



**DEPARTMENT OF HOMELAND SECURITY**

[Docket No. DHS-2015-0017]

**Notice of Public Workshop regarding the Cybersecurity Information Sharing Act of 2015 Implementation**

**AGENCY:** National Protection and Programs Directorate, DHS.

**ACTION:** Notice of Public Workshop.

**SUMMARY:** The Department of Homeland Security (DHS) announces a public workshop on Thursday, June 9, 2016 to discuss information sharing as related to Title I of the Cybersecurity Act of 2015, the Cybersecurity Information Sharing Act.

**DATES:** The workshop will be held on Thursday, June 9, 2016, from 9:00 am to 4:00 pm EDT. The meeting may conclude before the allotted time if all matters for discussion have been addressed.

**ADDRESS:** The meeting location is the Navy League of the United States, 2300 Wilson Boulevard #200, Arlington, VA 22201. [See the Submitting Written Comments section for the address to submit written or electronic comments.](#)

**SUPPLEMENTARY INFORMATION:** Information about the Cybersecurity Information Sharing Act of 2015 and Automated Indicator Sharing can be found at: <https://www.dhs.gov/ais>.

**FOR FURTHER INFORMATION CONTACT:** If you have questions concerning the meeting, please contact [cisimplementation@HQ.DHS.GOV](mailto:cisimplementation@HQ.DHS.GOV) or Robert Hopkins, Director, External Affairs, Office of Cybersecurity and Communications, Department of Homeland Security, [Robert.Hopkins@hq.dhs.gov](mailto:Robert.Hopkins@hq.dhs.gov) or (703) 235-5788.

## **Background and Purpose**

On December 18, 2015, the President signed into law the Cybersecurity Act of 2015 as a part of the FY16 omnibus spending bill. Both Congress and the White House were active on the issue of cybersecurity during 2015, with multiple bills passed in each chamber. The resulting law included in the omnibus spending legislation reflects a reconciliation of the cybersecurity bills passed in the House and Senate in 2015.

Title I, the Cybersecurity Information Sharing Act (CISA), authorizes companies to voluntarily share cyber threat indicators and defensive measures with the Federal Government, State, Local, Tribal, and Territorial (SLTT) entities, and other private sector entities through a capability and process established by DHS. The law also:

- Provides liability protection to private sector entities for information shared in accordance with the law;
- Directs DHS to share private sector cyber threat indicators and defensive measures in an automated and real-time manner with Federal departments and agencies for cybersecurity purposes;
- Establishes measures to ensure that cybersecurity information received, retained, or shared by the DHS mechanism will not violate the privacy or civil liberties of individuals, under procedures jointly drafted by the Department of Justice and DHS;
- Protects shared information from public disclosure; and
- Sunsets the provisions for these information sharing measures in 10 years.

The CISA establishes an additional statutory basis for the Department's information sharing efforts with the Automated Indicator Sharing (AIS) initiative, which enables real-

time sharing of cyber threat indicators between DHS and stakeholders in the public and private sectors. The DHS real-time sharing process (and the web form and email processes) for cyber threat indicator and defensive measure sharing do not replace pre-existing cyber incident and cyber-crime reporting.

The purpose of the public workshop is to engage and educate stakeholders and the general public on CISA implementation and related issues such as:

- What is CISA?
- What is the Automated Indicator Sharing (AIS) initiative?
- What are the privacy concerns around CISA and how are privacy protections built into information sharing?
- What is the benefit of participating in an Information Sharing and Analysis Organization (ISAO) as it pertains to CISA?
- How does an organization (Federal or non-federal) connect and participate in AIS?

The event will consist of a combination of keynote addresses, presentations, and panel discussions, each of which will provide the opportunity for audience members to ask questions.

### **Information on Service for Individuals with Disabilities**

For information on facilities or services for individuals with disabilities or to request special assistance at the public meeting, contact [cisaimplementation@hq.dhs.gov](mailto:cisaimplementation@hq.dhs.gov) and write “Special Assistance” in the subject box or contact the meeting coordinator from the FOR FURTHER INFORMATION CONTACT section of this notice.

### **Meeting Details**

Members of the public may attend this workshop by RSVP only up to the seating capacity of the room. A valid government-issued photo identification (for example, a driver's license) will be required for entrance to the meeting space. Those who plan to attend should RSVP by emailing [cisainplementation@hq.dhs.gov](mailto:cisainplementation@hq.dhs.gov) 7 days prior to the meeting. Requests made after June 2, 2016 may not be able to be accommodated.

We encourage you to participate in this meeting by submitting comments to the CISA Implementation mailbox ([cisainplementation@hq.dhs.gov](mailto:cisainplementation@hq.dhs.gov)), commenting orally, or submitting written comments to the DHS personnel attending the meeting who are identified to receive them.

### **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:** [cisainplementation@hq.dhs.gov](mailto:cisainplementation@hq.dhs.gov). Include the docket number in the subject line of the message.

(4) **Mail:** Robert Hopkins, Director, External Affairs, Office of Cybersecurity and Communications, NPPD, Department of Homeland Security, 245 Murray Lane, Mail Stop 0615, Arlington VA 20598-0615.

To avoid duplication, please use only one of these three methods. All comments must either be submitted to the online docket on or before June 2, 2016, or reach the Docket Management Facility by that date.

**AUTHORITY:** Secs. 103 and 105, Pub. L. No. 114-113, Div. N, Title I.

Dated: **May 16, 2016**

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

[FR Doc. 2016-12018 Filed: 5/20/2016 8:45 am; Publication Date: 5/23/2016]