Privacy Impact Assessment Update
for the

Enterprise Person (ePerson) System

DHS/USSS/PIA-016(a)

June 25, 2018

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

Reviewing Official
Philip S. Kaplan
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. USSS is updating this privacy impact assessment (PIA) to denote the addition of the Passport Operations (PASSOPS) functionality within ePerson and to include the interconnection of the Applicant Lifecycle Information System (ALIS) system, which queries ePerson for demographic information.

Overview

The Department of Homeland Security (DHS) USSS 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 originally stored within ePerson include: Personal Summary (basic demographic data (e.g., office assignment, Entry on Duty Date (EOD), pay grade), Personnel Recovery Information (PRI), 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). Secret Service discussed these types of information in DHS/USSS/PIA-016, published on January 27, 2017.

Since the 2017 PIA issuance, the scope of ePerson has expanded to now include the addition of the Passport Operations (PASSOPS) functionality within ePerson and the new interconnection with the Applicant Lifecycle Information System (ALIS), which queries ePerson for demographic information.

The Passport Operations (PASSOPS) functionality provides a user interface which interacts with the Passport application of ePerson. PASSOPS allows USSS Presidential Protection Division (PPD) personnel, designated as PASSOPS administrators, to manage, create lists, and report on passport status in support staffing of overseas events. PASSOPS collects details relating to the employee's branch assignment, place of birth (POB), and the names of family members to support this functionality. This data is viewed, edited, or entered exclusively by PPD PASSOPS administrators. PASSOPS administrators review each record reflecting that an employee has checked out or returned his or her Government passport for accuracy and work with the employee to ensure that any errors are corrected. The PASSOPS functionality does not use data from any commercial or otherwise publicly available source.

The Applicant Lifecycle Information System (ALIS) is an applicant tracking system used by the Security Management Division (SMD), Talent & Employee Acquisition Management Division (TAD), and Human Capital Management (HUM) to support the hiring process from beginning to end for USSS Special Agent (SA) and Uniform Division (UD) Officers and Administrative, Professional, Technical (APT) personnel. ALIS interfaces with the ePerson database for look-up capabilities to review USSS employee attribute information such as employee name, office code (e.g., HUM, CIO), and office location (e.g., country). ALIS will be discussed in further detail in a forthcoming PIA.

Reason for the PIA Update

USSS is updating DHS/USSS/PIA-016, originally published on January 27, 2017, to include the PASSOPS functionality and to cite the new system interconnection that occurs between ePerson and ALIS, which queries ePerson for demographic information.

Privacy Impact Analysis

Authorities and Other Requirements

USSS continues to cover the information maintained in this system 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.

USSS continues to rely on the SORNs listed in DHS/USSS/PIA-016,[1] originally published on January 27, 2017, to describe the collection of various types of records for the functions carried out by the ePerson application. In addition, the Official Passport Application and Maintenance Records SORN[2] covers PASSOPS 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.

Records that are entered by the USSS and retained exclusively within ePerson are covered largely by the General Records Schedules (GRS) of the National Archives and Records Administration (NARA). Since completion of the original PIA, NARA has updated and renumbered the GRS (e.g., the former GRS 1, "Civilian Personnel Records" has been superseded by a new GRS 2.0 covering "Human Resources"). However, retention protocols have not changed substantially since the original PIA. (See "Data Retention by the project" section below for additional detail.)

[1] *See* DHS/USSS/PIA-016 Enterprise Person (ePerson) System, *available at* www.dhs.gov/privacy.
[2] DHS/ALL-032 Official Passport Application and Maintenance Records, 76 FR 8755 (Feb. 15, 2011).

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 (PRA). The information is provided by employees and is exempt from coverage under the PRA.

Characterization of the Information

USSS continues to collect the information described in DHS/USSS/PIA-016, including:

- **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),[3] 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,

[3] SSNs in ePerson are part of an employee's HR profile that is viewed in ePerson. Access to the SSN is restricted to the individual employee and those in an authorized administrative role.

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; Special Agent 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 USSS collects and maintains family member passport information for

personnel assigned to overseas posts for accountability to the State Department, as the information is required for visa documents and passport renewals while abroad. 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 Investigative Support Duty desk.

This PIA Update captures how the PASSOPS functionality maintains details relating to the employee's branch assignment, place of birth (POB), and the names of family members to support the PASSOPS functionality. This data is viewed, edited, or entered exclusively by PPD PASSOPS administrators. This PIA Update also encompasses the interconnection between ePerson and ALIS enabling read-only access to the USSS employee demographic information residing in ePerson.

Neither the PASSOPS functionality nor the ALIS interconnection uses data from any commercial or otherwise publicly available source.

