SQUIRE PATTON BOGGS

DHS Releases Final Guidance on Sharing Cyber Threat Information

Final versions of the guidance, policies and procedures regarding the sharing of cyber threat indicators under the Cybersecurity Information Sharing Act of 2015 (CISA) were released June 15, 2016 by the US Department of Justice (DOJ) and the Department of Homeland Security (DHS). The four final guidance documents released by DHS and DOJ may be found here.

Background

In December 2015, President Obama signed CISA into law, in order to establish a voluntary cybersecurity information sharing process that encouraged public and private sector entities to share cyber threat indicators and defensive measures while protecting privacy and civil liberties. Cyber threat indicators are pieces of information, such as malicious IP addresses or the sender address of a phishing email (although, they can also be much more complicated). This information is to be shared by means of the DHS's free Automated Indicator Sharing (AIS) capability, which enables the exchange of data between the federal government and the private sector at machine speed.

AIS is a part of a DHS effort to create an ecosystem where, as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyberattacks. While AIS likely will not eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks. The goal is to commoditize cyber threat indicators through AIS so that tactical indicators are shared broadly between the public and private sector, enabling everyone to be better protected against cyberattacks.

Interim guidance was released in February 2016 and the final guidance further clarifies for federal agencies and the private sector how to share cyber threat data. The four final guidance documents consist of:

- **Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015** – This document (the Non-Federal Sharing Guidance) provides guidance on identifying the types of cyber threat indicators that should be shared and the types of information that should be excluded (primarily types of personally identifying information). Sharing conducted using the DHS AIS capability will receive liability protection under section 106(b) of CISA if the sharing is otherwise conducted in accordance with CISA. CISA also provides protections for sharing cyber threat indicators and defensive measures with any federal entity conducted pursuant to section 104(c) as follows:
  - A statutory exemption to federal antitrust laws for the sharing between and among private entities of cyber threat indicators, defensive measures, or assistance relating to the prevention, investigation or mitigation of a cybersecurity threat for a cybersecurity purpose.
  - Cyber threat indicators or defensive measures shared with the federal government under CISA are exempt from disclosure under federal state, tribal or local government freedom of information law, open government law, open meetings law, open records law, sunshine law or similar law requiring disclosure of information or records.
  - An exemption from certain regulatory uses: cyber threat indicators and defensive measures shared with the federal government under the Act shall not be used by any federal, state, tribal or local government to regulate, including through an enforcement action, the lawful activity of any non-federal entity or any activity taken by a non-federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure or sharing of a cyber threat indicator.
  - Sharing cyber threat indicators and defensive measures with the federal government does not constitute the waiver of any applicable privilege or protection provided by law; in particular, shared information does not surrender trade secret protection.
  - When so designated by the sharing entity, shared information shall be treated as commercial, financial and proprietary information.
  - The sharing of cyber threat indicators and defensive measures with the federal government under the Act shall not be subject to the rules of any federal agency or department or any judicial doctrine regarding *ex parte* communications with a decision-making official.
- **Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015** – This document (the Privacy and Civil Liberties Guidelines) establishes privacy and civil liberties guidelines governing the receipt, retention, use and dissemination of cyber threat indicators by a federal entity obtained in connection with the activities authorized by the CISA. Among other requirements, these guidelines call for federal agencies to identify and destroy any personal information of specific individuals or information that identifies specific individuals (Personally Identifying Data) that is received as part of any information received and to notify both the supplier of that information and any US person whose personal information is known or determined to have been shared in violation of CISA. The guidelines also mandate that information received can only be used for:

1. A cybersecurity purpose.
2. The purpose of identifying (i) a cybersecurity threat, including the source of such cybersecurity threat or (ii) a security vulnerability
3. The purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm or serious economic harm, including a terrorist act or a use of a weapon of mass destruction.
4. The purpose of responding to, investigating, prosecuting or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety.
5. The purpose of preventing, investigating, disrupting or prosecuting an offense arising out of a threat described in #3 above or any of certain enumerated offenses such as those relating to fraud and identity theft, espionage and censorship, and protection of trade secrets.

The guidelines also mandate that federal agencies establish a retention policy and ultimately destroy all information received in accordance with this retention policy.

- **Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015** – This document (the Federal Government Sharing Guidance) describes and governs the protocols, mechanisms and procedures by which federal agencies share cyber threat indicators and defensive measures both among such agencies and with private entities.
- **Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government** – This document (the Federal Operational Procedures) establishes procedures relating to the receipt of cyber threat indicators and defensive measures by all federal entities under CISA. It describes the processes for receiving, handling and disseminating information that is shared with DHS, including through operation of the DHS AIS system. It also states and interprets the statutory requirements for all federal entities that receive cyber threat indicators and defensive measures under CISA to share them with other appropriate federal entities.

Please contact us if you have questions about the new guidance, or would like to discuss how the guidance may have an impact on your business.

Contact

Robert B. Webb
Partner, Northern Virginia
T +1 703 720 7855
E robert.webb@squirepb.com