Privacy Impact Assessment
for the

Enterprise Person (ePerson) System

DHS/USSS/PIA-016

January 27, 2017

Contact Point
William Wilson
Branch Chief, Mission Applications
Information Resources Information Technology Operations (ITO)
U.S. Secret Service
(202) 406-5383

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS) Enterprise Person (ePerson) Suite of web-based applications delivers an agency-wide employee records management solution that meets the protective, investigative, and personnel management needs of the organization.

The ePerson application allows users to search, view, and maintain USSS employee information including: Personal Summary (basic demographic data, e.g., office assignment, Entry on Duty (EOD), pay grade), Personnel Recovery Information, Skills and Training, Business and Personal Contact Information, Emergency Contacts, Firearms/Marksmanship Score, Physical Fitness Assessment Score, Identification, Gas Tracking for USSS-issued vehicles, Career Tracking, Passport and Visa Information, and Personal Assets (such as assigned desktop computers, laptops, tablets, mobile devices, computer monitors, and commission books/official credentials for law enforcement personnel). USSS is conducting this PIA because ePerson uses personally identifiable information (PII) from DHS employees and contractors, as well as members of the public.

Overview

The ePerson application maintains USSS employee and contractor information, and allows users to search and view data related to the protective, investigative, and personnel management functions of the organization. The various types of information stored within ePerson include: Personal Summary (basic demographic data, e.g., office assignment, EOD, pay grade), Personnel Recovery Information, Skills and Training, Business and Personal Contact Information, Emergency Contacts, Firearms/Marksmanship Score, Physical Fitness Assessment Score, Identification, Gas Tracking for USSS-issued vehicles, Career Tracking, Passport and Visa Information, and Personal Assets (such as assigned desktop computers, laptops, tablets, mobile devices, computer monitors, and commission books/official credentials for law enforcement personnel).

Functions within the overarching ePerson application include: Organization, Career Tracking, Phase Entry Group (PEG) Search, Bids, Field Management, Firearms Tracking, Fitness Tracking, Gas Tracking, Monthly Activity Reporting System (MARS), Uniformed Division Leave, and Passport. User access and permissions vary across functionality within the ePerson application based on an individual's current roles within the organization; no individual outside of the USSS has access to this information. The roles described below highlight the major business functions within each module.

The ePerson application maintains employee data records in a secure database environment that is referenced under the Application Provisioning Services (APS) FISMA boundary. The ePerson database schema exists within the Enterprise Oracle Database environment providing maximum availability and stability. To ensure maximum accuracy with employee demographic data, the Information Technology Operations (ITO) conducts a nightly secure file transfer of HR Connect[1] data from the U.S. Department of the Treasury-operated human resources system to ePerson. This process only involves the transmission of information to ePerson; no data is sent back to HR Connect. Once information is populated into the ePerson database, the updated information is available to the end user upon request.

The ePerson Application connects with a number of other major applications associated with FISMA systems to allow them to query the ePerson database for employee demographic data. Systems that query ePerson for demographic information include: the Uniform Division Resource Management System (UDRMS), the Enterprise Financial System (EFS)[2], the Field Investigative Reporting (FIRS)[3], the Enterprise Case (eCase) management system[4], and the Agent Manpower and Protection Support (AMPS). ePerson is used as a source/repository for these systems.

UDRMS is a Uniformed Division tool for requesting and tracking work assignments. EFS, includes four applications that allow the USSS to conduct financial management functions. EFS includes: the Concur Travel Manager, which supports the processing of travel vouchers for USSS employees; Oracle Financials, which processes day to day financial transactions; CompuSearch PRISM, which manages the federal acquisition lifecycle process; and Annams Sunflower, which tracks the physical property. FIRS is a suite of capabilities designed to support law enforcement by digitizing, categorizing cases, threat assessments, crime patterns, standard operating procedures, and lessons learned. The eCase system is a case management tool that includes background cases, hospital surveys, White House surveys, and other miscellaneous cases serving as a management database in which users can edit, close, and create new cases. AMPS is used by the Presidential Protective Division (PPD), Vice-Presidential Protective Division (VPD) and the Dignitary Protection Division (DPD) to plan, direct, coordinate, and track the execution of security operations for their corresponding protectees.

