODNI and to establish the AEP Committee via charter. The MOU between ODNI and DHS governing the AEP is additionally subject to DNI Memorandum 10-00960, "Designation of Services of Common Concern." Pursuant to these authorities, DHS collects, uses, and retains the personally identifiable information of AEP applicants and participants.

The collection of an SSN is required because of some of the facilities to which the AEP participants must access in order to participate in the Program have access requirements that typically involve a background check. DHS and most other federal agencies have general authority under 40 U.S.C. 1315 to protect the buildings, grounds, and property owned, occupied, or secured by the Federal Government, and the persons on the property. The DHS Chief Security Officer has been formally delegated the authorities and responsibilities for the performance of security functions within the Department. Access to DHS physical facilities is governed by DHS Instruction Manual 121-01-011-01, *Visitor Management for DHS Headquarters and DHS Component Headquarters Facilities*, which establishes visitor management guidance and

[6] *See* DHS/USCIS/PIA-009 Central Index System (CIS), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

requirements for protecting DHS personnel and resources. Specifically, the manual covers management of visitor access into DHS HQ and DHS Component facilities according to visitor category, methods for identifying individuals, and by maintaining "Do Not Admit" lists. This Instruction Manual provides that the OCSO runs checks in NCIC, which are not possible without entry of the individual's SSN.

The legal authority for the CIMC to conduct inquiries into possible counterintelligence risks, with OCSO's assistance, is Executive Order 12333, pursuant to which the Under Secretary for Intelligence and Analysis (USIA) is authorized to collect information concerning, and conduct activities to protect against, intelligence activities directed against the United States by foreign powers, organizations, persons, and their agents.[7] Furthermore, the USIA is tasked with protecting the security of intelligence-related activities, information, and employees by appropriate means.[8]

I&A's Intelligence Oversight Guidelines (I&A IO Guidelines)[9] permit the conduct of intelligence activities for an authorized intelligence mission. Protecting against intelligence activities directed against the United States is an authorized national mission for I&A personnel. Performing CI vetting of AEP applicants to assess if they are connected to foreign intelligence entities (FIE) fits within the national intelligence mission.

I&A's IO Guidelines permit I&A personnel to intentionally collect U.S. Person information (USPI) where they have a reasonable belief that the collection activity furthers one or more of the national or departmental missions (as listed in Section 1.1 therein) and will result in the acquisition of USPI that falls within one or more of the standard or supplemental information categories (described in Section 2.2.3 therein).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The Office of Intelligence & Analysis Enterprise Records System (ERS) SORN[10] allows the Department to integrate the intelligence and information sharing functions and activities of the DHS intelligence enterprise to provide the most valuable, actionable intelligence and intelligence-related information for the Nation's leadership, all components of DHS, the IC, and other DHS partners.

---

[7] *See* Executive Order 12333, United States Intelligence Activities, at 1.4(b).
[8] *See* Executive Order 12333, United States Intelligence Activities, at 1.4(f).
[9] *See* Instruction No. IA-1000, Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (2017), on file with the DHS Privacy Office and *available at* https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf.
[10] *See* DHS/I&A-001 Enterprise Records System (ERS) System of Records, 73 Fed. Reg. 28128 (May 15, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.

The DHS Advisory Committees SORN[11] allows the Department to collect and maintain information on advisory committee members and on applicants to identify the most qualified applicant and ensure a balanced advisory committee.

The DHS Personnel Security Management SORN[12] allows for the collection of information related to background investigations and adjudications as well as other activities relating to personnel security management responsibilities at DHS.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The information system supporting the project is a shared drive on the unclassified DHS-wide computer system. The System Security Plan is issued by the Department's Chief Information Security Officer (CISO) pursuant to the System Security and Authorization Process Guide, Version 14 (June 15, 2018). The CISO as the Authorizing Official (AO) provides the unclassified DHS-wide computer system with an Ongoing Authorization (OA) to operate, in conformity with OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, these are administrative records governed by General Records Schedule (GRS) 5.1, item 010. This schedule pertains to records accumulated by the individual office that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists. Records include: staff locators, unofficial organizational charts, and office seating charts; office-level administrative policies and procedures and files related to their development; calendars or schedules of daily activities of non-high-level officials; informal requests and tracking of personnel training, travel, supplies, and equipment, excluding procurement and payment records and forms requesting training (e.g., SF-182); internal office activity and workload reports; studies and analyses of office administrative functions and activities; non-mission related management reviews and surveys; and minutes of meetings related to administrative activities.

