



**9110-9B**

**DEPARTMENT OF HOMELAND SECURITY**

**[Docket No. DHS-2018-0029]**

**Privacy Act of 1974; System of Records**

**AGENCY:** Department of Homeland Security.

**ACTION:** Notice of a Modified System of Records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify a current DHS system of records titled, “DHS/All-016 Correspondence Records System of Records.” This system of records allows the Department to collect and maintain correspondence records. The Department is updating this system of records to reflect changes to the categories of individuals, categories of records, and routine uses. Specifically, these changes include expanding the categories of individuals to include third party subjects of correspondence who may not be the sender or recipient. The Department is also expanding the categories of records to permit the collection of an individual’s phone number, call and customer service center records, receipt number, case numbers relevant to the correspondence, and account IDs associated with correspondence between the Department and the responding party. DHS is updating routine use (E) and adding routine use (F) to comply with new policies pertaining to data breach procedures. The Department is making non-substantive edits to the routine uses to align with previously published Department systems of records notices (SORNs). Lastly, 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 become effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2018-0029 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.

*Instructions:* All submissions received must include the agency name and docket number DHS-2017-0029. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

*Docket:* For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general and privacy questions, please contact: Philip S. Kaplan, [Privacy@hq.dhs.gov](mailto:Privacy@hq.dhs.gov), 202-343-1717, Chief Privacy

Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

## **SUPPLEMENTARY INFORMATION:**

### **I. Background**

DHS is updating this Department-wide SORN under the Privacy Act for DHS correspondence records. DHS will use this system to collect and maintain correspondence records submitted by the general public, DHS personnel, and others. This SORN does not apply to correspondence related to Freedom of Information Act (FOIA) or Privacy Act requests, or to correspondence received in the course of standard immigration benefit application processes. This SORN also does not cover the underlying records associated with a response to correspondence.

This system allows DHS to collect and maintain incoming information and responses to inquiries, comments, or complaints made to the Department. Categories of individuals, categories of records, and routine uses of this system of records notice have been updated to better reflect the Department's correspondence record systems. This system modification will expand the categories of individuals to cover third parties whose information is submitted by the sender or recipient through an inquiry, comment, or complaint. DHS may collect and respond to this information from a third party. However, any investigations or awards initiated as a consequence of a third party's correspondence would not be covered under this SORN. DHS is also expanding the categories of records to permit the collection of an individual's phone number, call and customer service center records, receipt number, and case or account number associated or referenced in the

correspondence. DHS is modifying routine use (E) and adding routine use (F) to conform to Office of Management and Budget (OMB) Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (Jan. 3, 2017). All following routine uses are being re-lettered to account for the additional routine use. Non-substantive language changes have been made to additional routine uses to clarify disclosure policies that are standard across DHS and to align with previously published DHS SORNs. This modified 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, 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.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of

records to OMB and to Congress.

**SYSTEM NAME AND NUMBER:** Department of Homeland Security (DHS)/ALL-016  
Department of Homeland Security Correspondence Records System of Records.

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Records are maintained at several Headquarters locations and in component offices of the Department of Homeland Security, in both Washington, D.C. and field locations.

**SYSTEM MANAGER(S):** For DHS Headquarters, the System Manager is the Chief Information Officer, cio@hq.dhs.gov, 202-447-3735, Department of Homeland Security, Washington, D.C. 20528. For components of DHS, the System Managers are their respective Chief Information Officers. Links to component contact information can be found at <https://www.dhs.gov/direct-contact-information> under “Contact information for DHS Components.”

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 5 U.S.C. 301, 31 U.S.C. 1115(b)(6), 44 U.S.C. 3101, 44 U.S.C. 3506, 40 U.S.C. 11313, E.O. 13571.

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to manage all correspondence including incoming information and responses to inquiries, comments, or complaints made to DHS.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Individuals who submit inquiries, complaints, comments, or other correspondence to DHS, excluding Privacy Act or FOIA requests, or standard immigration applications; individuals who are the subject of the correspondence; and any responding individual on behalf of DHS are

covered by this SORN.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

- Full name;
- Physical and mailing addresses;
- Email address;
- Phone number;
- Web form information (e.g., IP addresses);
- Who the complaint, compliment, comment, or issue is about;
- Incoming correspondence excluding Privacy Act or FOIA requests, or standard immigration applications;
- DHS's reply;
- Responder's name on behalf of DHS;
- Call and Customer Service Center records (to include recordings of calls and online real time interactions with customer service representatives);
- Associated case or file numbers (e.g., Alien Number);
- Receipt number;
- Account ID;
- Additional unsolicited personal information provided by the individual (including Social Security number); and
- Other related materials.

**RECORD SOURCE CATEGORIES:** Records are obtained from all sources of

incoming correspondence and responses by DHS. A non-exclusive list of correspondence sources includes members of the general public, call and customer service centers, unions, trade organizations, non-profits, business or governmental entities, including the news media and congressional offices.

**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. 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. 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 or General Services

Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 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 suspects or has confirmed that there has been a breach of the system of records; (2) 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 (3) 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 another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the 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.

G. 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.

H. To an appropriate Federal, state, tribal, territorial, 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.

I. To another Federal agency to refer correspondence or respond to correspondence given the nature of the complaint, compliment, comment, or issue.

J. To unions recognized as exclusive bargaining representatives of the individual under the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114, the Merit Systems Protection Board, arbitrators, the Federal Labor Relations Authority, and other parties responsible for the administration of the Federal labor-management program for the purpose of processing any corrective action, or grievances, or conducting administrative hearings or appeals, or if needed in the performance of other authorized duties.

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 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:** Records may be retrieved by individual name and date of correspondence.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF**

**RECORDS:** Executive level records are permanent and files are cut off annually and transferred to the National Archives and Records Administration 15 years after cut-off date, in accordance with National Archives and Records Administration (NARA) General Schedule DAA-0563-2013-0005-0003. Public correspondence and communication that require no formal response or action are temporary and are destroyed when 90 days old, unless longer retention is authorized when required for business use, in accordance with NARA General Records Schedule (GRS) 6.4, item 20. Correspondence relating to a specific case or action is not considered public correspondence and will be filed and maintained with the appropriate case or action file under its specific retention schedule. DHS Components may create their own retention schedules for correspondence received. NARA GRS 4.1, item 010, covers when a Department, Component, office, or individual is tasked to review the correspondence or inquiry. Actual assignments and any reminder emails that an action is required are destroyed immediately, or when no longer needed for reference.

**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 any paper files or computer systems 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 Chief FOIA Officer, or a component FOIA Officer, whose contact information can be found at

<http://www.dhs.gov/foia> under “contact 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 JRA provide a right of access, certain records about a person may be available under FOIA.

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 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/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, in accordance with 6 CFR Part 5.21, 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 or covered JRA records, see "Record Access Procedures" above, and 6 CFR Part 5.

**NOTIFICATION PROCEDURES:** See "Record Access Procedures."

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** 73 FR 66657.

Philip S. Kaplan,  
Chief Privacy Officer,  
Department of Homeland Security.  
[FR Doc. 2018-20876 Filed: 9/25/2018 8:45 am; Publication Date: 9/26/2018]