WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

DHS, DOJ Release Final Cyber Threat Information Sharing Guidelines Under CISA

June 24, 2016

AUTHORS

Daniel K. Alvarez | **Naomi Parnes**

Last week, the Department of Homeland Security ("DHS") and Department of Justice ("DOJ") released the Federal Government's final guidance regarding the sharing of cyber threat indicators and defensive measures between and among Federal and non-Federal entities under the Cybersecurity Information Sharing Act of 2015 ("CISA").[1] This effort is part of a broader cybersecurity strategy being implemented by the Obama Administration to incentivize information sharing about cybersecurity threats without undermining appropriate privacy and civil liberties protections. Specifically, the documents released last week by DOJ and DHS include:

- Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government;
- Privacy and Civil Liberties Final Guidelines; and
- Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities.

[1] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title I (2015).

This past February DHS and DOJ, in conjunction with the Office of the Director of National Intelligence and the Department of Defense, also published guidance for Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under CISA.

Even though these guidance documents are not rules and, as a result, do not carry the force of law, they do help to clarify three important issues for any entities that may be considering sharing relevant cybersecurity information with the Federal Government: (1) what information you can share; (2) with whom you can share it; and (3) what protections attach to the sharing. Being comfortable with the answers to these questions is critical to any entity's decision to share cybersecurity information.

Background: The Cybersecurity Information Sharing Act

CISA, enacted in December 2015 as part of the Consolidated Appropriations Act of 2016, is intended to facilitate and encourage increased sharing of certain cybersecurity information among the private sector; state, local, tribal, and territorial governments; and the Federal Government. To accomplish this purpose, CISA does two things:

(1) It directs DHS to create a voluntary cybersecurity information sharing process that encourages public and private entities to share information on cyber threat indicators and defensive measures while still protecting sensitive or classified information and privacy and civil liberties; and

(2) It provides certain statutory protections – including protections from disclosure under the Freedom of Information Act and, in some cases, protection against liability that might otherwise arise from sharing the information – for non-Federal entities that share with DHS, other companies, or their regulator, depending on the specific mechanism used for sharing.

What Information Can Be Shared

Section 104(c) of CISA allows non-Federal entities to share "cyber threat indicators" and "defensive measures" with any other Federal or non-Federal entity for a "cybersecurity purpose." However, in Section 104(d)(2), CISA requires those non-Federal entities to take steps to protect personal information.

Cyber Threat Indicators

CISA defines a cyber threat indicator as information that is **directly related to and necessary to identify or describe a cybersecurity threat**. The statute refers specifically to information necessary to describe or identify things like malicious reconnaissance, methods for defeating security controls, security vulnerabilities, malicious cyber command and control, actual or potential harm caused by an incident, and any other attributes of a cybersecurity threat.

Defensive Measures

CISA defines a defensive measure as an action, device, procedure, technique, or other measure applied to an information system or information stored on, processed by, or transiting an information system that **detects, prevents, or mitigates** a known or suspected cybersecurity threat or security vulnerability.

Cyber Threat Indicators and Defensive Measures Must Be Scrubbed of Personal Information

CISA requires a non-Federal entity to remove any information from a cyber threat indicator or defensive measure that it **knows at the time of sharing** to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat before sharing the indicator or defensive measure. Neither CISA, nor the guidance, defines personal information; however, each Federal agency will apply its own definition of personal information ("PI") and/or personally identifiable information ("PII").

As an example, the DHS/DOJ guidance explains that a company may share a phishing email as a cyber threat indicator. The personal information of the sender of the email could be included as part of the cyber threat indicator because it is directly related to the threat. However, because the name and email address of the target who received the phishing email is not directly related to or "necessary to identify or describe" the threat, that information must be scrubbed before it is shared with another entity.

The guidance further highlights that certain highly sensitive information is unlikely to be directly relevant to a cyber threat or defensive measure. Examples include: protected health information, including information covered under the Health Insurance Portability and Accountability Act; human resources information; consumer information or history; financial information that may be covered under the Gramm-Leach-Bliley Act; and identifying information of children under the age of 13 as covered by the Children Online Privacy Protection Act.

