



9112-FL

## DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2019-0059]

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

**AGENCY:** Department of Homeland Security.

**ACTION:** Notice of a New 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-044 DHS eRulemaking System of Records.” DHS eRulemaking allows the public to search, view, download, and comment on all DHS rulemaking and notice documents in one central online system. It consists of a public facing interface, [www.regulations.gov](http://www.regulations.gov), and a portal visible to DHS, called the Federal Docket Management System (FDMS). This system of records notice covers the various records maintained by the Department of Homeland Security and its Components pertaining to written data, views, or arguments submitted to the Department. This newly established system will be included in DHS’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. 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-2019-0059 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: Jonathan R. Cantor, Acting 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-2019-0059. 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:** Jonathan R. Cantor, (202) 343-1717, [Privacy@hq.dhs.gov](mailto:Privacy@hq.dhs.gov), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

**SUPPLEMENTARY INFORMATION:**

I. Background

In October 2002, the eRulemaking Program was established as a cross-agency initiative under Section 206 of the E-Government Act of 2002. The eRulemaking system, managed by the General Services Administration, effective as of October 1, 2019, is a centralized repository for all Federal rulemaking dockets, including Notices of Proposed Rulemaking, Interim Rules, supporting materials such as scientific or economic analyses, and public comments, as well as for non-rulemaking dockets, such as Notices. It consists of a public facing interface, [www.regulations.gov](http://www.regulations.gov), and a portal visible to DHS, called the Federal Docket Management System (FDMS). The Federal Docket Management System

is a Federal-wide document management system. DHS employees may self-register to use FDMS.gov and will only see dockets belonging to their Component.

Persons who use eRulemaking to submit a comment on a DHS or a DHS component Federal rulemaking may be asked to provide name and contact information (e-mail or mailing address). If that submission meets all requirements, as determined by DHS, it will be posted on the public eRulemaking website—<http://www.regulations.gov>—for public viewing, and all the contents of the posted comment will be searchable. eRulemaking provides a full text search capability, including any name and identifying information submitted in the body of the comment. Names of individuals and organizations submitting comments using the eRulemaking system, if names are provided, will be posted on the <http://www.regulations.gov> site with their respective comments for public viewing. Contact information (such as email or mailing address) will not be available for public viewing, unless the submitter includes that information in the body of the docket submission. DHS does retain submitted contact information as part of this system in FDMS.

DHS may choose not to post certain types of information contained in a docket submission yet preserve the entire submission to be reviewed and considered as part of the rulemaking docket by the Component. For example, comments containing material restricted from disclosure by Federal statute may not be publicly posted or viewable on <http://www.regulations.gov>, but will be retained and considered by DHS. Similarly, if a person chooses to submit a comment on a rulemaking through the mail rather than through <http://www.regulations.gov>, or if a person submits a comment through mail after being directed to do so by DHS instructions because of sensitive contents of that

individual's comment (e.g., if it constitutes Chemical-terrorism Vulnerability Information, Protected Critical Infrastructure Information, or Sensitive Security Information), that comment may not appear on the public website, but will be retained and considered by DHS as part of the rulemaking process.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-044 DHS eRulemaking 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 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 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 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-044 eRulemaking 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-044 eRulemaking.

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Records are maintained at the DHS Headquarters in Washington, D.C., and Component offices in DHS, in both Washington, D.C. and field offices. Records received through [www.regulations.gov](http://www.regulations.gov) or uploaded to FDMS are retained at GSA Headquarters in Washington, D.C.

**SYSTEM MANAGER(S):** Associate General Counsel for Regulatory Affairs, [dhsogcregulations@hq.dhs.gov](mailto:dhsogcregulations@hq.dhs.gov), Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, SE, Washington, D.C. 20528.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** Section 206(d) of the E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. 3501 note); 5 U.S.C. § 553; 6 U.S.C. 101, et seq.

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to permit members of the public to review and comment on DHS rulemakings and notices. DHS will use any submitted contact information to seek clarification of a comment, respond to a comment when warranted, and for such other needs as may be associated with the rule making or notice process.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Any individual who provides personally identifiable information to DHS when commenting on a DHS rulemaking or notice and individuals mentioned or identified in the body of a comment.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Categories of records contained in eRulemaking include:

- Name
- Mailing Address
- Email Address
- Phone Number
- Fax Number
- Representative Name
- Organization name
- Additional information provided in the submitted comment and other supporting documentation provided in response to a DHS rulemaking or notice.

**RECORD SOURCE CATEGORIES:** DHS receives records from members of the public; representatives of Federal, state, or local governments; non-government organizations; and the private sector.

**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 agencies 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. secs. 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 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 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.

I. To the General Services Administration, as the system manager of FDMS, to provide technical or other administrative support.

J. 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. The records may be stored on magnetic disc, tape, and digital media.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** DHS may be retrieve records by keyword, document identification number, comment tracking number, document title, Code of Federal Regulation (CFR) (search for a specific title within the CFR), CFR citation (search for the part or parts within the CFR title being searched), document type, document sub type, date posted, and comment period end date.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** DHS retains records covered by the eRulemaking system in accordance with General Records Schedule (GRS) 4.2, Item 001, and 6.6, Item 30. Public comments received in response to a proposed SORN are destroyed three years after publication but may be kept longer if required for business use. Public comments received in response to a proposed rule are destroyed one year after publication of the final rule or decision to abandon publication but may be kept longer if required for business use.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** The GSA information technology system that hosts regulations.gov and FDMS is in a facility protected by physical walls, security guards, and requires identification badges. Rooms housing the information technology system infrastructure are locked, as are the individual server racks. All security controls are reviewed on a periodic basis by external assessors. The controls themselves include measures for access control, security awareness training, audits, configuration management, contingency planning, incident response, and maintenance.

Records in FDMS are maintained in a secure, password-protected electronic system that uses security hardware and software to include multiple firewalls, active intrusion detection, encryption, identification and authentication of users.

DHS safeguards records maintained outside of FDMS and www.regulations.gov 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 or Component's 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 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 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 or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- 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 the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

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, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

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

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

**HISTORY:** None.

Jonathan R. Cantor,  
Acting Chief Privacy Officer,  
Department of Homeland Security.

[FR Doc. 2020-04983 Filed: 3/10/2020 8:45 am; Publication Date: 3/11/2020]