Under NARA Disposition Authority DAA-GRS-2016-0016-0001, these records are designated as temporary and are destroyed when business use ceases.

[11] *See* DHS/ALL-009 Department of Homeland Security Advisory Committees, 73 Fed. Reg. 57639 (October 3, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[12] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 85 Fed. Reg. 64511 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The AEP Program is exempt from the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The categories of individuals for whom information is collected and the information collected include:

AEP Applicants

The following information is collected via the AEP Application Form:

- First and Last Name, Middle Initial, and Preferred Name;
- Phone Number;
- Email;
- Company/Organization;
  - Affiliation;
- U.S. Citizen (yes or no);
- Topics of Interest (up to three);
- How the applicant learned of the AEP Program;
- Qualifications; and
- Personal Statement.

Employers of AEP Applicants

The following information is collected via the AEP (Supervisor Endorsement) application form:

- Name of Applicant;
- Company/Organization;
- Supervisor Information;

- First and Last Name, Middle Initial;
- Organization;
- Title/Position; and
- Phone Number and email.

- Endorsement of Applicant (yes or no);
  - Endorsement/approval of the applicant's participation in this program (yes or no); and
  - Acknowledgement that the AEP program requires a six-month (three to five hours per week) commitment from the applicant (yes or no).
- Additional Information;
  - Supervisor's statement as to why the applicant would be a good candidate for this program; and
  - Supervisor's statement regarding how the applicant's participation in the program will benefit them, as well as their organization and its mission.

AEP Selectees

The following information is collected on a separate form for security and other onboarding purposes:

- First and Last Name, Middle Initial;
- Organization;
- Date of Birth;
- SSN; and
- Place of Birth (City and State).

Separately, private sector provisional selectees must disclose certain types of foreign associations, including:

- Any dual citizenship;
- Foreign identification (e.g., passports, visas, licenses, border crossing cards);
- Recent (within one-year) or Continuous Foreign Contacts (e.g., via telephone, email, social media, foreign officials, foreign companies, family ties to a foreign country, foreign acquaintances, foreign exchanges, or foreign organizations);

- Foreign travel (last two years dates and locations), indicating official business or personal;
- Foreign affiliation(s) (e.g., US-based foreign organizations, foreign nongovernmental organizations (NGOs), foreign education, foreign employment, receiving foreign support) (yes or no, and if yes, the name of the country);
- Foreign property holdings (yes or no, and if yes, the name of the country);
- Foreign bank accounts held (yes or no; and if yes, the name of the country); and
- Sponsorship of foreign nationals (e.g., visas, immigration) (yes or no).

The AEP participants are also given accounts in the travel management application "Concur" in order to facilitate reimbursement of their travel expenses. The Concur accounts are created by the DHS Federal Law Enforcement Training Center (FLETC), pursuant to a Memorandum of Understanding between I&A and FLETC that covers a range of financial management services. This information is separate from the application form and is provided to the Budget Travel Office. The form collects the selectee's name, date of birth, SSN, bank name, bank address, bank information (e.g., bank account number).

2.2. What are the sources of the information and how is the information collected for the project?

All of the above information is collected directly from the individual AEP applicants/selectees, except as stated below.

The information collected regarding foreign associations is conveyed to the DHS OCSO and then to I&A's CIMC for counterintelligence vetting of the AEP applicants' employers, as described above. The CIMC only conveys back to the AEP staff whether there are any counterintelligence risks associated with the AEP applicants' employer; no additional information is received or retained by AEP staff.

