Publications and Data. The document is available to the public via *http://www.phe.gov/Preparedness/planning/science/Pages/AccessPlan.aspx.* The public comment period will end 30 days after posting in the **Federal Register**.

FOR FURTHER INFORMATION CONTACT: Please submit comments via email to Lorian Smith at *lorian.smith@hhs.gov.*

SUPPLEMENTARY INFORMATION: Pursuant to Section 103 of the America COMPETES Reauthorization Act of 2010 (Pub. L. 111–358), the Executive Office of the President, Office of Science and Technology Policy (OSTP) issued a memorandum on February 22, 2013 to the heads of federal agencies directing them to develop plans to enhance access to the results of federally-funded scientific research. ASPR is voluntarily developing a public access plan in order to maximize availability of digitally-formatted scientific data resulting from research supported wholly or in part by federal funding that will improve the public's ability to locate and access this data.

Background: This plan considers the interests and needs of various stakeholders, including, but not limited to, federally funded researchers, universities, libraries, publishers, data users and civil society groups.

Availability of Materials: The draft copy of the ASPR Public Access Plan will be posted on the phe.gov Web site: *http://www.phe.gov/Preparedness/planning/science/Documents/AccessPlan.pdf.*

Procedures for Providing Public Input: All comments must be received within 30 days of the publication of notice. Please submit comments to Lorian Smith via email *lorian.smith@hhs.gov.*

Dated: May 15, 2015.

Nicole Lurie,

Assistant Secretary for Preparedness and Response.

[FR Doc. 2015–12561 Filed 5–26–15; 8:45 am]

BILLING CODE 4150–28–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2015–0017]

Notice of Request for Public Comment Regarding Information Sharing and Analysis Organizations

AGENCY: Office of Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security.

ACTION: Request for Public Comment.

SUMMARY: This Notice announces a public comment period to allow input from the public on the formation of Information Sharing and Analysis Organizations (ISAOs) for cybersecurity information sharing, as directed by Executive Order 13691. DHS is soliciting public comments and questions from all citizens and organizations related to the provisions of E.O. 13691 ''Promoting Private Sector Cybersecurity Information Sharing'' of February 13, 2015. The purpose of this request for comment is to gather public input and considerations related to DHS' public engagements and implementation of E.O. 13691 including the selection of a ''standards organizations'' and approved activities of the selected standards organization.

DATES: The comment period will be held until July 10, 2015. *See* **SUPPLEMENTARY INFORMATION** *section for the address to submit written or electronic comments.*

Specific Comments Sought

Individuals and organizations providing comment to this DHS request are requested to address the following questions during this open comment period. However, all comments related to E.O. 13691 will be accepted. As such, submitted comments are not required to address the following five questions to receive due consideration by the Government. At the conclusion of this comment period a DHS will compile and address these comments to the extent practicable in a document which will be made broadly available and may result in further dialog via this forum or other means.

1. Describe the overarching goal and value proposition of Information Sharing and Analysis Organizations (ISAOs) for your organization.

2. Identify and describe any information protection policies that should be implemented by ISAOs to ensure that they maintain the trust of participating organizations.

3. Describe any capabilities that should be demonstrated by ISAOs, including capabilities related to receiving, analyzing, storing, and sharing information.

4. Describe any potential attributes of ISAOs that will constrain their capability to best serve the information sharing requirements of member organizations.

5. Identify and comment on proven methods and models that can be emulated to assist in promoting formation of ISAOs and how the ISAO ''standards'' body called for by E.O. 13691 can leverage such methods and models in developing its guidance.

6. How can the U.S. government best foster and encourage the organic development of ISAOs, and what should the U.S. government avoid when interacting with or supporting ISAOs?

7. Identify potential conflicts with existing laws, authorities that may inhibit organizations from participating in ISAOS and describe potential remedies to these conflicts.

8. Please identify other potential challenges and issues that you believe may affect the development and maturation of effective ISAOs.

SUPPLEMENTARY INFORMATION: Executive Order 13691 can be found at: *https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.*

Background and Purpose

On February 13, 2015, President Obama signed Executive Order 13691 intended to enable and facilitate ''private companies, nonprofit organizations, and executive departments and agencies . . . to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.'' The order addresses two concerns the private sector has raised:

- How can companies share information if they do not fit neatly into the sector-based structure of the existing Information Sharing and Analysis Centers (ISACs)?
- If a group of companies wants to start an information sharing organization, what model should they follow? What are the best practices for such an organization?

ISAOs may allow organizations to robustly participate in DHS information sharing programs even if they do not fit into an existing critical infrastructure sector, seek to collaborate with other companies in different ways (regionally, for example), or lack sufficient resources to share directly with the government. ISAOs may participate in existing DHS cybersecurity information sharing programs and contribute to near-real-time sharing of cyber threat indicators.

Submitting Written Comments

You may also submit written comments to the docket using any one of the following methods:

(1) *Federal eRulemaking Portal: http://www.regulations.gov.* Although comments are being submitted to the Federal eRulemaking Portal, this is a tool to provide transparency to the general public, not because this is a rulemaking action.

(2) *Email: ISAO@hq.dhs.gov.* Include the docket number in the subject line of the message.

(3) *Fax:* 703–235–4981, Attn: Michael A. Echols.

(4) *Mail:* Michael A. Echols, Director, JPMO–ISAO Coordinator, NPPD, Department of Homeland Security, 245 Murray Lane, Mail Stop 0615, Arlington VA 20598–0615.

To avoid duplication, please use only one of these four methods. All comments must either be submitted to the online docket on or before July 10, 2015, or reach the Docket Management Facility by that date.

Authority: 6 U.S.C. 131–134; 6 CFR. 29; E.O. 13691.

Dated: May 13, 2015.

Andy Ozment,

Assistant Secretary, Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. 2015–12691 Filed 5–26–15; 8:45 am]

BILLING CODE 9110–9P–P

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: Privacy Office, Department of Homeland Security.

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 June 26, 2015. This updated system will be effective June 26, 2015.

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, DC 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, DC 20528. For privacy questions, please contact: Karen L. Neuman, (202) 343–1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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 Web sites.

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 Web site at *http://www.dhs.gov/privacy*), the NOC monitors publicly available online forums, blogs, public Web sites, 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