9110-9B

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0074]

Privacy Act of 1974; System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/ALL-014 Department of Homeland Security Personnel Contact Information." This system of records covers DHS's collection and maintenance of records concerning DHS personnel (including Federal employees and contractors) for workforce accountability; DHS and non-DHS Federal employees, contractors, or other individuals who participate in or respond to all-hazard emergencies, including technical, manmade, or natural disasters, or who participate in emergency response training exercises; and individuals identified as emergency points of contact. Categories of individuals, categories of records, and retention schedules for this system of records have been modified and expanded to better reflect the Department's emergency personnel location record systems. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This modified system will be included in the DHS inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified 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-2017-0074 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 and privacy questions, please contact Philip S. Kaplan, Sam.Kaplan@hq.dhs.gov, (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, DHS proposes to modify a current DHS system of records titled, "DHS/ALL-014 Personnel Emergency Contact Information."

This system of records covers DHS's collection and maintenance of records concerning current and former DHS personnel (including Federal employees and contractors) for workforce accountability (e.g., tracking employee locations for safety and security purposes); Federal employees, contractors, or other individuals (e.g., state, local, tribal, and territorial [SLTT] personnel) who participate in or who respond to all-

hazards emergencies including technical, manmade, or natural disasters, or who participate in emergency response training exercises; and individuals identified as emergency points of contact. DHS collects information of family members, next of kin, or other designated emergency contact persons for use in the event of an emergency.

Categories of individuals, categories of records, and retention schedules for this system of records have been modified and expanded to better reflect the Department's emergency personnel location record systems.

Categories of individuals have been expanded to include former DHS personnel; current and former Federal employees, contractors, or other individuals (e.g., SLTT personnel) who participate in or conduct emergency response training exercises; and individuals identified by current or former DHS personnel as emergency points of contact, including family members and next of kin.

DHS is updating the category of records to include geospatial location information. DHS may collect this information from DHS personnel, including Federal employees and contractors; current and former Federal employees, contractors, or other individuals who participate in or conduct emergency response training exercises; current and former Federal employees, contractors, or other individuals who respond to all-hazards emergencies including technical, manmade, or natural disasters. DHS collects this information in order to facilitate the response efforts of deployed DHS and non-DHS personnel to all-hazards emergencies and provide a clear operational picture of the location of emergency personnel. This enables DHS or the emergency managers to better direct emergency personnel and the overall response effort.

In the course of responding to, or planning for, all-hazards emergencies, DHS may contact, locate, and deploy DHS personnel; implement the Continuity of Operations (COOP) Plan; and participate in emergency response training exercises. DHS may also utilize Federal Government employees from other Federal agencies who are deployed as a part of a mission assignment (pursuant to 42 U.S.C. sec. 5197(c)) and non-Federal Government employees, such as other SLTT personnel. This system of records encompasses the collection, storage, and use of information associated with such activities and for all individuals that participate in those activities. Additionally, for emergency notification purposes, DHS may contact the identified emergency contacts or next of kin of the individual.

DHS is updating the record retention schedule to reflect the new and revised General Records Schedules under the Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA) M-12-18, Managing Government Records Directive (Aug. 24, 2012). The previous General Records Schedules have been superseded.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-014 Personnel Emergency Contact Information system of records notice (SORN) 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 addition, information may be shared with appropriate Federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this SORN. This updated system will be included in the Department's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles 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 covered persons with a statutory right 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-014 Personnel Emergency Contact 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-014 Personnel Emergency Contact Information.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at DHS and Federal Emergency Management Agency (FEMA) Headquarters in Washington, D.C. and field offices.

Personnel emergency contact information is typically maintained locally by individual DHS offices.

SYSTEM MANAGER(S): The System Manager is the Director, Office of Operations Coordination (OPS), Department of Homeland Security, Washington, D.C. 20528.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Homeland Security Act of 2002, 6 U.S.C. sec. 313, 314, 317, 320, 321a, and 711; Robert T. Stafford Disaster Relief and Emergency Assistance Act, *as amended*, 42 U.S.C. sec. 5144, 5149, 5170b, 5192, and 5197.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is for DHS workforce accountability, to support DHS all-hazards emergency response deployments and exercises, and to contact designated persons in the event of an emergency.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals in this system include:

- Current and former DHS personnel, including Federal employees and contractors;
- Current and former Federal employees, contractors, or other individuals (e.g., SLTT personnel) who participate in or conduct emergency response training exercises;
- Current and former Federal employees, contractors, or other individuals (e.g., state, local, tribal, and territorial (SLTT) personnel) who respond to all-hazards emergencies including technical, manmade, or natural disasters;

and

- Individuals identified by current or former DHS personnel as emergency points of contact, including family members and next of kin.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records related to current and former DHS personnel, including Federal employees and contractors, include:

- Name;
- Work contact information (address, email address, phone, fax);
- Personal contact information (address, email address, phone numbers, pager number, and personal identification number [PIN]);
- Company/organization name;
- Supervisor name and contact information.