The information collected from AEP selectees on DHS Form 11000-13 is conveyed to USCIS in order to verify the selectees' citizenship and OCSO to conduct background checks for purposes of facilitating access to DHS facilities. USCIS and OCSO only convey back to AEP staff whether there were any issues with the checks conducted.

No other information is conveyed to AEP staff about the AEP applicants and selectees unless there is a particular problem, such as enrolling them into a direct deposit system, processing a claim for travel expenses, or granting access to an IT system or facility.

2.2 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.3 Discuss how accuracy of the data is ensured.

The purpose of the counterintelligence checks conducted by the CIMC and the background checks conducted by OCSO is to ensure that the information being provided by the AEP applicants and selectees to AEP staff is accurate and complete. Additionally, all of the above information is collected directly from the individual AEP applicants/selectees or supervisors of AEP applicants/selectees.

2.4 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that either the counterintelligence checks, the U.S. citizenship check, or the security check reveals inconsistencies between the personally identifiable information provided by the applicant and the results of the database checks, with one or the other being inaccurate or outdated.

Mitigation: This risk is mitigated. AEP staff coordinates with the appropriate offices and, as appropriate, returns to the AEP selectee for clarification or additional information in order to ensure the accuracy of all data before taking any action adverse to the AEP selectee.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The AEP Program uses the information solicited from AEP applicants to enable the AEP selection boards to select the most competitive candidates from among the applicants to become AEP selectees.

Additionally, the AEP Program uses the information solicited from AEP selectees to verify their U.S. citizenship, facilitate their access to federal facilities and IT systems, and process direct deposit or other forms of reimbursement for travel expenses they incur in the course of the program. Information about the applicant's foreign associations is used to assess whether there are counterintelligence risks associated with the applicant's participation in the program.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. As described above, the OCSO performs background checks on AEP selectees to ensure they have no criminal history that would preclude their access to federal facilities. If a selectee is found to have dual citizenship or other foreign ties, OCSO will assist I&A's CIMC with examining foreign associations for purposes of the CIMC's counterintelligence risk assessment. USCIS will verify that the selectee is a U.S. citizen. FLETC provides financial management support to I&A pursuant to an MOU and helps to process direct deposit forms and reimbursement of travel expenses to AEP selectees.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that the materials circulated to the selection boards could be misplaced, circulated to a party by accident who is not part of the selection board, or otherwise intercepted.

Mitigation: This privacy risk is mitigated. AEP staff provide the Application binders directly to the selection board member. The selection board members are reminded that this information contains the applicants' personally identifiable information (full name, email, and phone number). Once the selections are made, the application binders are returned to the AEP staff to destroy, via shredding, all hard copies. Binders are only handled by the selection board member(s) associated with making programmatic decisions.

Privacy Risk: There is a risk that others outside of the AEP staff who have no need to access this information might access it on the office shared drive, or that sensitive personally identifiable information may be compromised in transmission to OCSO, FLETC, or other entities who need the information to support the AEP Program.

Mitigation: This privacy risk is mitigated. All documents containing personally identifiable information are password protected on an I&A unclassified shared drive and only the AEP staff members with a need to know have access to the password. Documents transmitted (e.g., to OCSO, USCIS, FLETC, or DIA) with personally identifiable information are password protected and sent in a manner consistent with DHS guidance for handling sensitive PII. When the participants are no longer affiliated with the AEP their personally identifiable information

