9110-17

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2016-0023]

Privacy Act of 1974; Department of Homeland Security, Federal Emergency Management Agency-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of 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 system of records titled, "DHS/Federal Emergency Management Agency (FEMA)-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records." This system of records authorizes DHS/FEMA to monitor, collect, and maintain information from publicly available social media sources to provide critical situational awareness in support of FEMA's mission to reduce the loss of life and property and protect the nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters. FEMA's social media monitoring initiative was neither designed nor intended to collect personally identifiable information (PII); however, given the unpredictable nature of disasters and emergency management, the content that is posted, and the voluntary and unrestricted nature of social media, it is possible for FEMA to collect, maintain, and in extremis circumstances, disseminate a limited amount of PII to first

responders. FEMA is publishing this System of Records Notice because FEMA may collect PII from social media for certain narrowly tailored categories. For example, in the event of an in extremis situation involving potential life and death, FEMA will collect and share certain PII with Federal, State, local, tribal, and territorial first responders in order for them to take the necessary actions to save a life, such as the name and location of a person asking for help during a man-made or natural disaster. This new system of records 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 [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0023 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, please visit 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. 20528. For privacy questions, please contact: Karen L. 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 establish a new DHS system of records titled, "DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records."

This system of records will allow DHS/FEMA to maintain a state of disaster and emergency response readiness through situational awareness of publicly available information posted on social media to take appropriate actions when necessary or to provide information related to a disaster to the first responder community for situational awareness purposes. Situational awareness is defined as "information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision-making." See sec. 515 of

the Homeland Security Act (6 U.S.C. 321d(b)(1)).

The DHS/FEMA Office of Response and Recovery (ORR), Response Directorate is the office responsible for situational awareness activities and also operates DHS/FEMA Watch Centers, including the National Response Coordination Center (NRCC) and FEMA's Regional Response Coordination Centers (RRCC). The Operational Use of Publicly Available Social Media for Situational Awareness Initiative, as led by the DHS/FEMA ORR, monitors and reviews publicly available social media and uses a set of keywords or "hash-tags" to find and retrieve content relevant to DHS/FEMA for situational awareness purposes. Under this Initiative, DHS/FEMA generally will not: (1) actively seek PII; (2) post any information; (3) actively seek to connect with other internal/external personal users; (4) accept other internal/external personal users' invitations to connect; or (5) interact on social media sites. However, DHS/FEMA is permitted to establish user names and passwords to form profiles and follow relevant government, media, and subject matter experts on social media sites in order to use search tools under established criteria and search terms for monitoring that supports providing situational awareness and establishing a common operating picture.

DHS/FEMA social media monitoring is not designed to collect PII from members of the public; however, given the unpredictable nature of disasters and emergency management and the unrestricted nature of social media, DHS/FEMA may collect a limited amount of PII from the public through its monitoring of social media. The information may be provided to first responders during in extremis situations involving the possible loss of life. PII on the following categories of individuals may be collected

when it lends credibility to the report or facilitates coordination with Federal, State, local, tribal, territorial (SLTT), foreign, or international government partners: (1) individuals within the United States in extremis situations involving potential life or death circumstances; (2) senior U.S. Government officials who make public statements or provide public updates about natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents; (3) U.S. Government spokespersons who make public statements or provide public updates about natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents; (4) U.S. private sector officials and spokespersons who make public statements or provide public updates about natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents; (5) names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article, or who use traditional and/or social media in real time to keep their audience situationally aware and informed; and (6) public officials, current and former, who are victims of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.

Consistent with DHS's information-sharing mission, information stored in the DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness 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, DHS/FEMA may share information from this system 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.

DHS is publishing this system of records notice to describe DHS/FEMA's collection of PII through social media monitoring. DHS/FEMA collects and maintains minimal PII that is necessary to respond to, report on, and contact or assist individuals in extremis situations. 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. 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-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness 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.

DHS/FEMA-013

System of Records:

Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)-013

System name:

DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records.

Security classification:

Unclassified.

System location:

DHS/FEMA retains records at the DHS/FEMA Headquarters in Washington, D.C., DHS/FEMA regional field offices, and at the DHS National Operations Center, in Washington, D.C.

Categories of individuals covered by the system:

Categories of individuals covered by the system:

- Individuals located within the United States in extremis situations involving potential life or death circumstances;
- Senior U.S. Government officials who make public statements or provide public updates about natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents;

- U.S. Government spokespersons who make public statements or provide public updates about natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents;
- U.S. private sector officials and spokespersons who make public statements or provide public updates about natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents;
- Names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed (including known subject matter experts such as emergency management volunteers, tornado spots, and Community Emergency Response Team members) about natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents; and
- Current and former public officials who are victims of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.

Categories of records in the system:

Through the course of normal social media monitoring, FEMA does not collect any records from individuals. However, in extremis situations FEMA may collect:

- Individual's name;
- Social media account information including: Email address, Login ID, Handle, User Name, or Alias;

- Address or approximate location (via geo-coded submission);
- Job title or Position;
- Phone numbers, email address, or other contact information included in or associated with a user profile;
- Date and Time of post; and
- Additional details relevant to an in extremis situation (e.g., details of an individual's physical condition).

This system of records may also include:

- Reports related to incidents or updates seen via social media;
- Links to original social media content described in reports; and
- Links to other open source media such as a publicly available news websites.

Authority for maintenance of the system:

6 U.S.C. 313(b)(2)(A)-(H); 6 U.S.C. 314(b)(1), 6 U.S.C. 314(a)(17); and 6 U.S.C. 321d(b)(1).

Purpose(s):

The purpose of this system is to monitor and review publicly available social media Internet sources for situational awareness to maintain timely, actionable decision-making. DHS/FEMA collects PII through social media Internet sources to respond to and provide potentially lifesaving assistance to the individual only in extremis situations.

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 United States 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 or her official capacity;

3. Any employee or former employee of DHS in his or 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 (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 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 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 Federal, State, local, tribal emergency management agencies, and the National Center for Missing and Exploited Children, and other partners who assist in emergency response, reunification, or rescue efforts.

Disclosure to consumer reporting agencies:

None.

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

Storage:

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

Retrievability:

Much of the data within this system does not pertain to an individual; rather, the information pertains to locations, geographic areas, facilities, and other things or objects not related to individuals. However, in the event that PII is collected, DHS/FEMA may retrieve records by date, time stamp, incident name, individual name, or social media user name.

Safeguards:

DHS/FEMA safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access

policies. Strict controls are in place 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 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:

FEMA's ORR is collaborating with FEMA Records Management Division and NARA to establish an approved retention and disposal policy for any records created through this initiative related to its situation reports and responses to in extremis situations. However, all PII from reports are redacted once the information is sent to the appropriate first responders in extremis situations.

System Manager and address:

Director of National Watch Center, Response Directorate, FEMA, 500 C Street, SW, Washington, D.C. 20472.

Notification procedure:

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 DHS/FEMA Freedom of Information Act (FOIA) Officer, 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 FOIA 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 FOIA 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 the above 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:

DHS/FEMA may collect information from members of the public, first responders, press, volunteers, and others that provide publicly available information on social media sites including online forums, blogs, public websites, and message boards. All DHS/FEMA users of social media are clearly identified as DHS/FEMA employees and do not collect any information that is not publicly available or inaccessible due to user privacy settings.

Exemptions claimed for the system:

None.

Dated: April 14, 2016.

Karen L. Neuman,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2016-09191 Filed: 4/20/2016 8:45 am; Publication Date: 4/21/2016]