Uses of the Information

USSS continues to use ePerson to provide an internal agency-wide employee records solution. The addition of the PASSOPS functionality enables personnel from PPD to control the check out and check in status of Government passports assigned to USSS employees. When USSS employees are assigned to travel overseas and a Government passport is required, they check out and subsequently return their passport. PASSOPS enables PPD administrators to log when the employee's Government passport is in use for travel and when that employee returns the passport after the assignment is completed.

ALIS interfaces with the ePerson database providing the user with look-up capabilities to review USSS employee attribute information such as employee name, office code (e.g., HUM,

CIO), and office location (e.g., country), in order to identify USSS personnel who are reviewing applicants in ALIS.

Neither PASSOPS nor the ePerson system have roles that are assigned or fulfilled by other components. The ePerson system is not accessible by other components or agencies.

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

Mitigation: This risk is mitigated by restricting access to a small group of PASSOPS administrators. Use of Active Directory groups for authorizing and authenticating PASSOPS administrators ensures that no other USSS employee has the ability to view, edit, or enter data into PASSOPS.

Notice

USSS is providing notice about the addition of the PASSOPS functionality and ability of ALIS to query ePerson through the publication of this PIA update.

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 that 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 applications within ePerson, as well as the ways in which that information is used remains unchanged and is provided to individuals through the SORNs listed in the previous PIA.[4]

The Official Passport Application and Maintenance Records SORN provides notice for PASSOPS 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.

Data Retention by the project

Although there are no substantial changes to data retention requirements, revision and reissuance of NARA's General Records Schedules has changed many of the citations for records schedules associated with ePerson. For example, ePerson's personnel-related records are now retained based on the schedule contained in GRS 2.0, "Human Resources" rather than the legacy GRS 1, "Civilian Personnel Records." The updated records retention schedules are as follows:

- Records related to official employee passports and official passport registers are temporary, and will be destroyed when superseded or obsolete, according to GRS 2.2, Item 091.
- Gas Tracking records are considered space, vehicle, equipment, stock, and supply administrative and operational records, and will be destroyed when 3 years old or 3 years

[4] *See* DHS/USSS/PIA-016 Enterprise Person (ePerson) System, *available at* www.dhs.gov/privacy.

after they are superseded, but longer retention is authorized if required for business use, according to GRS 5.4, Item 010.

- Squad Management records, including notifications of personnel actions and copies of Standard Form 50, which documents all individual personnel actions such as employment, promotions, transfers, and separation, copies that are maintained in personnel offices, are temporary and will be destroyed when business use ceases, according to GRS 2.2, Item 50.
- Career bids and requests for non-competitive personnel action, which include the agency copy of requests submitted to the Office of Personnel Management for approval of non-competitive personnel action on such matters as promotion, transfer, reinstatement, or change in status, are temporary and will be retained for 1 year, according to GRS 2.1, Item 080.
- Employee summary and photograph records are considered Administrative Records and are temporary, to be destroyed when business use ceases, according to GRS 5.1, Item 010.
- Home to Work (HTW) reports are considered facility, space, vehicle, equipment, stock, and supply administrative and operational records, and will be destroyed when 3 years old or 3 years after superseded, but longer retention is authorized if required for business use, according to GRS 5.4, Item 010.
- Firearms (skills and training) records are considered weapons requalification records, and contain the records of requalification by an individual in the use of firearms, shotguns, off-duty weapons, and intermediate weapons. These records will be cut off on the separation/retirement of the individual and kept 5 years in ePerson after cutoff or until superseded or obsolete, according to NARA N1-087-97-2, Item 05.

Information Sharing

Information is not generally shared outside of DHS as part of normal operations. Information sharing by the applications within ePerson discussed in the previous PIA remain unchanged.

However, all information maintained within PASSOPS may be shared, upon request, in accordance with the purposes and routine uses specified in the Official Passport Application and Maintenance Records SORN. To the extent that information may be released pursuant to any routine uses, such a release is made only if it is compatible with the purposes of the original collection, as determined on a case-by-case basis.

Redress

The individual right to access, redress, and correction has not changed with this update. 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 Freedom of Information Act (FOIA) 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.

Auditing and Accountability

There is no change in the auditing and accountability as described in DHS/USSS/PIA-016. USSS continues to employ technical and security controls to preserve the confidentiality, integrity, and availability of ePerson, which is validated as part of Continuous Monitoring. These technical and security controls mitigate privacy risks associated with unauthorized access and disclosure.

Responsible Official

William Wilson
Branch Chief
Information Technology Operation (ITO)
U.S. Secret Service
Department of Homeland Security

Christal Bramson
Acting Privacy Officer
U.S. Secret Service
Department of Homeland Security

Approval Signature

[Original, signed copy on file with the DHS Privacy Office]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security