9110-17

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0035]

Privacy Act of 1974; Department of Homeland Security Federal Emergency Management Agency - 012 Suspicious Activity Reporting System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current system of records titled, "Department of Homeland Security/Federal Emergency Management Agency – 012 Suspicious Activity Reporting System of Records." This system of records allows the Department of Homeland Security/Federal Emergency Management Agency to collect and maintain records on individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged with the analysis and appropriate handling of suspicious activity reports. As a result of the biennial review, the Federal Emergency Management Agency has made non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2014-0035 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: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, 245 Murray Drive, SW, Building 410, STOP-0655, Washington, D.C. 20528.
- Instructions: All submissions received must include the agency name and docket number for this rulemaking. 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: Eric M. Leckey, (202) 212-5100, Privacy Officer, Federal Emergency Management Agency, Department of Homeland Security, Washington, D.C. 20478. For privacy questions please contact: Karen Neuman (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, 245 Murray Drive, SW, Building 410, STOP-0655, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of

Homeland Security (DHS) Federal Emergency Management Agency (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." FEMA collects, maintains, and retrieves records of individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged with the analysis and appropriate handling of suspicious activity reports. FEMA's Office of the Chief Security Officer (OCSO), Fraud and Investigations Unit manages this process. FEMA Suspicious Activity Reports (SAR) are secured in a room monitored by FEMA OCSO special agents and analysts to reduce any risk of unauthorized access.

FEMA SARs may be shared with federal, state, local, and tribal jurisdictions that have the responsibility of investigating suspicious activities within their jurisdictions. FEMA SARs that do not have a nexus to terrorism or hazards to homeland security, (as determined by FEMA OCSO special agents or analysts) are forwarded to the appropriate jurisdiction (such as sheriff offices, county/city police, and state police). FEMA SARs that have a nexus to terrorism or hazards to homeland security, (as determined by FEMA OCSO special agents or analysts), are shared with the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF), Federal Protective Service, and/or other federal agencies that are required to investigate and respond to terrorist threats or hazards to homeland security.

As a result of the biennial review, FEMA has made non-substantive changes to simplify the formatting and text of the previously published notice. FEMA's SAR process is authorized and governed by 44 CFR Chapter 2 "Delegation of Authority;" 42 U.S.C. § 5196(d); Executive Order No. 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; the National Security Act of 1947, as amended; and FEMA Manual 1010-1 "Federal Emergency Management Agency Missions and Functions."

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 updated 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 the U.S. government collects, maintains, uses, and disseminates 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. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

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 of Records

Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) – 012

System name:

DHS FEMA – 012 Suspicious Activity Reporting.

Security classification:

For official use only (FOUO) and law enforcement sensitive (LES).

System location:

FEMA maintainsrecords at FEMA Headquarters in Washington, D.C., and in field offices.

Categories of individuals covered by the system:

Categories of individuals includes individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged

with the analysis and appropriate handling of suspicious activity reports.

Categories of records in the system:

- Case/incident number;
- Name (first, middle, and last);
- Address (number, street, apartment, city, and state);
- Age;
- Sex;
- Race;
- Signature (investigator, analyst, or law enforcement officer (LEO));
- Jurisdiction;
- Injury code (if applicable);
- Telephone numbers (home, business, or cell);
- Other contact information (e.g., email address); and
- Property information (name, quantity, serial number, brand name, model, value, year, make, color, identifying characteristics, and/or registration information).

Authority for maintenance of the system:

44 CFR Chapter 2 “Delegation of Authority;" 42 U.S.C. § 5196(d); Executive Order No. 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; the National Security Act of 1947, as amended; and FEMA Manual 1010-1 “Federal Emergency Management Agency Missions and Functions.”

Purpose(s):

The purpose of this system is to collect, investigate, analyze, and report suspicious activities to the Federal Bureau of Investigations (FBI) Joint Terrorism Task Force (JTTF), Federal Protective Service, and/or other federal, state, or local agencies required to investigate and respond to terrorist threats or hazards to homeland security.

Routine uses of records maintained in the system, including categories of users and the 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 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 U.S. 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 the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; 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 compromise and 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 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.

I. 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.

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 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.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

FEMA stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, and digital media.

Retrievability:

FEMA retrieves records by case/incident number, name, address, and/or date.

Safeguards:

FEMA safeguareds records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. FEMA imposes strict controls to minimize the risk of compromising the information that is being stored. FEMA limits access to the computer system containing the records 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.

Retention and disposal:

Pursuant to National Archives and Records Administration (NARA) 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

when five years old. 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 Investigator General (OIG)'s periodic reports to Congress are cut off when the case is closed, retired to the Federal Records Center (FRC) five years after cutoff, and then transferred to NARA 20 years after cutoff. All other investigative case files are placed in inactive files when case is closed, cut off at the end of fiscal year, and destroyed 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.

System Manager and address:

Office of the Chief Security Officer, Fraud and Investigation Unit, 1201 Maryland Avenue, SW, Washington, D.C. 20024.

Notification procedure:

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 or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief of the FEMA Disclosure Branch whose contact information can be found at http://www.dhs.gov/foia under "contacts." 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, 245 Murray Drive, SW, Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your 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. While no specific form is required, you 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 you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe 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 your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records are obtained from individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged with the analysis and appropriate handling of suspicious activity reports, commercially available systems, and also from other federal, state, and local law enforcement agencies.

Exemptions claimed for the system:

The Secretary of Homeland Security 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) pursuant to 5 U.S.C. § 552a (k)(2).

Dated: June 24, 2014.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2014-16112 Filed 07/10/2014 at 8:45 am; Publication Date: 07/11/2014]