BILLING CODE 9110-9P-P

DEPARTMENT OF HOMELAND SECURITY

Notice of Request for Public Comment regarding Information

Sharing and Analysis Organizations

[Docket No. DHS-2015-0017]

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 EO 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 EO 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 EO 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 EO 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