# Information Sharing: CISA and Beyond

Erin B. Sheppard
Phillip R. Seckman

**April 27, 2017**

# Overview

- Cybersecurity Information Sharing Act ("CISA") of 2015
- CISA procedures and guidance
- CISA in action
- Recent trends and future developments

# Cybersecurity Information Sharing Act ("CISA") of 2015

# Background

- Signed into law on December 18, 2015
- Purposes:  CISA was enacted to:
  - Improve cybersecurity through information sharing, and
  - Remove potential legal impediments preventing private entities from monitoring and sharing information about cyber threats.
- Major provisions:
  - Federal agencies to develop procedures to facilitate information sharing among agencies and between agencies and private entities.
  - Private entities authorized to monitor their systems and share certain information with government and among themselves.
  - Private entities protected from any liability associated with monitoring and sharing, so long as conducted in accordance with the law.

PUBLIC CONTRACTING INSTITUTE

# Development of Procedures for Sharing Cyber Threat Information

- CISA provides that federal agencies will develop and issue procedures to promote sharing of information in the hands of the federal government:
  - Classified cyber threat indicators and defensive measures to be shared with non-governmental entities with appropriate clearances;
  - Sharing of information concerning cyber threat indicators, defensive measures, and cybersecurity threats that can be declassified or that is unclassified;
  - Information about cyber threats that can be shared in a timely fashion to prevent or mitigate the adverse effects of such threats; and
  - Cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government.
- CISA also required the Department of Homeland Security and Department of Justice to certify a process for private entities to share information with the government and issue guidance for private entities wishing to participate.

PUBLIC CONTRACTING INSTITUTE

# Authorization for Private Entities to Monitor, Operate Defensive Measures, and Share Information

CISA provides three authorizations to private entities:

1) Private entities are authorized to monitor their information systems (or the systems of others, with consent) for cybersecurity threats.
2) Private entities are authorized to operate defensive measures.
   - Includes any "action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."
   - Does not include measures that destroy or render unusable the information systems of anther entity.
3) Private entities are authorized to share information about cyber threats and defensive measures, both with the federal government and with other private entities.

PUBLIC CONTRACTING INSTITUTE

# CISA Limits and Protections on Sharing

- CISA includes limitations and precautionary measures to protect privacy of information that may reside on an information system.
- Private entities must:
  1) Remove personal information not related to a cyber threat prior to sharing.
  2) Limit use of information to cybersecurity purposes.
  3) Use DHS information sharing system as the vehicle to share threat information with the government.

Note: "Cybersecurity purpose" means for the purpose of protecting an information system or information from a “cybersecurity threat” or “security vulnerability,” as those terms are defined.

PUBLIC CONTRACTING INSTITUTE

# CISA Protections from Liability

- CISA provides that private entities are protected from liability for monitoring information systems and sharing cyber threat information.
- Monitoring and sharing must be done in accordance with CISA's provisions and limitations to enjoy protection from liability.
  - Note, this could be taken to mean that entities must use the information sharing process set up by the Department of Homeland Security, known as the Automated Indicator Sharing ("AIS") system.
  - However, DHS guidance indicates that it also accepts information via web submission and via email, and considers these methods of sharing as eligible for protection.
- Prior to CISA, private entities were concerned that liability under the Electronic Communications Privacy Act could be triggered by attempts to share cyber threat information.  CISA's liability protection addresses that problem.

PUBLIC CONTRACTING INSTITUTE

# CISA Procedures and Guidance

# Overview

- CISA required government agencies to issue several guidance documents and procedures to implement CISA. All of the following have been issued, and in some cases, already updated:
  - DHS and DOJ guidance to non-federal entities concerning the sharing of information with the government
  - Guidance issued by multiple agencies concerning information sharing by the federal government
  - Guidance for federal agencies concerning the receipt of shared threat information.
  - DHS and DOJ guidance on privacy protection.
- DHS and DOJ issued their initial guidance on February 16, 2016, as required, and issued updated guidance on June 15, 2016.
- All guidance available on the website of the U.S. Computer Emergency Readiness Team (US-CERT), at https://www.us-cert.gov/ais.

# Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under CISA

- As required by CISA, DHS and DOJ collaborated on guidance for private entities to share information with the government under CISA.
- Scope:
  1. Identifies types of information that would qualify as a cyber threat indicator under CISA and that would be unlikely to include information that should not be shared.
  2. Identifies types of information protected under otherwise applicable privacy laws and unlikely to be directly related to a cyber threat.
  3. Explains how to identify and share defensive measures.
- DHS and DOJ describe the type of information that can be shared, the methods and format in which it will be accepted by the government.
- DHS and DOJ also outline how non-federal entities can share information between themselves while enjoying protection under CISA.

PUBLIC CONTRACTING INSTITUTE

# Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under CISA

- The Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate federal entities collaborated to issue guidance describing the federal government's procedures for sharing information under CISA.
- The guidance document describes numerous processes and best practices already in place at various federal agencies.
  - Example: The Department of Homeland Security Enhanced Cybersecurity Services (ECS) Program is an existing, voluntary program for information sharing.
  - Example: The DHS Cyber Information Sharing and Collaboration Program (CISCP) is a program through which DHS shares information about threats with critical infrastructure partners.
- CISA guidance notes that the government already has processes in place to share threat information under E.O. 13,636. Those processes will be expanded to cover all non-federal entities under threat.