---

[1] See Department of Treasury, HR Connect PIA-2011, *available at* https://www.treasury.gov/SitePolicies/Documents/HRC%20PIA%202011.pdf
[2] See DHS/ALL/PIA-053 DHS Financial Management Systems, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-all-053-fms-september2016.pdf.
[3] See DHS/USSS/PIA-009(a) Field Investigative Reporting System (FIRS), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-firs-november2016.pdf.
[4] An analysis of the privacy impacts associated with the Enterprise Case (eCase) system will be provided in a forthcoming PIA, and will be available at https://www.dhs.gov/privacy-impact-assessments

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 information maintained in this system is solicited and obtained under the authority of 18 U.S.C. 3056 and 3056A; 5 CFR Part 293; 22 U.S.C. 211a, 213, and 218; and 5 U.S.C. 4103.

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

To permit the collection of various types of records for the functions carried out by the ePerson application, USSS relies on the following SORNs:

- OPM/GOVT-l General Personnel Records: outlines the collection and maintenance of an official repository of information related to a government employee's personnel records and reports of personnel actions.[5]
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS): outlines the collection and maintenance of a discreet set of PII in order to provide authorized individuals with access to IT systems and information.[6]
- DHS/ALL-014 Personnel Emergency Contact Information System of Records: outlines the collection and maintenance of workforce accountability records necessary to support DHS all-hazards emergency response deployments and exercises, as well as to contact designated persons in the event of an emergency.[7]
- DHS/ALL-032 Official Passport Application and Maintenance Records System: outlines the collection and maintenance of a copy of an official passport application or maintenance record on DHS employees and individuals who are associated with the Department.[8]
- DHS/ALL-037 E-Authentication Records System of Records: outlines the collection of information in order to authenticate an individual's identity for the purpose of a credential to electronically access a DHS program or application.[9]

---

[5] See OPM/GOVT-1 General Personnel Records, *available at* https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf.
[6] See DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), *available at* https://www.regulations.gov/document?D=DHS-2008-0042-0001.
[7] See DHS/ALL-014 Personnel Emergency Contact Information System of Records, *available at* https://www.regulations.gov/document?D=DHS-2015-0037-0001.
[8] See DHS/ALL-032 Official Passport Application and Maintenance Records System, *available at* https://www.regulations.gov/document?D=DHS-2010-0090-0001.
[9] See DHS/ALL-037 E-Authentication Records System, *available at*

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

The ePerson system security plan is in process. The system security plan will be completed upon adjudication of this PIA.

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

Yes. Records that are entered by the USSS and retained exclusively within ePerson are covered largely by General Records Schedule (GRS) 1, Civilian Personnel Records. However, certain modules within ePerson are covered under provisions specific to the type of subject matter addressed (e.g., passport tracking records are treated as "identification credential receipts, indexes, listings, and accountable records" and are held until all listed credentials are accounted for per GRS 11, item 4b; Home-to-Work/Gas Tracking reports are managed as Motor Vehicle Operator Files under GRS 10, item 7, etc.) The retention of records maintained within the ePerson system that were pulled from the Department of the Treasury's HRConnect system are employee demographics, employee work assignments, and employee contact information governed by GRS 4.2, item 130 and GRS 4.3, item 31. GRS 3.1 and 3.2 govern, as appropriate, General Technology Management and Information Systems Security[10] retention aspects of ePerson.

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.

No. None of the information maintained within the ePerson system is collected directly from members of the public, and is therefore not covered by the Paperwork Reduction Act. The information is provided by employees and is exempt from coverage under the PRA.

https://www.regulations.gov/document?D=DHS-2014-0039-0001.

