Information Sharing and Analysis Organizations (ISAOs)

America's cyber adversaries move with speed and stealth. To keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. However, many companies have found it challenging to develop effective information sharing organizations—or Information Sharing and Analysis Organizations (ISAOs). In response, President Obama issued the 2015 Executive Order 13691 directing the Department of Homeland Security (DHS) to encourage the development of ISAOs.

Overview

Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, directs DHS to:

- Develop a more efficient means for granting clearances to private sector individuals who are members of an ISAO via a designated critical infrastructure protection program;
- Engage in continuous, collaborative, and inclusive coordination with ISAOs via the DHS National Cybersecurity and Communications Integration Center (NCCIC), which coordinates cybersecurity information sharing and analysis amongst the Federal Government and private sector partners; and
- Select, through an open and competitive process, a non-governmental organization to serve as the ISAO Standards Organization. This ISAO Standards Organization

will identify a set of voluntary standards or guidelines for the creation and functioning of ISAOs.

ISAO Standards Organization

A Notice of Funding Opportunity (NOFO) for the ISAO Standards Organization Cooperative Agreement was posted online to Grants.gov on May 26, 2015. The application submission deadline was July 17, 2015. To locate the NOFO and application package, please visit www.grants.gov/web/grants/search-grants.html and search "97.128" in the CFDA Number search bar on the top left of the page. The Funding Opportunity Number is DHS-15-NPPD-128-001.

The Awardee for the ISAO Standards Organization Cooperative Agreement is the University of Texas at San Antonio (UTSA) with support from the Logistics Management Institute (LMI) and the retail Cyber Intelligence Sharing Center (R-CISC). As per the Executive Order, the UTSA team has been continuously working with, and will continue to work with, existing information sharing organizations, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs. Please visit the ISAO Standards Organization webpage for more information on the standards development process at www.ISAO.org.

Key Goals

Through public, open-ended engagements, the ISAO Standards Organization will develop transparent best practices that align with the needs of all industry groups, not just those traditionally represented by ISACs. Although formation and operations standards must still be developed via open-ended public engagement run by the Standards Organization, the ISAO standards are intended to be:

- **Voluntary-** participation in and the formation of ISAOs is not mandatory. Rather, it is meant to be completely optional and voluntary.
- **Transparent** – through a collaborative and transparent process, public and private sector entities will have the opportunity to provide input on the developing standards.
- **Inclusive –** participants from any sector, non-profit or for-profit, expert or novice, should be able to participate in or form their own ISAO.

- **Actionable –** participants will receive a useful and practical set of voluntary standards and best practices to utilize as a guide if they choose to participate in or form an ISAO.
- **Flexible –** any affinity of interest should be able to form ISAOs. Standards are not intended to be prescriptive as to prevent ISAO formation or harming the current processes of existing information sharing organizations.

Expanding the Current Model

Currently, most private sector information sharing is conducted through Information Sharing and Analysis Centers (ISACs). ISACs operate through a sector based model, meaning that organizations within a certain sector (i.e. financial services, energy, aviation, etc.) join together to share information about cyber threats. Although many of these groups are already essential drivers of effective cybersecurity collaboration, some organizations do not fit neatly within an established sector or have unique needs. Those organizations that cannot join an ISAC but have a need for cyber threat information could benefit from membership in an ISAO.

How Can I Comment and Provide Input to the Process?

DHS ***strongly encourages*** you and your organization to participate in the ISAO Voluntary Standards Development process. Since the ISAO Executive Order was signed on February 13, 2015, DHS has held several engagements to collaborate with and solicit the viewpoints of the public and key stakeholders. Although DHS may host additional future engagements, UTSA will be actively collaborating with the public during this period.

Stakeholders are strongly encouraged to contact the Standards Organization by emailing ISAO@LMI.org with comments, input, or general inquiries regarding the standards process. Providing your contact information to the Standards Organization immediately will ensure timely communication on updates and future events.

Please see the ISAO Engagements page and the ISAO Standards Organization Webpage for information regarding past meetings, engagement White Papers, published Federal Register Notices, public comments, future engagements, and other relevant material.

Read frequently asked questions about ISAOs and Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing. You may also contact the DHS ISAO inbox at ISAO@hq.dhs.gov with any further inquiries.

More DHS Information Sharing Efforts

EO 13691 compliments ongoing DHS information sharing efforts such as the Cyber Information Sharing and Collaboration Program (CISCP), DHS's flagship program for public-private information sharing. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities. Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners. Further, CISCP provides a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses.

The Enhanced Cybersecurity Services (ECS) program is a voluntary information sharing program that helps U.S.-based public and private entities defend their systems against unauthorized access, exploitation, or data exfiltration. ECS achieves this by sharing sensitive and classified cyber threat information with approved Commercial Service Providers (CSPs), thus enabling the CSPs to better protect their ECS customers.

Last Published Date: April 13, 2016