9110-9B-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0046]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of New Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, "DHS/ALL-040 DHS Personnel Recovery Information System of Records." This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This new system will be effective upon publication. Routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2017-0046 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Philip S. Kaplan, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "DHS/ALL-040 Personnel Recovery Information System of Records."

The DHS Personnel Recovery Programs are responsible for: ensuring that DHS personnel and contractors assigned overseas or on official travel outside the continental United States (OCONUS) have proper training and equipment to fulfill their respective mission; maintaining a twenty-four (24) hour monitoring center for all overseas personnel who are traveling outside their country of assignment; executing a coordinated response to personnel recovery incidents; maintaining a notification system within DHS to provide emergency-related notifications as needed without jeopardizing the safety of DHS personnel (including federal employees and contractors); and providing and developing tracking and locating technology.

DHS will use the information collected in this system of records in furtherance of its responsibilities to prevent, prepare for, and respond to circumstances in which DHS and contractor personnel have been abducted, detained, held hostage, declared missing, or impacted by a terrorist attack, natural disaster, government takeover, transportation accident, or are otherwise isolated from friendly support, pursuant to Presidential Policy

Directive (PPD)-30,[1] Hostage Recovery Activities, issued in 2015.

Presidential Policy Directive-30 directs each department and agency with overseas responsibilities to, among other things, provide personnel recovery preparation, education, and training programs to enable personnel recovery from a threat environment.

This system of records is being established to document the types of personal information collected on individuals, and to ensure that such information is appropriately shared to enable the recovery of DHS personnel (including federal employees and contractors) assigned overseas or on official travel abroad in the event they are isolated from friendly support. The Personnel Recovery Information System will be used to facilitate collaboration with the Department of State (DOS) and other federal agencies. The information will be maintained in DHS systems that serve as data repositories of personnel data.

Information covered by the Personnel Recovery Information System of Records is only used for personnel recovery purposes, and is only shared outside DHS to further its personnel recovery objectives with permission from DHS personnel.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-040 Personnel Recovery Information System may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In

[1] Presidential Policy Directive-30 directs a renewed, more agile United States Government response to hostage-takings of U.S. nationals and other specified individuals abroad. Presidential Policy Directive-30 supersedes and revokes NSPD-12, United States Citizens Taken Hostage Abroad, dated February 18, 2002, along with Annex 1 and Appendix A to NSPD-12, dated December 4, 2008, and is available at https://www.whitehouse.gov/the-press-office/2015/06/24/presidential-policy-directive-hostage-recovery-activities.

addition, DHS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles (FIPP) in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/ALL-040 Personnel Recovery Information System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/ALL-040 Personnel Recovery Information.

SECURITY CLASSIFICATION: Unclassified, Sensitive, For Official Use Only, Law enforcement-Sensitive.

SYSTEM LOCATION: Records are maintained at the DHS Headquarters in Washington, D.C., component headquarters and field offices, and as component-specific systems. Electronic/Information Technology (IT) records are maintained within DHS systems that serve as data repositories of personnel data.

SYSTEM MANAGER(S): For DHS Headquarters components, the System Manager is the Deputy Chief Freedom of Information Act (FOIA) Officer, Department of Homeland Security, Washington, D.C. 20528. For components of DHS, the System Manager can be found at http://www.dhs.gov/foia under "Contacts."

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Authority for maintaining this system is in 6 U.S.C. sec. 236; 8 U.S.C. sec. 1103; 22 U.S.C. secs. 4801, 4802, and 4805; and Presidential Policy Directive (PPD)-30, Hostage Recovery Activities.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to permit DHS's collection, use, maintenance, dissemination, and storage of information to: facilitate identification of DHS personnel (including employees and contractors) assigned overseas or on official travel abroad for whom DHS has the responsibility to recover or account; maintain situational awareness of the location of DHS personnel; and coordinate support services for personnel who have been abducted, detained, held hostage, declared missing, impacted by a terrorist attack, natural disaster, government takeover, aircraft/motor vehicle accident, or are otherwise isolated from friendly support.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DHS personnel (including federal employees and contractors) and non-DHS Federal employees who are members of DHS-led task forces assigned overseas or on official travel outside the United States. Information will also be collected from family members, domestic partners, and emergency contacts of personnel assigned overseas or on official travel outside the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