[10] General Records Schedules provide the disposition authorization for records common to agencies of the Federal Government: GRS 3.1 -- General Technology Records, are records such as developing, operating, and maintaining computer software, systems, and infrastructure improvements; complying with information technology policies and plans; and maintaining data standards. GRS 3.2 -- Information Systems Security Records are records such as protecting the security of information technology systems and data, and responding to computer incidents.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

The ePerson application, consisting of multiple function-based components, serves as a data repository of information pertaining to USSS personnel; including employees, contractors, and their dependents/emergency points of contact. Below is a list of the applications and the type of PII each application processes:

- **The Person application:** contains data related to employee demographics, including the personal identification of an individual employee and his/her assigned equipment. The information collected includes: Social Security number (SSN), nickname/alias, foreign language proficiency, scars, tattoos, physical disfigurements, training, military history, assigned government cell phone, employee dependents, contact information, emergency contacts, passport, and employment history within the organization. The collection of data represents essential, basic information often required for event security planning and daily use relating to the assignment of duties.
- **The Firearm component:** maintains a listing of armed personnel (gun carriers) names and their respective firearm skills and training proficiencies with weapons. This application enables armed employees to view and track their own firearms/ marksmanship test scores.
- **The Fitness component:** maintains the names, birthdates, and medical information, to include medical waivers, related to the physical fitness of uniformed officers and agents. The Fitness application enables employees subject to fitness tests to view their own fitness scores, and to track conditioning progress. Administrators are enabled to verify/approve transactions entered by their employees.
- **The Organization component:** maintains a graphical representation of an employee's position within the organization to include career history of the employee. It contains employee photographs, unique employee identification numbers, duty assignment information, and foreign travel information.
- **The Careers component:** maintains personal information related to the application process, such as name, birthdate, SSN, and unique employee identification number. It enables an employee to view and bid on duty assignments. It enables managers to select employees for duty assignments or reassign employees to vacant duty assignments as necessary.
- **The Field Management component:** maintains details about vehicles assigned to employees, and contains employee names and driver's license numbers. The Field

Management component allows the personnel within USSS offices who manage vehicles, known as squad managers, to create, modify, and remove employees from specific assignments in support of tasks when vehicles are involved. It is used to log the number of miles that a USSS employee travels in vehicles that he/she has been assigned, and between his/her home and work location.

- **The Gas Tracking component:** maintains office certifications of gas transactions charged on an employee's gas card. It is used to display the amount of gas consumed per month by an office. Administrators are able to verify/approve transactions entered by their employees. This component collects the employee's name, as well as the supervisor's name, which is used in order to verify expenditures and gas card number.
- **The Monthly Activity Reporting System (MARS):** enables USSS employees to log their hours worked. The name of the employee is displayed only because the employee has accessed the ePerson system.
- **Maintenance Application:** enables ePerson administrators the ability to add, change, or modify functional capabilities for applications. No PII is being collected in this application.
- **The Reports Component:** ePerson allows end users to view, sort, and categorize various data from its several applications into reports using an Excel or PDF format for documentation purposes. Reports may include PII, specifically an individual's first and last name.
- **The Help application:** maintains user manuals related to the ePerson suite of applications.
- **The Uniformed Division (UD) Leave application:** enables UD officers to request dates of leave and overtime assignments on their government-issued mobile devices. It enables Uniformed Division Officers to request dates of leave by name and date.
- **The Phase Entry Group (PEG) Search Component:** provides users the ability to search for agents by their PEG designation, which consists of the year and quarter in which an individual became a special agent. It is a search functionality designed to permit queries across other applications within ePerson. The search results are temporary and are not stored once the screen is refreshed. The PEG search result displays photo; first, middle, and last name; office; title; SA EOD (exact date when individual became agent); PEG Number; #1 protection preference; phase; and biographic details (navigates to a person's biographic details within ePerson).
- **The Passport application:** enables the USSS Liaison Division to track employees' passports (Official, Diplomatic, and Personal) and visas. It contains employee names, the names of family members (who are dependents of employees who have been assigned to work overseas), home addresses, telephone numbers, and unique passport and visa numbers. The passport information is collected when an applicant fills out an application for a passport or passport renewal. The information is used to record and manage travel

documents according to expiration dates, approved location, and related data. The system does not create new information.

