9110-9A

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0025]

Privacy Act of 1974; Department of Homeland Security Office of Operations Coordination and Planning-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of an updated 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 Department of Homeland Security system of records titled, "Department of Homeland Security/Office of Operations Coordination and Planning-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records." The Office of Operations Coordination and Planning National Operations Center created the Publicly Available Social Media Monitoring and Situational Awareness Initiative to assist the Department of Homeland Security (DHS) and its Components involved in fulfilling DHS's statutory responsibility to provide situational awareness. As a result of a biennial review of this system, the Department of Homeland Security/Office of Operations Coordination and Planning is updating this system of records notice to (1) clarify the information that may

be collected about anchors, newscasters, or other on-scene reporters; (2) permit the collection of information about current and former public officials who are potential victims of incidents or activities related to Homeland Security; (3) clarify the system classification level; and (4) clarify the record source categories. This updated system will continue to 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 DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2015-0025 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, 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: Michael Page, (202) 357-7626, Privacy Point of Contact, Office of Operations Coordination and Planning, 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, 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) Office of Operations Coordination and Planning (OPS) proposes to update and reissue a current DHS system of records titled, "DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records."

The DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records allows the DHS/OPS National Operations Center (NOC) to fulfill its mandate to provide situational awareness and a common operating picture for the entire Federal Government, and for state, local, and tribal governments as appropriate, and to ensure that critical terrorism and disaster-related information reaches government decision-makers. 6 U.S.C. § 321d(b). As a result of a biennial review of this system, DHS is updating this SORN to (1) clarify that the fifth category of individuals may include any of the categories of records for anchors, newscasters, or on-scene reporters; (2) expand the sixth category of individuals to include current and former public officials who are potential victims of incidents or activities related to Homeland

Security; (3) limit the system classification to Unclassified and For Official Use Only; and (4) update the record source categories to clarify that all records within this system are collected from publicly available social media websites.

As described in the DHS/OPS/PIA-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative Privacy Impact Assessment and associated updates (which are available on the DHS Privacy Office website at http://www.dhs.gov/privacy), the NOC monitors publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators, the NOC monitors activities on social media for information it can use to provide situational awareness and establish a common operating picture. The NOC gathers, stores, analyzes, and disseminates relevant and appropriate de-identified information to federal, state, local, and foreign governments, and private sector partners authorized to receive situational awareness and a common operating picture. Under this initiative, OPS generally does not: 1) actively seek personally identifiable information (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, OPS 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. Furthermore, 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, foreign, or international government partners: 1) U.S. and foreign individuals in extremis situations involving potential life or death circumstances; 2) Senior U.S. and foreign government officials who make public statements or provide public updates; 3) U.S. and foreign government spokespersons who make public statements or provide public updates; 4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates; 5) Anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional or social media in real time to keep their audience situationally aware and informed; 6) public officials, current and former, who are victims or potential victims of incidents or activities related to Homeland Security and; 7) known terrorists, drug cartel leaders, or other persons known to have been involved in major crimes or terror of Homeland Security interest who are killed or found dead.

The NOC will identify and monitor only information needed to provide situational awareness and establish a common operating picture. The NOC will use this information to fulfill the statutory mandate set forth in 6 U.S.C. § 321d(b) to include the sharing of information with foreign governments and the private sector as otherwise authorized by law.

DHS is authorized to implement this program primarily through 6 U.S.C. § 121; 44 U.S.C. § 3101; Executive Order (E.O.) 13388; 6 U.S.C. § 321d; and Homeland Security Presidential Directive 5. Routine uses contained in this notice include sharing with the Department of Justice (DOJ) for legal advice and representation; to a

congressional office at the request of an individual; to NARA for records management; to contractors in support of their contract assignment to DHS; to appropriate federal, state, tribal, local, international, foreign agency, or other appropriate entity including the privacy sector in their role aiding OPS in their mission; to agencies, organizations, or individuals for the purpose of audit; to agencies, entities, or persons during a security or information compromise or breach; or to an agency, organization, or individual when there could potentially be a risk of harm to an individual. This system of records is not subject to the Paperwork Reduction Act because DHS is not requesting specific information from the public.