Entities With Whom to Share This Information

CISA authorizes non-Federal entities to share cyber threat indicators and defensive measures with both Federal and non-Federal entities for a cybersecurity purpose, and directs DHS to establish and certify a sharing mechanism for non-Federal entities to share with the Federal Government through DHS.

Sharing via DHS

There are several ways to share cyber threat indicator and defensive measure information directly with DHS:

1. Automated Indicator Sharing ("AIS") – The AIS initiative is an automated capability that receives, processes, and disseminates cyber threat indicators and defensive measures in real time after removing any PI/PII or other sensitive information not directly related to the cybersecurity threat. Non-Federal entities that participate in AIS will also **receive indicators and defensive measures** that other entities share with DHS through AIS.

2. Web form – Non-Federal entities may submit indicators and defensive measures through a DHS Web form. Submitters may remain anonymous from both the government and anyone the information is later shared with. However, the form is auto-filled to share the submitter's contact information and organization name with the U.S. Government.

3. Email – Non-federal entities may also email cyber threat indicator and defensive measure information directly to DHS.

Finally, a non-Federal entity may share information with DHS indirectly by first sharing the information with an Information Sharing and Analysis Center ("ISAC") or an Information Sharing and Analysis Organization ("ISAO") that then passes the information to DHS. However, the specific protections that attach to such indirect sharing will be a function of how the ISAC or ISAO shares with the Federal Government.

Sharing with Other Non-Federal and Federal Entities

Non-Federal entities may still share with other non-Federal entities, including private entities, and with Federal entities outside the DHS-certified mechanism. However, as discussed below, such sharing may not receive the full array of protections provided by CISA.

Statutory Protections for Sharing Under CISA

Among the most important components of CISA are the various protections provided for sharing of cyber threat indicators and defensive measures consistent with the statute.

Liability Protections

One of the most important aspects of CISA is that it grants entities liability protection for certain kinds of sharing. Specifically, CISA says that "[n]o cause of action shall lie" with respect to sharing of information via the DHS-certified sharing mechanism that is otherwise consistent with the statute (i.e., for a cybersecurity purpose, scrubbed of personal information).

Importantly, once an entity shares information through the DHS capability – at which point the liability protections attach – other Federal entities may then communicate with the non-Federal entity regarding that specific information without losing liability protection.

Other Protections that Attach to Sharing with the Federal Government

While liability protections generally attach only to sharing via the DHS-certified mechanism, CISA provides certain protections for sharing cyber threat indicators and defensive measures with any Federal entity for cybersecurity purposes that is otherwise consistent with the statute. Specifically, CISA provides the following protections:

- Exemption from Federal and state disclosure laws – indicators or defensive measures shared under CISA are exempt from disclosure under Federal, state, tribal, or local government freedom of information laws; open government laws; open meetings laws; open records laws; sunshine laws; or similar laws.
- Exemption from certain state and Federal regulatory uses – indicators and defensive measures may not be used in enforcement actions, but may inform the development or implementation of regulation.
- No waiver of privilege for shared material.
- Treatment of commercial, financial, and proprietary information – when so designated by the sharing entity, the information will be treated as such.
- Ex parte communications waiver – the sharing of a cyber threat indicator or defensive measure under CISA shall not be subject to the rules of any Federal agency or judicial doctrine regarding ex parte communication with a decision-making official.

Protections for Sharing with Private Entities

CISA ratifies the policy statement issued by DOJ's Antitrust Division and the Federal Trade Commission in May 2014, stating that private entities' sharing of cyber threat indicators and defensive measures for a cybersecurity purpose would **not violate antitrust laws**.

Conclusion

The final guidance provided by DHS and DOJ is helpful, but companies will still want to ensure that they are taking appropriate steps to ensure that the information being shared is consistent with CISA's requirements, and that the sharing is being done in a way that maximizes the protections provided for in the statute.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202 303 1125; dalvarez@willkie.com), Naomi Parnes (202 303 1225; nparnes@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

June 24, 2016