Categories of records related to DHS and non-DHS individuals identified as emergency points of contact may include:

- Name;
- Work contact information (address, email address, phone, fax);
- Personal contact information (address, email address, phone numbers, pager number, and pin number); and
- Relationship to current or former DHS personnel.

Categories of records related to DHS and non-DHS Federal employees, contractors or other individuals who participate in or who respond to all-hazards emergencies including

technical, manmade or natural disasters, or who participate in emergency response training exercises may include:

- Name;
- Social Security number;
- Date of birth;
- Identifiers related to deployment;
- Height, weight, and other personal characteristics, if applicable;
- Work contact information (address, email address, phone, fax);
- Personal contact information (address, email address, phone numbers, pager number, and pin number);
- Deployment contact information (lodging address and phone number) while deployed;
- Company/organization name and organization code;
- Job information (position title, start date, duty status, pay status, and employment type);
- Supervisor name and contact information;
- Deployment point of contact name and contact information;
- Approvals, authorizations, certifications, and proficiency levels for training and deployment;
- Information on deployment position (program area, position type);
- Geospatial location information;
- Status of credentials for access to regulated facilities;

- Status of Government credit card (yes or no);
- Clearance and access level;
- Deployment information (duty station, dates, and lodging);
- Skills inventory, qualifications, specialties, and proficiency levels;
- Volunteered medical information;
- Emergency response group/non-emergency response group status; and
- Emergency recall rosters.

RECORD SOURCE CATEGORIES: Records are obtained from DHS personnel (including Federal employees and contractors); individuals who participate in or conduct exercises or who respond to all-hazards emergencies including technical, manmade, or natural disasters; and other government agencies.

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 the U.S. Attorneys Offices, or other Federal agency conducting litigation or 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, only 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, 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 an appropriate Federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To a Federal, state, tribal, or local agency, if the information is relevant and necessary, for the requesting agency's approval on the issuance of a security clearance or for the purpose of providing support in an all-hazards emergencies including technical, manmade, or natural disasters.

I. To Federal, state, tribal, local, international, or foreign governmental agencies or executive offices, relief agencies, and non-governmental organizations, when disclosure is appropriate for performance of the official duties required in response to all-hazards including technical, manmade, or natural disasters.

J. To identified emergency contacts of:

1. Current and former DHS personnel, including Federal employees and contractors;
2. Current and former Federal employees, contractors, or other individuals who participate in or conduct exercises; or
3. Current and former Federal employees, contractors, or other individuals who respond to all-hazards emergencies including technical, manmade, or natural disasters.

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 or 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 an 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 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: DHS retrieves records by an individual's name, location, or other personal identifier.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records relating to current and former DHS employees, and individuals designated as emergency points of contact, will be reviewed annually and will be updated as necessary, and will be destroyed when obsolete, or upon separation or transfer of the employee, in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) GRS 5.3, Item No. 020 (DAA-GRS-2016-0004-0002). Records on non-DHS individuals will be deleted when obsolete and of no longer use to the Department. The Department also intends to rely on GRS 2.7, Employee Health and Safety, which is currently pending with NARA. Federal Emergency Management Agency Records Schedule EOM-16, which will cover records related to deployment activities, will be submitted by FEMA to NARA for review and approval. FEMA proposes that records related to deployment activities be considered temporary records with a cutoff at the end of each calendar year and are destroyed 50 years after the cutoff date.

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 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 an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform to the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's 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, an individual 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, the individual should:

- Explain why the individual believes the Department would have information on him/her;

- Identify which component(s) of the Department the individual believes may have the information about him or her;
- Specify when the individual believes 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 an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying his/her agreement for the first individual to access his or her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's 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 procedure."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 81 FR 48832 (July 26, 2016); 73 FR 61888 (October 17, 2008).

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2018-05403 Filed: 3/15/2018 8:45 am; Publication Date: 3/16/2018]