Consistent with DHS's information sharing mission, information contained in the DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records may be shared with other DHS Components, as well as appropriate federal, state, local, tribal, territorial, foreign, or international government agencies. This sharing will take place only after DHS determines that the receiving DHS Component or agency has a verifiable need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions 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 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" as a U.S. citizen or a lawful permanent resident. 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/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative 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)/Office of Operations Coordination and Planning (OPS)-004.

System name:

DHS/OPS-004.

Security classification:

Unclassified, For Official Use Only.

System location:

Records are maintained at the Department of Homeland Security (DHS) Office of Operations Coordination and Planning (OPS) National Operations Center (NOC) Headquarters in Washington, D.C. and field locations.

Categories of individuals covered by the system:

Categories of individuals covered by the system may include:

- U.S. and foreign individuals in extremis situations involving potential life or death circumstances;
- Senior U.S. and foreign government officials who make public statements or provide public updates;
- U.S. and foreign government spokespersons who make public statements or provide public updates;
- U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates;
- Anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional or social media in real time to keep their audience situationally aware and informed;
- Current and former public officials who are victims or potential victims of incidents or activities related to Homeland Security; and
- Known terrorists, drug cartel leaders, or other persons known to have been involved in major crimes or terror of Homeland Security interest (e.g., mass shooters such as those at Navy Yard or Los Angeles airport), who are killed or found dead.

Categories of records in the system:

Categories of records in the system may include:

- Full name;

- Affiliation;
- Position or title; and
- Publicly available user ID.

Authority for maintenance of the system:

6 U.S.C. § 121; 44 U.S.C. § 3101; Executive Order (E.O.) 13388; Office of Operations Coordination and Planning Delegation 0104; and Homeland Security Presidential Directive 5.

Purpose(s):

The purpose of this system is to fulfill the DHS Office of Operations and Coordination's (OPS) statutory responsibility to provide situational awareness and establish a common operating picture for the entire Federal Government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers. DHS/OPS NOC may share information with private sector and international partners when necessary, appropriate, and authorized by law.

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 other federal agencies conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation or proceedings and one of the following is a party to the litigation or proceedings or has an interest in such litigation or proceedings:

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 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 appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk.

H. To the entire federal government, to state, local, and tribal governments, and to appropriate private sector individuals within the Critical Infrastructure Key Resources

Community to provide situational awareness and establish a common operating picture and to ensure that critical disaster-related information reaches government decision makers when PII lends credibility to the report or facilitates coordination with interagency or international partners.

Disclosure to consumer reporting agencies:

None.

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

Storage:

DHS/OPS 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.

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, some personal information may be captured. Most information is stored as free text and any word, phrase, or number is searchable.

Safeguards:

DHS/OPS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. OPS 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.

Retention and disposal:

In accordance with NARA records schedule # N1-563-08-23, OPS maintains records for 5 years.

System Manager and address:

Director, Office of Operations Coordination and Planning, National Operations Center, U.S. Department of Homeland Security, Washington, D.C. 20528.

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 Chief Privacy Officer or OPS Freedom of Information Act Officer (FOIA), whose contact information can be found at http://www.dhs.gov/foia under "FOIA 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 FOIA Officer, Department of Homeland Security, 245 Murray Drive, S.W., 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 DHS Privacy Act regulations set forth in 6 C.F.R. Part 5, Subpart B. 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 (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:

Information contained in this system is obtained from publicly available social media websites.

Exemptions claimed for the system:

None.

Dated: May 13, 2015.

Karen L. Neuman,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2015-12692 Filed: 5/26/2015 08:45 am; Publication Date: 5/27/2015]