Mandatory fields include the following:

- Full Name;
- Alias(es);
- Business title/position title;
- Gender;
- Biometric (*i.e.*, fingerprint data and facial photographic data) and other information (*i.e.*, race, ethnicity, weight, height, eye color, hair color) collected to conduct background checks;
- Foreign Travel Itinerary;
- Foreign Language and Fluency Level;
- Personnel Recovery Training and Year Received;
- Other Pertinent Training;
- Prior Military/Branch;
- Assignment Reason Narrative;
- Assignment Location;
- Work Email Address;

- Security clearance information;
- Business Cellular International Mobile Station Equipment Identity (IMEI);
- Business Phone Number;
- Passport numbers and other travel documents (official or diplomatic, and personal), including expiration date;
- Citizenship;
- Emergency contact information (at post and at home);
- Identity verification or security questions and responses;
- Supervisor contact information; and
- Emergency contact information.

Optional fields include the following:

- Blood Type;
- Scars;
- Tattoos;
- Disfigurement;
- Medical Conditions;
- Allergies;
- Medication;
- Personal Cellular Phone Number;
- Personal Cellular IMEI;
- Other Electronic Device Type;
- Other Electronic Device IMEI;

- Personal Email Address #1;
- Personal Email Address #2;
- Regional Security Officer (RSO) Name;
- RSO Direct Phone;
- RSO Cell Phone;
- Marine Post One Phone;
- Regional Embassy/Consulate;
- Tracking Device IMEI;
- Personnel Recovery Equipment;
- Cellular –World;
- Cellular – World IMEI;
- Cellular – Local;
- Cellular – Local IMEI;
- Religious preference;
- Sizing information (*e.g.*, shirt size, pant size, hat size, shoe size);
- Vehicle information;
- Real-time location information;
- Kit issuance; and
- Information about family members and domestic partners of personnel assigned OCONUS (name, passport numbers and issuing country, contact information, date of birth, work location, school name and location, medical conditions, and photographs).

RECORD SOURCE CATEGORIES: Records are obtained from DHS personnel (including federal employees and contractors).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. sec. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist another federal recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach; or

2. DHS suspects or has confirmed that there has been a breach of this system of records; and (a) DHS has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, harm to DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (b) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to

the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To the Department of State (DOS) when necessary to coordinate U.S. Embassy or Consulate support services for the employee.

H. To federal, state, and local governmental agencies or executive offices, and foreign governments, when disclosure is appropriate for proper planning or coordination of personnel recovery efforts or assistance, as described in PPD-30.

I. To family members when the subject of the record is unable or unavailable to sign a waiver and is involved in an emergency situation, and the release is for the benefit of the subject.

J. To members of Congress when the information is requested on behalf of a family member of the individual to whom access is authorized under routine use I.

K. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS stores records in this system electronically or on paper in secure facilities at the DHS Headquarters in Washington, D.C., as well as component headquarters and field offices, in a locked

drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by an individual's name, biometric information, employee ID number, and telephone number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: For information used to account for personnel and maintain communication during emergencies, office dismissal, and closure situations, the Personnel Recovery Information system of records will retain records until superseded or obsolete, or upon separation or transfer of the employee, in accordance with NARA General Records Schedule 5.3, Item 20.

For all other information in this system of records, the information will be maintained in accordance with NARA General Records Schedule 5.2, Item 10. This information is also retained until superseded or obsolete, or upon separation or transfer of the employee.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or component's Freedom of Information Act (FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and

- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, see "Record Access Procedures" above.

NOTIFICATION PROCEDURES: See "Record Access Procedures."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: DHS/ALL-040 is a new system of records and DHS has not published any prior notices that apply to the records.

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2017-23203 Filed: 10/24/2017 8:45 am; Publication Date: 10/25/2017]