collected for security purposes (SSN, date of birth and place of birth) is destroyed.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The AEP staff provide notice to the AEP applicants and selectees about the collection of information in the emailed instructions and on the web page that announces the annual kick-off of the program, in addition to this PIA. Future AEP application forms, as well as the security forms used to solicit further information from the AEP selectees, will contain a formal Privacy Act Statement. Moreover, the AEP staff are in regular contact with AEP applicants and selectees and can answer any questions about why particular personally identifiable information is being solicited.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The AEP Program is entirely voluntary. All announcements related to the program make clear that AEP applicants must complete the application in order to be considered by the selection board. Applicants are made aware that the purpose of the program is to enable them to engage directly with members of the U.S. intelligence community in secure federal facilities and using IT systems owned and controlled by the U.S. Government. AEP staff explain to AEP selectees why certain personally identifiable information is being collected, and the AEP selectees are informed that they may not be able to access federal IT systems or facilities, receive travel reimbursements, or otherwise participate in the program if they decline to provide the information requested. AEP selectees apply to the program at-will and can remove themselves at any time.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that AEP applicants or selectees may not fully understand why different types of personally identifiable information are being collected and retained.

Mitigation: This privacy risk is mitigated. In addition to the publication of this PIA and the inclusion of Privacy Act notices on all forms, the AEP staff are in regular contact with AEP applicants and selectees and can be personally responsive to any questions or concerns they might have.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

When an AEP applicant becomes an AEP provisional selectee, the AEP staff retain their applications for the duration of the program cycle.

If an AEP applicant is not ultimately selected, their application file is still retained for up to two months after the program cycle begins, unless the individual opts to withdraw their application. This is because some AEP selectees may later be found ineligible to participate, or decide to drop out of the program, and the retention of other applicants' application files enables AEP staff to quickly fill the vacancy with another qualified candidate.

Once the six-month program concludes and travel reimbursement is settled, AEP staff delete or destroy all files containing the active participants' SSN, date of birth, and place of birth. However, the full name, email address, and phone number of participants are retained indefinitely. This information is added to the contact list of public-private sector partners to:

- Share information that may be relevant to the public/private sector participants;
- Continue with building and strengthening DHS I&A's public-private sector partnerships;
- Solicit topic ideas and new potential participants for the next AEP cycle; and
- Address requests from recipients that have reviewed AEP participants published work to either schedule interviews or presentations.

These are administrative records governed by General Records Schedule (GRS) 5.1, item 010. This schedule pertains to records accumulated by the individual office that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists. Records include: staff locators, unofficial organizational charts, and office seating charts; office-level administrative policies and procedures and files related to their development; calendars or schedules of daily activities of non-high-level officials; informal requests and tracking of personnel training, travel, supplies, and equipment, excluding procurement and payment records and forms requesting training (e.g., SF-182); internal office activity and workload reports; studies and analyses of office administrative functions and activities; non-mission related management reviews and surveys; and minutes of meetings related to administrative activities.

Under NARA Disposition Authority DAA-GRS-2016-0016-0001, these records are designated as temporary and are destroyed when business use ceases.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that the materials collected as part of the AEP application process could be retained longer than necessary on applicants who are not selected, or that information about these individuals could be confused or intermingled with the application packages on selectees.

Mitigation: This risk is partially mitigated. Retention requirements are outlined in the AEP SOPs and adhered to under the oversight of the AEP Program Manager. Applicants who are not selected do not receive a request for full name, place of birth, SSN, and date of birth. The documents containing the requested personally identifiable information of the selected participants are secured in a separate restricted folder. When an applicant is not selected, their application file is retained for up to two months after the program cycle begins unless the individual opts to withdraw their application. In either case, those files are then deleted.

The personally identifiable information of selected participants is deleted at the completion of the program's cycle. However, with their approval, participants' contact information remains on file for the purposes of contacting previous participants about future program activities.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. The information collected from AEP applicants is shared with members of selection boards, who are recruited from ODNI, for purposes of selecting the AEP selectees from the pool of applicants.

Additional information collected from AEP selectees is also shared externally in order to:

- Facilitate group access to federal facilities (specific federal facilities may vary from year to year depending upon the program) that require the submission of name, SSN, date of birth, and/or place of birth;
- Facilitate government-funded travel and direct deposit of reimbursement of participants' travel expenses. This information may be shared with the National Finance Center, part of the U.S. Department of Agriculture, for purposes of processing payments.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The ERS SORN's routine uses allow for external sharing as necessary to "properly manage

and oversee…organizational activities of I&A, including administrative responsibilities related to interagency support, litigation support, congressional affairs and oversight, records management, intelligence and information oversight, human capital, and internal security."