PUBLIC CONTRACTING INSTITUTE

# Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government

- Another set of procedures mandated by CISA and issued on June 15, 2016, establishes procedures relating to the receipt of cyber threat indicators and defensive measures by all federal entities under CISA.
- Describes use of DHS's AIS system for sharing and disseminating information in real time.
- Provides further guidance on accepted other than real time methods for sharing information, including through the internet and through email.

# Privacy and Civil Liberties Final Guidelines

- Interim guidance issued on February 15, 2016. Final guidance jointly issued by DHS and DOJ on June 15, 2016.
- Requires federal agencies to follow procedures designed to limit the effect on privacy and civil liberties of federal activities under CISA.
- Describes how federal agencies should implement CISA while effectuating principles consistent with privacy and civil liberties, including transparency, limits on use, and accountability.

# Status of DHS CISA Implementation: Real Time Data Sharing

- DHS's AIS system developed under CISA enables real-time information sharing.
- Statistics on CISA implementation:
  - 201 non-federal agencies have signed AIS terms of use.
  - 93 of these have fully completed technical requirements.
  - 12 are information sharing/analysis organizations like HITRUST or ISPs.
  - Other participants: 6 counties, state/local agencies, utilities, and 34 different federal agencies.
- DHS reports low false-positive rates and is focusing on the quality of information shared.
- DHS has also stated that sharing among federal agencies has dramatically increased.

# Status of DHS CISA Implementation: Review of Agency Systems

- DHS's Office of Inspector General ("OIG") has also completed a review of the agency's cybersecurity systems pursuant to Section 406 of CISA.
- The DHS OIG found that the agency had implemented many required controls, but it found some areas for improvement:
  - Not all DHS components used data exfiltration protection capabilities to support data loss prevention, forensics and visibility, and digital rights management.
  - DHS had not developed policies and procedures to ensure that contractors implement data protection solutions.
- DHS may respond to the OIG's report by requiring contractors to implement data loss prevention (DLP) or data rights management (DRM) solutions.

# Trends and New Developments

# Future Developments: The Trump Administration's Cybersecurity Policies

- Homeland Security Secretary John Kelly's speech on April 19, 2016, highlighted cybersecurity among many issues facing DHS:

  "Cyber threats present a tremendous danger to our American way of life. The consequences of these digital threats are no less significant than threats in the physical world. And so every day, we prepare to fight what many people can't even imagine."

- Secretary Kelly mentioned continuing partnerships with industry and creating a culture in which all businesses can defend themselves from cyber attacks.
- The headline quote from Secretary Kelly's speech: "no more muskets; our federal cybersecurity needs heavy artillery."

PUBLIC CONTRACTING INSTITUTE

# Future Developments: The Trump Administration's Cybersecurity Initiatives

- Prior to his inauguration, President Trump issued a statement addressing allegations of Russian hacking during the election season.
  - President Trump stated that he would "appoint a team to give me a plan within 90 days of taking office" to "aggressively combat and stop cyberattacks."
- Trump appointed former New York Mayor Rudy Giuliani to lead the cybersecurity task force.
  - However, no final actions or initiatives have been announced.
- President Trump has also created an initiative known as the White House Office of American Innovation, led by Jared Kushner.
  - This initiative is intended to focus on modernizing the technology and data infrastructure of federal departments and agencies.
- White House Office of Science and Technology Policy remains largely understaffed.

# Future Developments:  Executive Orders

- The Trump Administration has released a draft Executive Order for comment.
  - First issued in draft in early February.
  - The major provisions of the order call for review of policies, adversaries, and vulnerabilities.
- Trump is reportedly expected to sign the order this week.
  - Current reports suggest that he will leave out a section that concerned modernizing federal IT systems.
  - This goal will be addressed by the work of the Office of American Innovation.

# Future Developments: Information Sharing and Analysis Organizations

- Information Sharing and Analysis Organizations ("ISAOs")
  - Public or private entities created to gather information about and facilitate communication of cyber threats.
  - Development of ISAOs encouraged by E.O. 13,691 (Feb. 13, 2015), Promoting Private Sector Cybersecurity Information Sharing.
- The Information Sharing and Analysis Organization Standards Organization ("ISAO SO"), has issued a draft set of frequently asked questions for general counsels. The ISAO Q&A encourages corporate counsel to consider the benefits of information sharing and weigh risks on a case by case basis.
- The ISAO SO states that "several critical infrastructure sectors have dramatically improved their cybersecurity posture by creating and operating Information Sharing and Analysis Centers."
- Formation and use of ISAOs likely to continue.

# Future Developments: Increased Industry Involvement

- On April 13, 2017, Microsoft published a three-part series of policy papers outlining rules for nations and technology companies and proposing an international organization devoted to cybersecurity.
- Microsoft's proposed "Tech Accord" would involve an industry commitment to the following principles:
  1. No assistance for offensive cyber operations.
  2. Assistance to protect customers everywhere.
  3. Collaboration to bolster first-response efforts.
  4. Support for governments' response efforts.
  5. Coordination to address vulnerabilities.
  6. Fighting the proliferation of vulnerabilities.
- Even if never adopted, these Microsoft's proposals demonstrate industry belief in the need for collaboration and increasing industry involvement.

# Questions?

**Erin B. Sheppard**

**(202) 496-7533**

**erin.sheppard@dentons.com**

**Phillip R. Seckman**

**(303) 634-4338**

**phillip.seckman@dentons.com**