- **The Personnel Recovery application:** will enable the recovery of USSS personnel and contractors assigned overseas or on official travel abroad in the event they are isolated from friendly support. This functionality will display username (first initial of the first name and last name) information on monitoring screens with accurate time synchronization across time zones so analysts can have better situational awareness of overseas personnel when needed. The first initial and last name of the employee/contractor will be manually added to the management console. Information maintained within the application includes the employee's nickname/alias, foreign language proficiency, scars, tattoos, physical disfigurements, training, military history, assigned government cell phone, and government and personal email addresses. The capability to search other employees' personnel recovery information is restricted to the following users: Personnel Recovery Information (PRI) Administrator and PRI ISD Duty desk.

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

The ePerson system displays data from the ePerson enterprise database under the APS umbrella and is internal to USSS. Information used by ePerson is pulled directly from the Department of the Treasury's HRConnect system during automated daily refreshes. Some information is obtained from USSS employees.

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

No. The ePerson system does not use data from any commercial or otherwise publicly available source.

2.4 Discuss how accuracy of the data is ensured.

The ePerson systems relies upon the source system (HRConnect) to ensure that data used by the ePerson system is accurate and complete. The database administrators look at the outputs of the Extract Transfer Load (ETL) logs to verify that all transactions have been processed. The ePerson application business owner(s) validate information that resides in each module. When corrections are made to data in HRConnect, the update information is uploaded into ePerson during a daily data refresh, ensuring that only the most current data is used.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that ePerson may collect more information than is necessary and relevant to accomplish its designated functions.

Mitigation: The ePerson system performs a broad scope of HR functions, thus collecting a large amount of information. The type of data collected about USSS personnel is limited to only that information necessary to complete human resources and business functions. This risk is mitigated through the provision of training to USSS employees on the collection of only the necessary and appropriate PII for performing the tasks associated with each application/component. PII is collected to enable positive identification so that the individual is not erroneously identified as or linked to another individual. Given the variety of functions for which it was designed, it is no possible to further mitigate this risk.

Privacy Risk: Since information is pulled from a separate system, rather than directly from individuals, there is a privacy risk that information about individuals may be inaccurate.

Mitigation: This risk is mitigated through the provision of access for each USSS employee to the Department of the Treasury's HRConnect system in order to review, update, and correct his/her own information in the source system. The system updates daily to ensure refresh occurs in a timely manner.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The ePerson suite of web-based applications delivers an agency-wide employee records management solution that meets the protective, investigative, and personnel management needs of the organization. The ePerson application allows personnel to enter, update, and view limited data relevant to their respective mission or operational need. The data, mostly related to contact, travel, and operational information, is used to facilitate: the review of qualifications; assignment to specific roles/duties; tracking of location; and other administrative functions. A list of the components of the ePerson application, as well as the types of PII data processed within the application, is outlined in section 2.1.

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?

No. The ePerson application is not accessible to other components or agencies.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of unauthorized access and inappropriate use and dissemination of the information maintained in ePerson.

Mitigation: This risk is mitigated through USSS's protection of PII through the implementation of security groups within the Microsoft Active Directory. Employees requiring access to ePerson are given written authorization from appointed business owner(s). The ePerson application has a robust audit trail that logs any action by users and administrators. The system also locks sessions after twenty minutes of inactivity, limits access to authorized individuals, prevents account access after three unsuccessful login attempts, and warns users that unauthorized, improper use or access to the system may result in disciplinary action as well as civil and criminal penalties. Additionally, all searches and information received are kept in the system log files for audit and quality control purposes. The logs are audited monthly by the business owner and Information System Security Officer (ISSO).

Privacy Risk: There is a privacy risk to data minimization that ePerson maintains SSN and other internal unique identification numbers to perform functions within the application.

Mitigation: This risk is not mitigated. The information is properly managed through the maintenance of strict access controls within the system, through the provision of training on the appropriate use of the information, and the housing of information on a closed network.

Privacy Risk: There is a privacy risk that information in ePerson may be used for purposes outside those for which it was collected.

