May 2016
Volume 11, Issue 5

Cybersecurity Information Sharing Act of 2015

ENTERPRISE INFORMATION SECURITY PROGRAM
Keeping our organization's data safe.

Enterprise Information Security Program

Tacoma

From the Desk of Ron Jimerson, Chief Information Security Officer

We've all heard talk of the Cybersecurity Information Sharing Act, but what does it really mean? We hope that this newsletter is a quick cheat sheet that highlight the key takeaways, as well as provide resources for additional information if you'd like to conduct a deeper dive into the topic.

The Basics

President Barack Obama signed the Cybersecurity Information Sharing Act of 2015 (CISA) into law on December 18, 2015, as Division N of the Consolidated Appropriations Act of 2016. While there are four cyber components to Division N, CISA arguable has some of the most far-reaching implications as it authorizes cybersecurity information sharing between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government.

*More information on the **Cybersecurity Information Sharing Act of 2015** is available at: https://www.congress.gov/bill/114th-congress/senate-bill/754.*

The term cyber threat information, as referenced in the Cybersecurity Information Sharing Act of 2015, is made up of the following:

- Cyber Threat Indicator – information that is necessary to describe or identify: malicious reconnaissance; a method of defeating a security control or exploitation of a security vulnerability; a security vulnerability; a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable to defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or any combination therof.
- Defensive Measure is defined as an action, devices, 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.

What does it mean?

CISA details how public and private entities share cyber information and establishes provisions for the information's protection, including the protection of personally identifiable information (PII). Specifically it:

- requires the federal government to release periodic best practices. Entities will then be able to use the best practices to further defend their cyber infrastructure.

- identifies the federal government's permitted uses of cyber threat indicators and defensive measures, while also restricting the information's disclosure, retention and use.
- authorizes entities to share cyber threat indicators and defensive measures with each other and with DHS, with liability protection.
- protects PII by requiring entities to remove identified PII from any information that is shared with the federal government. It requires that any federal agency that receives cyber information containing PII to protect the PII from unauthorized use or disclosure. The U.S. Attorney General and Secretary of the Department of Homeland Security will publish guidelines to assist in meeting this requirement.

Some Guidance

There were four documents that were delivered to congress that DHS has posted online. All of which were meant to provide some guidance while seeking compliance with CISA. These documents are available at https://www.us-cert.gov/ais and include:

- Guidance for sharing information by the federal government;
  https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf

- Guidance to businesses and other non-federal entities for sharing cyber threat indicators and defensive measures with the federal government;
  https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec 105%28a%29%29.pdf

- Interim operational procedures for sharing cyber threat indicators and defensive measures with the federal government;
  https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf

- Privacy and civil liberties interim guidance.
  https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec 105%28b%29%29.pdf

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™