Why Do We Care About Information Sharing?
U.S. Federal Cybersecurity Operations Team
National Roles and Responsibilities*

**DOJ/FBI**
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

**DHS**
- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS’s jurisdiction

**DoD**
- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction

---

**INTELLIGENCE COMMUNITY:** Cyber Threat Intelligence & Attribution

**SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS**

**PROTECT** | **PREVENT** | **MITIGATE** | **RESPOND** | **RECOVER**

---

Coordinate with Public, Private, and International Partners

*Note: Nothing in this chart alters existing DOJ, DHS, and DoD roles, responsibilities, or authorities*
Partnership

• Partnerships enable all entities, whether public or private sectors, to engage in security programs, undertake research and development, and manage other resources more cost-effectively and efficiently within a collaborative multi-member environment.

• Establishing a common operational picture accessible to both public and private entities, by aggregating and analyzing information shared among trusted partners, also facilitates protective actions, mitigation efforts, and coordination necessary for efficient and effective response to cyber threats and incidents.
• **Information Sharing and Analysis Center (ISAC):** The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. **PRESIDENTIAL DECISION DIRECTIVE/NSC-63**

• Information sharing has been a core responsibility of DHS since its creation per the Homeland Security Act of 2002,
  
  • The Critical Infrastructure Information Act of 2002
  
  • Homeland Security Information Sharing Act.
Information Sharing

• Information sharing is essential to the protection of critical infrastructure and to furthering cybersecurity for the Nation.

• As the lead federal department for the protection of critical infrastructure and the furthering of cybersecurity, the Department of Homeland Security (DHS) has developed and implemented numerous information sharing programs.

• Through these programs, DHS develops partnerships and shares substantive information with the private sector, which owns and operates the majority of the Nation’s critical infrastructure.
National Infrastructure Protection Plan
HSPD-7
Helping Companies Join with Trusted Partners: Currently Through Sector-Based ISACs
Cyber Information Sharing and Collaboration Program (CISCP)

- Automated Indicator Sharing
- Indicator Bulletins
- Analysis Reports
- Priority Alerts
- Recommended Practices
Enhanced Cybersecurity Services (ECS)
Achieving Circulation
NCCIC Goal

“To maximize, to the fullest extent possible, the near-real-time dissemination of all relevant and actionable cyber threat indicators among the private sector and Federal Departments and Agencies for the purposes of network defense, and, within any statutory limitations, law enforcement purposes, while ensuring appropriate privacy and civil liberties protections.”

To do this, the NCCIC must be able to receive data from individual private sector and government entities; filter sensitive information; analyze the information; and disseminate cyber threat indicators for the purposes set forth in the legislation, and within the limitations set forth in the legislation.
• Receives incident reports from .gov and private partners (97,000 in 2014)

• Turns these reports into actionable alerts (12,000 in 2014)
NCCIC/US-CERT & ICS-CERT

• Information distributed via:
  • Alerts
  • Advisories
  • Bulletins
  • Technical Documents
  • US-CERT Portal
  • ICS-CERT Monitor
A key requirement of the legislation designating the NCCIC as the single civilian cybersecurity center for the private sector to share cyber threat indicators is the development and implementation of a near-real-time sharing capability, which provides robust protections to safeguard Personally Identifiable Information (PII), Protected Critical Infrastructure Information (PCII) and other sensitive data.
Information Sharing & Analysis Organizations
Through the ISAO E.O, called “Promoting Private Sector Cybersecurity Information Sharing” the President tasked the Department of Homeland Security (DHS) to build and manage a new ISAO model.

A new ISAO model is the next step in the information sharing maturity process.

- Enhance the Nations cyber defenses by adding a new layer of network defense, expands sharing relationships beyond traditional CIKR Sectors down into the fabric of America, and expands potential partnerships with private sector entities.

- Build upon the foundation established by Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.

The ISAO E.O. advances DHS’ efforts to assist private sector partners in building their cybersecurity capacity and resilience.
Executive Order Overview

• Under the E.O. the Secretary of Homeland Security (Secretary) is to strongly encourage the development of ISAOs.

• Directs ISAO implementation to be consistent with applicable laws and subject to the availability of appropriations.

• Secretary is to consult with Federal entities and appropriate regulators responsible for conducting cybersecurity related activities.
  – Amend sections of the National Industrial Security Program
  – Ensure appropriate privacy and civil liberties protections
  – Set parameters for the Standards Organization
  – Implementation based on existing laws and authorities

• **DHS Secretary is to enter into agreement with a non-governmental entity to serve as the ISAO Standards Organization (SO).**
Standards Organization (SO)

- University of Texas at San Antonio selected as the Standards Organization (SO) [www.isao.org](http://www.isao.org)
  - Support from the Logistics Management Institute (LMI) and the Retail – Cyber Intelligence Sharing Center (R-CISC)
- All inputs from DHS held engagements, Federal Register Notices, and workshop White Papers have been provided to the SO
- The SO will be expected to continue the engagements
  - Nov. 9 2015 SO held Initial Public Meeting
- Through these engagements, open public review and comment process, soliciting the viewpoints of existing entities engaged in cybersecurity information sharing, owners and operators of critical infrastructure, relevant Federal agencies, and other public and private sector stakeholders, the SO will **identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs**
WHY Enhance the ISAC Model

ISAC approach originally focused on CIKR sectors. This was a prudent first step and in line with risk management prioritization efforts at the time.

1. ISACs are Mainly Sector Based
2. Not all companies fit neatly into any sector
3. No Baseline Membership Standards across ISACs
4. Dependent on Industry for Sub-sector Outreach
5. Few ISAC options for “Less Cyber Capable Companies”

Which ISAC would the following fit into?

- HVAC Vendors
- Law Firms
- Mega Churches
- Electronic Crime Investigators
- National Assoc. Of MBAs, National Associations of Accountants
- Construction Companies
- Small businesses wanting to associate with each other / not sector based
- Bio-tech Laboratories

Notional ISAC Model

ISACs + ISAOs - Empowering Communities
Empowering Communities

From ~ 16 Sector-based entities with varying ideas of ISAC member qualification and requirements…… to

Game Changer

1000s of potential sharing entities (with unlimited numbers of members) built on baseline requirements for trusted sharing.
To support Government and Industry reduction of cyber risks, IACI promotes cyber resilience best practice, education, and information sharing guidance by assuring awareness of threats, and providing management and operations services to Information Sharing & Analysis Organizations (ISAOs) worldwide.

The International Association of Certified ISAOs (IACI), is a 501(c)6 non-profit organization headquartered at The Global Institute for Cybersecurity + Research, NASA/Kennedy Space Center, Florida.

www.certifiedisao.org
ISAO Best Practices
Deeper Questions

Many Questions to be answered. Public/Private activities underway to answer them........

- Should ISAOs be required to announce their ownership and funding structure?
- How prescriptive should Voluntary Standards be?
- What is the role of Government?
- Will ISAOs create too much noise?
- Might E.O. 13691 set the table for greater cybersecurity coordination and management?
Helping Companies Share Useful Information: STIX/TAXII
CISA: Removing Barriers

The Cybersecurity Information Sharing Act (CISA) was passed into law in December 2015.

Provides protections for organizations sharing information with DHS, removing some barriers to sharing that CISCP stakeholders have expressed in the past.

- Anti-Trust
- Liability
- FOIA
- Privacy
QUESTIONS

Michael Echols
International Association of Certified ISAOs
mechols@certifiedisao.org