6.3 Does the project place limitations on re-dissemination?

There are limitations placed on the AEP selection board personnel with regard to the AEP application files they review, as described above. Personally identifiable information is shared with other agencies to facilitate group access to federal facilities; any limitations on re-dissemination are governed by existing law (e.g., Privacy Act of 1974) and the applicable rules, policies, and privacy documentation regarding the maintenance of visitors' logs for those facilities. The information sharing that occurs between I&A, FLETC, and the National Finance Center for purposes of processing reimbursements is strictly governed by MOUs and other written arrangements and policies between these institutions.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The AEP selection board staff retains detailed records of who serves on the selection boards each year and which applicants' files were considered by those boards. The AEP staff also retains records of which facilities were visited by each class or year of AEP selectees, which serve as record that the selectees' personally identifiable information was shared with those agencies.

The financial transactions between I&A, FLETC, and the National Finance Center that involve the sharing of personally identifiable information are accounted for by the I&A Chief Financial Officer (CFO) in the normal course of maintaining I&A's financial records.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that the members of the selection boards may retain information from the application files they are reviewing or share the information improperly, including through personal recollection.

Mitigation: This privacy risk is partially mitigated. The binders containing the AEP application files are collected from the selection board members at the end of the selection board proceedings. Selection board participants are also given detailed instructions about the confidentiality of the files and the proceedings.

Privacy Risk: With respect to sensitive personally identifiable information shared with FLETC and, via FLETC, the National Finance Center, there is a risk that the information could be mishandled by the receiving agency.

Mitigation: This risk is mitigated. I&A has established an MOU that outlines the data handling requirements with respect to the reimbursement process of the AEP Program. Further,

the National Finance Center is required to adhere to the government-wide security and privacy requirements that apply to financial and payroll data, to include its own SORNs, as discussed in U.S. Department of Agriculture PIAs.[13]

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

The ERS SORN describes the correction process for redress of source records. However, because of the classified and sensitive nature of most of I&A's activities, in accordance with Privacy Act requirements, DHS has exempted the I&A ERS from the Act's requirement to permit individuals access to records about themselves held by I&A and has published a final rule to amend its regulations to reflect this exemption.[14]

Notwithstanding applicable exemptions, DHS reviews all requests for access, regardless of citizenship or immigration status, on a case-by-case basis. When such a request is made, and compliance would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of DHS, and in accordance with procedures and points of contact published in the applicable SORN. DHS has a process in place to provide an individual the opportunity to request access to their record(s) and request the correction of their record(s). DHS will review each request and may waive the exemption for access to records when it believes that providing access would not adversely affect homeland security efforts. Individuals seeking access to any record containing information that is part of an I&A system of records, or seeking to contest the accuracy of its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request to DHS.[15] Requests processed under the Privacy Act will also be processed under FOIA; requesters will always be given the benefit of the statute with the more liberal release requirements. FOIA does not grant an absolute right to examine government documents; it establishes the right to request records and to receive a response to the request.

Under the Information Sharing Environment (ISE) Privacy and Civil Liberties Protection Policy,[16] DHS established a process to permit individuals to file a privacy complaint. Individuals who have privacy complaints concerning analytic division intelligence activities may submit complaints to the Privacy Office at privacy@hq.dhs.gov. Individuals may also submit complaints

[13] *See* https://www.usda.gov/home/privacy-policy/privacy-impact-assessments.
[14] Final Rule for Privacy Act Exemptions, 73 Fed. Reg. 56922 (Sept. 30, 2008).
[15] Individuals seeking access to records may submit a FOIA or Privacy Act request. *See* https://www.dhs.gov/freedom-information-act-foia.
[16] *See:* DHS Privacy and Civil Liberties Policy Guidance Memorandum, 2009-01, The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy (Jun. 5, 2009) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.

alleging abuses of civil rights and civil liberties or possible violations of privacy protections by DHS employees, contractors, or grantees to the Office of the Inspector General (OIG) at the OIG Hotline website.[17] Individuals may also file complaints alleging violations of civil rights and civil liberties by going to the CRCL website,[18] completing the fillable form, and emailing it to CRCLCompliance@hq.dhs.gov.

