DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2022-0042]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security Federal Emergency Management Agency.

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 update and reissue a current system of records titled, "Department of Homeland Security/Federal Emergency Management Agency (FEMA)-012 Suspicious Activity Reporting System of Records." This system of records allows DHS/FEMA to collect, maintain, and retrieve records on individuals reported as being involved in suspicious activities, individuals who report suspicious activities, and individuals charged with the analysis and appropriate handling of suspicious activity reports. DHS/FEMA is updating this system of records to (1) revise contact and administrative information associated with this system of records, (2) add to the categories of records collected, (3) modify routine uses, and (4) other non-substantive changes. This updated 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 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-2022-0042 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: Mason Cutter, 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-2022. 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 questions please contact: Tammi Hines, (202) 646-3606, FEMA-Privacy@fema.dhs.gov, Privacy Officer, Federal Emergency Management Agency, Department of Homeland Security, Washington, D.C., 20478. For privacy questions please contact: Mason Cutter, (202) 343-1717, Privacy@hq.dhs.gov, 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, DHS/FEMA proposes to update and reissue a current DHS/FEMA system of records titled, "DHS/FEMA-012 Suspicious Activity Reporting System of Records." FEMA's mission is to "support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards." In support of this mission, and to ensure the safety of its citizens and first responders, FEMA collects, maintains, and retrieves records of individuals reported as being involved in suspicious activities and of individuals who report suspicious activities. FEMA's Office of the Chief Security Officer (OCSO), Fraud Investigations and Inspections Division (FIID) manages this process. Investigators and Analysts are assigned to complete the analysis of suspicious activity reports; they are also responsible for the appropriate handling of such reports.

FEMA Suspicious Activity Reports may be shared with federal, state, local, and tribal jurisdictions with responsibility for investigating suspicious activities within their jurisdictions. FEMA Suspicious Activity Reports that have a nexus to terrorism or hazards to homeland security, as determined by FEMA FIID Investigators or Analysts, and require immediate attention are reported to the police or law enforcement agency of jurisdiction via telephone and uploaded into the Federal Bureau of Investigation's (FBI) eGuardian system by FEMA FIID Investigators or Analysts in coordination with the agency that reported the information. All investigators and analysts who submit reports to the eGuardian system are trained in the DHS Nationwide Suspicious Activity Reports Initiative, per DHS policy.

FEMA is updating this System of Records Notice to reflect the following changes: (1) the contact information for general questions and administrative information has been updated, as well as the Authority for Maintenance of the System section; (2) the categories of records have been updated to clarify the information collected in suspicious activity reports; and (3) Routine Use E has been modified and Routine Use F has been added to conform to Office of Management and Budget (OMB) Memorandum M-17-12 regarding breach notification and investigation.

Furthermore, non-substantive changes to simplify the formatting and text of the previously published notice and the references to FEMA's Office of Chief Security Officer (OCSO) have been updated to identify FEMA's Fraud Investigations and Inspections Division as the specific office responsible for suspicious activity reporting.

Consistent with DHS's information sharing mission, information stored in the DHS/FEMA-012 Suspicious Activity Reporting System of Records 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 system of records notice.

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. The Privacy Act defines "individual" 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, and judicial review of 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/FEMA-12 Suspicious Activity Reporting System of Records.

In accordance with 5 U.S.C. 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)/Federal Emergency Management Agency (FEMA)-012 Suspicious Activity Reporting System of Records.

SECURITY CLASSIFICATION: For official use only (FOUO) and law enforcement sensitive (LES). This system does not contain classified information.

SYSTEM LOCATION: Records are maintained on a FEMA Exchange Server that is access-controlled and under the management and control of the Federal Emergency Management Agency (FEMA) Office of Chief Information Officer at FEMA Headquarters, 500 C Street SW, Washington, D.C., 20472.