Mitigation: To mitigate these risks, the USSS uses this information for the limited purpose of providing an agency-wide employee records management solution. Access to the system is

limited to authorized USSS employees who have a need to know in the furtherance of their roles and responsibilities. All USSS employees and contractors are required to follow Rules of Behavior contained in the DHS Sensitive Systems Policy Directive 4300A, as well as take annual computer security and privacy training, which includes instruction on the appropriate use and handling of sensitive data and proper security measures.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

The USSS provides notice of the collection of employee information through Privacy Act Statements provided on the ePerson website. USSS employees and contractors are provided with Privacy Act Statements when they complete the onboarding process with the Office of Human Resources, which provide notice that their personnel information will be collected and maintained for a variety of purposes. General notice regarding the types of information collected by the ePerson application, as well as the ways in which that information is used, is provided to individuals through the SORNs listed in Section 1.2. Additional notification is provided through the publication of this PIA.

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

There is no opportunity for the USSS personnel providing this information to decline or opt out of the agency processes that use this suite of applications.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals identified as family members and emergency points of contact will not receive notice that USSS is collecting, maintaining, and using their information.

Mitigation: DHS/All-014 Personnel Emergency Contact Information System of Records provides notice of USSS's collection of information for workforce accountability and individuals identified as employee family members and emergency points of contact. Additionally, USSS employees are advised to provide notification to their emergency points of

contract and family members that their contact information will be maintained by the USSS. Other SORNs listed in Section 1.2 provide general notice of the purpose of collection, redress procedures, and the routine uses associated with the collection of the information.

This PIA provides similar notice to the general public as to the collection and use of the information for this purpose.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Records retained by USSS within the ePerson application are covered largely by General Records Schedule (GRS) 1, Civilian Personnel Records. For example, career bid data is treated as Merit Promotion Case Files ("records relating to the promotion of an individual that document qualification standards, evaluation methods, selection procedures, and evaluations of candidates") and retained for 2 years after the personnel action is completed, per GRS 1, item 32. Other GRS schedules govern data specific to the type of subject matter addressed (e.g., passport tracking records are treated as "identification credential receipts, indexes, listings, and accountable records" and are held until all listed credentials are accounted for per GRS 11, item 4b; Home-to-Work/Gas Tracking reports are managed as Motor Vehicle Operator Files under GRS 10, item 7; etc.) Likewise, as pending revisions to the GRS, DHS enterprise schedules, and agency records schedules are formalized, corresponding retention changes, if any, will be applied to data in the system.

The ePerson records that were pulled from HRConnect, the source system owned and operated by the Department of the Treasury, are governed by General Records Schedule (GRS) 4.2, item 130 and GRS 4.3, item 31 and are automatically overwritten when updated data is ingested each night. GRS 3.1 and 3.2 govern, as appropriate, General Technology Management and Information Systems Security retention aspects of ePerson.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained for longer than is required or needed in ePerson.

Mitigation: This risk is mitigated through the provision of proper records retention training to all system users and the periodic auditing of the system. The information maintained within the ePerson application will be retained in accordance with approved records schedules.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

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.

No, information is not generally shared outside of DHS as part of normal operations. However, all information maintained within ePerson may be shared, upon request, in accordance with the purposes and routine uses specified in the SORNs listed in Section 1.2. In the event that personnel recovery is initiated, USSS would provide information to appropriate agencies.

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

Any information maintained in ePerson may be shared in accordance with the purposes and routine uses specified in the SORNs listed in Section 1.2 in support of the dual mission of the USSS. To the extent that information may be released pursuant to any routine uses, such release may be made only if it compatible with the purposes of the original collection, as determined on a case-by-case basis.

6.3 Does the project place limitations on re-dissemination?

Yes. When users log on to ePerson, they are advised that information obtained from the system should be shared only with those individuals or entities that have an official need to know as part of their official responsibilities, and that steps should be taken to ensure that the PII contained therein is appropriately safeguarded. The conditions of transmission provide that information should not be disseminated without authorization from the USSS. These conditions may be covered by MOUs, MOAs, other agreements, and/or in a letter of transmission.

All information collected, maintained, used, and disseminated from the ePerson application is covered by the Privacy Act. As such, information may only be disseminated consistent with the routine uses in the governing SORNs and existing sharing agreements, when applicable.

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

As required by the Privacy Act of 1974, authorized personnel properly document the dissemination of information obtained from the system in their memorandum of record on the matter.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: To the extent that information may be released pursuant to any routine uses, there is a privacy risk that PII may be disclosed outside of the Department for the purpose that is inconsistent with the original collection of data.