The procedures for submitting FOIA or Privacy Act requests for I&A records are available in 6 C.F.R. Part 5. FOIA requests can be submitted electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form or via mail or email to:

Office of Intelligence & Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528
Attn: FOIA Officer
Email: I&AFOIA@hq.dhs.gov

AEP applicants and selectees additionally can direct their request to the AEP staff via the email address AEP@hq.dhs.gov, as the AEP staff stay in periodic contact with AEP alumni. A simple request for a small and discrete record set can often be accommodated informally.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As discussed in Section 7.1, the ERS SORN has been exempted from the Privacy Act's requirements to permit individual access. Individuals may nonetheless request access to their records under the FOIA process described above, and DHS may, on a selective basis, provide the requested records. Individuals may also file a privacy complaint as previously described.

AEP applicants and selectees should direct their requests, questions or concerns to the AEP staff via the email address AEP@hq.dhs.gov. After the applicants' or selectees' cycle is complete, the only information retained is their name, phone number, and email address. If they desire to update this information, they can send an email to the AEP inbox. All other documentation is destroyed.

7.3 How does the project notify individuals about the procedures for correcting their information?

AEP applicants and selectees are all instructed to contact the AEP staff if they have questions or concerns via the email AEP@hq.dhs.gov. These instructions are included on communications related to AEP, including the application forms. This PIA and the ERS SORN

[17] *Available at* https://www.oig.dhs.gov/hotline/hotline.php.
[18] *Available at* https://www.dhs.gov/file-civil-rights-complaint.

also provide notice.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Because I&A's records that are subject to the ERS SORN have been largely exempted from access and redress obligations under the Privacy Act, there is a risk that AEP applicants, selectees, or alumni of the program will face difficulties gaining access to their records and/or correcting inaccuracies.

Mitigation: This risk is partially mitigated. The AEP staff make themselves available to assist AEP applicants, selectees, and alumni who have questions or concerns about their personally identifiable information. Requests will be considered to determine whether they would adversely affect homeland security.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

AEP staff and selection board members receive annual online privacy training and are provided a copy of this PIA. The AEP Program Manager oversees the training of the AEP staff and conducts process reviews to ensure the SOP and PIA are followed. Each year the SOP is reviewed for the accuracy of the established processes or revised as updates are required.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All AEP staff and all DHS selection board members complete annual online privacy training. This privacy training has been included as an annual training requirement for all of DHS I&A. Completion of this training is confirmed by DHS I&A. Notifications of those who have or have not completed this training are sent to AEP leadership and the AEP team member receives a direct email containing only their personally identifiable information.

The ODNI selection board members are required to take the same training to handle personally identifiable information for the application through ODNI. They do not receive additional training from DHS I&A but receive guidance from AEP staff on the sensitivity of the data contained in the applications. ODNI does not have access to the DHS unclassified network.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only a small number of AEP staff members have access to the sensitive personally

identifiable information (including SSNs) stored in a restricted folder on the I&A unclassified shared drive. These AEP staff members manage the team roster, applications and collection of personally identifiable information, and direct deposit forms on the shared drive. Access is provisioned by a supervisor. AEP staff update the data, remove records not required, and ensure the accuracy of the data collected/maintained. Passwords to the restricted folder are changed every six months.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any new MOUs or information sharing agreements will be reviewed by the I&A Privacy Office and other appropriate oversight offices (e.g., legal).

Responsible Official

Tammy Padilla
Public-Private Analytic Exchange Program
Office of Intelligence and Analysis
U.S. Department of Homeland Security
(202) 447-3338/(202) 510-4782

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717