9110-9B

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0075]

Privacy Act of 1974; System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of New Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "Department of Homeland Security/ALL-042 Personnel Networking and Collaboration System of Records." This system of records allows DHS to collect and maintain records containing biographic information of employees and contractors of DHS for the purpose of professional networking and employee collaboration. This newly established 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 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-2017-0075 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 establish a new DHS system of records, "DHS/ALL-042 Personnel Networking and Collaboration System of Records."

DHS is issuing this system of records notice (SORN) to allow for the collection and sharing of biographical and professional information from Department personnel to facilitate and streamline collaborative work efforts, interactions, communications, and networking among Department employees, contractors, and grantees. Individuals may provide their general background or profile information, professional status and achievements, as well as educational accomplishments, for the purpose of fostering internal employee collaboration and communication across the homeland security enterprise. For instance, individuals may provide this information as part of DHS's use of social networking software-like tools within their closed, secure networks (e.g., blogs, which foster communication about new developments to internal teams and selected external partners within the DHS enterprise; wikis, which effectively aggregate and

publish the subject matter expertise of multiple authorized contributors; Facebook-like "walls," which allow ongoing discussions and information-sharing about specific topics; employee directories and organizational charts, which facilitate communication and networking, and social search/tagging, which allows DHS employees and contractors to add keywords, descriptors, and ratings to documents and other content). Individuals covered by this system who provide biographic information encourage communication and collaboration within the Department.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-042 Personnel Networking and Collaboration 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, 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 SORN.

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 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-042 Personnel Networking and Collaboration 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-042 Personnel Networking and Collaboration System of Records.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at the DHS Headquarters in Washington, D.C., and field offices.

SYSTEM MANAGER(S): For DHS Headquarters, 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 5 U.S.C. 301, 44 U.S.C. 3101; 44 U.S.C. 3534; Homeland Security Act

of 2002, and as amended; Executive Order 13576 (June 13, 2011).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to permit DHS's collection of biographical and professional information of current DHS employees, contractors, and grantees to facilitate connections and collaboration among individuals supporting the Department's mission; aid in the identification of individuals within an organization; and to ensure efficient collaboration within the Department.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Current DHS personnel, including employees, contractors, and grantees working in furtherance of the Department's mission. Former DHS personnel information may be included until the information is disposed of in accordance with National Archives and Records Administration retention schedules. This system covers all individuals who are authorized to access DHS information technology resources, which may include any lawfully designated representative of private enterprises and federal, state, territorial, tribal, local, international, or foreign government agencies or entities, in furtherance of the DHS mission.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Individual's name;
- Individual's photograph;
- Position/Title;
- Organization/Component affiliation;
- Business phone numbers;

- Business email addresses;
- Work/Office addresses;
- Educational background/history and accomplishments;
- Professional background/work history and accomplishments;
- Individual's military experience, if applicable; and
- Other relevant biographical information that the individual may voluntarily provide.

RECORD SOURCE CATEGORIES: Records are voluntarily obtained from the individual employee, contractor, or grantee.

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.

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: Records may be retrieved by an individual's name, component or affiliation, position or title, email

address, or an Electronic Data Interchange Personal Identifier. The Electronic Data Interchange Personal Identifier is a unique number assigned to the Personal Identity Verification (PIV) card that uniquely identifies each user. Records are not retrievable by message content or information contained therein.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records connected to social media that are not hosted on a DHS server are managed in accordance with General Records of the Department of Homeland Security Records Schedule Number DAA-0563-2013-0003. Information used to establish a profile on non-DHS information sharing and social media websites will be cut off at the end of the calendar year, and destroyed 5 years after the information has been superseded, or is obsolete. All other records covered by this SORN are managed in accordance with General Records Schedule (GRS) 5.1, item 010. Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists should be destroyed when the business use ceases.

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: 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 with 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 he/she 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/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/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, see "Record Access Procedures" above.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2018-04001 Filed: 2/27/2018 8:45 am; Publication Date: 2/28/2018]