Mitigation: To mitigate this risk, disclosure may be made only by authorized USSS employees requiring a need to know in the furtherance of their respective duties. Authorized USSS employees may only share information pursuant to routine uses specified in the SORNs listed in Section 1.2. Authorized USSS users of the system document the dissemination of information obtained from the system in a memorandum of record. In addition, system administrators conduct periodic reviews of audit logs which report instances of user login, logoff, login failures, data access failure or success instances, and who accessed the data along with what activity was performed while logged in. Any anomalies are reported to the project manager, who in turn verifies and validates anomalies with business owner(s). If nefarious acts are suspected, they are reported in accordance with the USSS Incident Response Plan.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Authorized users may view their personal and individual information at any time in ePerson. Additionally, individuals seeking notification of, and access to, any information contained in ePerson, or seeking to contest its content, may submit a request in writing to the USSS Freedom of Information Act/Privacy Act (FOIA/PA) Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223.

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

Basic employee information as described in Section 2.1 is received from HRConnect by ePerson and, if correction is required, the employee must contact appropriate USSS HR Specialists or log into HRConnect to make the changes to his/her own data. All employees can update their own demographic information. ePerson Administrators can correct inaccurate information that is reported by an employee. Limited editing capability exists in the modules to allow updates to be made in the ePerson application. Executives, managers, supervisors, and employees can make updates to some fields subject to access permissions and authorities. Fields that are not allowed to be modified provide instructions via drop down to the user on the procedures to follow to correct inaccurate or erroneous information.

Individuals seeking notification of and access to any information contained in ePerson, or seeking to contest its content, may submit a request in writing to the USSS Freedom of Information Act/Privacy Act (FOIA/PA) Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223.

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

ePerson provides instructions for employees, supervisors, and administrators to modify and correct information at initial ePerson training, and these instructions remain available on the ePerson help page. Individuals are also provided notices about the procedures for correcting information in the SORNs listed in Section 1.2.

The procedure for submitting a request to correct information is outlined in this PIA in Questions 7.1 and 7.2.

7.4 Privacy Impact Analysis: Related to Redress

There is minimal privacy risk related to redress because individuals have access to correct some information directly in the source system and can request correction of inaccurate information by contacting the user's HR Specialist. A supervisor is required to verify and make appropriate changes if an individual feels his/her information is inaccurate. Users may also contact the Information Resources Management Division helpdesk for assistance.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

The ePerson application employs technical controls, including role-based access and audit logs, to ensure that information is used in accordance with the stated practices in this PIA. An individual must have a valid and active USSS network account to access ePerson. There are also technical safeguards, such as the use of client software installed on work stations that requires a valid approved user identification and password. This data is maintained in the USSS data center and a back-up copy is maintained at a geographically separate location. Audit logs are captured and reviewed monthly.

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

All USSS employees and contractors are required to complete annual privacy and security training to ensure that they have a sufficient understanding of proper handling and safeguarding of PII. The USSS also provides written ePerson user guides and online help to the end-user.

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

Business owners and office points of contact are assigned for each function and/or module within the ePerson application. The business owners identify what accounts are needed for ePerson, informing administrators how to associate user accounts to established active directory groups to assign specific roles and permissions.

User roles within ePerson are established based on the specific role and function of each member. The ePerson business owner validates perspective users' need to know for access to the system, and then submits a request to the ePerson administrators to add personnel to appropriate group memberships. Once provided access, USSS employees are able to view their own information.

DHS physical and information security plans dictate who may access USSS computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology

procedures for granting access to USSS computers. Access to the information is strictly limited by access controls to those who require it for completion of their official duties.

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?

All information sharing agreements, MOUs, and new uses of information are reviewed by the USSS Privacy Office, Office of Chief Counsel, and the respective program office.

Responsible Officials

William Wilson
Branch Chief
Mission Applications
Information Resources Information Technology Operations (ITO)
U. S. Secret Service
Department of Homeland Security

Latita Payne
Privacy Officer
U. S. Secret Service
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.