SYSTEM MANAGERS: Office of the Chief Security Officer, Fraud Investigations and Inspections Division, 500 C Street SW, Washington, D.C., 20472.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 42 U.S.C. 5196(d); Executive Orders 12333 and 13388; 40 U.S.C. 1315(b)(2)(F); 6 U.S.C. 314 of the Homeland Security Act of 2002, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; and the National Security Act of 1947, as amended.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect, investigate, analyze, and report suspicious activities to the police or law enforcement agency of jurisdiction and upload the Suspicious Activity Reports into the FEMA Exchange Server in coordination with the agency that reported the information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by the system include individuals reported as being involved in suspicious activities, individuals who report suspicious activities, and Fraud Investigations and Inspections Division Investigators and Analysts assigned to analyze and appropriately handle suspicious activity reports.

CATEGORIES OF RECORDS IN THE SYSTEM:

The following fields related to individuals may be maintained in this system:

- Report of the suspicious activity (e.g., description of the suspicious activity and physical descriptors of individuals involved in suspicious activity);
- Case/incident number;
- Name (first, middle, and last);
- Address (number, street, apartment, city, and state);

- Age;
- Sex;
- Race for subject description;
- Signature (investigator, analyst, or law enforcement officer (LEO));
- Jurisdiction over the suspected activity;
- Injury code (a dropdown that lists the codes in question (0-None, 1-Refused, 2-First Aid, 3-Hospital, 4-Deceased) (if applicable));
- Telephone numbers (home, business, or cell);
- Other contact information (e.g., email address); and
- Property information (e.g., name, quantity, serial number, brand name, model, value, year, make, color, identifying characteristics, registration information).

RECORD SOURCE CATEGORIES: Records are obtained from individuals reported as being involved in suspicious activities, individuals who report suspicious activities, Fraud Investigations and Inspections Division Investigators and Analysts, commercially available systems (LexisNexis) and other federal, state, and local law enforcement 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. 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 to another federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant and 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 their official capacity;

3. Any employee or former employee of DHS in their 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. §§ 2904 and 2906.

D. To an agency, organization, or individual 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 an appropriate federal, state, tribal, local, international counterterrorism agencies when DHS becomes aware of an indication of a threat or potential threat to security, and when such use is to assist in counterterrorism efforts.

J. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life, property, or other vital interests of a data subject and disclosure is proper and consistent with the official duties of the person making the disclosure.

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 is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined 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/FEMA stores records in this system electronically on the access-controlled FEMA Exchange Server.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/FEMA retrieves records by case/incident number, name, address, and/or date.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Pursuant to National Archives and Records Administration Schedule Number N1-311-99-6, Items 1, 2, and 3, files containing information or allegations that are of an investigative nature but do not relate to a specific investigation are destroyed after five (5) years. Investigative case files that involve allegations made against senior agency officials, attract significant attention in the media, attract congressional attention, result in substantive changes in agency policies and procedures, or are cited in the Office of the Inspector General's (OIG) periodic reports to Congress are cut off when the case is closed, retired to the Federal Records Center (FRC) five (5) years after cutoff, and then transferred to the National Archives and Records Administration twenty (20) years after cutoff. All other investigative case files are placed in inactive files when a case is closed, cut off at the end of fiscal year, and destroyed ten (10) years after cutoff, except those that are unusually significant for documenting major violations of criminal law or ethical standards by agency officials or others.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/FEMA safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS systems security and access policies. DHS/FEMA imposes 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 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: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/FEMA will consider individual requests to determine whether information may be released. Thus, 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 FEMA's Freedom of Information Act (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 them, 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, or electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form. 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 themself 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 their identity, meaning that the individual must provide their 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. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. An individual may obtain more information about this process at http://www.dhs.gov/foia. In addition, the individual should:

- Explain why they believe the Department would have information being requested;
- Identify which component(s) of the Department they believe may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the DHS 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 Judicial Redress Act (JRA) records, individuals may make a request for amendment or correction of a Department record 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. When an individual is making a request for amendment or correction of Departmental records about themself 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.

NOTIFICATION PROCUEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

HISTORY: 79 FR 40124 (July 11, 2014).

****

Mason C. Clutter,
Acting Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2023-06745 Filed: 3/30/2023 8:45 am; Publication Date: 3/31/2023]