Clients&FriendsMemo

Potential Risks and Rewards of Cybersecurity Information Sharing Under CISA

With Final Guidance Companies are Better Positioned to Evaluate Whether to Participate in the Cybersecurity Information Sharing Program

July 21, 2016

When President Obama signed into law the Cybersecurity Act of 2015, which was designed to facilitate information sharing on cybersecurity threats between the public and private sectors, proponents hailed it as "our best chance yet to help address this economic and national security priority in a meaningful way."[1] Others – including some of the biggest players in the technology industry – decried it as "a thinly disguised surveillance provision," and something to be avoided pending further information on how it would be implemented. Interim guidance issued earlier this year by the Office of the Director of National Intelligence, the Department of Homeland Security, the Department of Defense, and the Department of Justice, lacked many of the details that industry insiders were waiting for.[2] Now, with final guidance having been issued (the "Final Guidance"), in-house counsel have more insight into the potential risks and rewards that await companies who opt to participate in the information sharing program, and can advise management and their boards of directors accordingly.[3]

---

1 *See generally* Ken Wainstein, Keith Gerver & Peter Carey, "President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing," (Dec. 24, 2015), http://www.cadwalader.com/resources/clients-friends-memos/president-obama-signs-cybersecurity-act-of-2015-to-encourage-cybersecurity-information-sharing (*quoting* Press Release, U.S. Chamber of Commerce, U.S. Chamber President Comments on Omnibus Spending Bill (Dec. 16, 2015), https://www.uschamber.com/press-release/us-chamber-president-comments-omnibus-spending-bill; Jenna McLaughlin, *Hasty, Fearful Passage of Cybersecurity Bill Recalls Patriot Act*, The Intercept (Dec. 19, 2015), https://theintercept.com/2015/12/19/hasty-fearful-passage-of-cybersecurity-bill-recalls-patriot-act/).

2 *See* Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015 (Feb. 16, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf.

3 On June 15, 2016, the Department of Homeland Security and the Department of Justice issued the Final Guidance intended to assist the private sector: 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 (https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf). Two related documents released the same day provide guidance to federal government entities: (1) Final Procedures Related to

I. CISA's Cybersecurity Information Sharing Program

Title I of the Cybersecurity Act of 2015, referred to as the Cybersecurity Information Sharing Act ("CISA"), created a framework to facilitate the sharing of information on cybersecurity threats between the federal government and the private sector. Under that framework, companies who are the victim of cyber-attacks (whether successful or unsuccessful) are encouraged to voluntarily report them to the Department of Homeland Security ("DHS"). In exchange, participants qualify to receive real-time alerts from federal, state, local and international intelligence and law enforcement agencies and other private sector companies who have been the targets of attacks, as well as information and best practices about defensive measures taken. So long as the sharing is made in accordance with CISA's requirements, participants qualify for protection against civil and other liability that may otherwise apply to the release of such information.

CISA, together with the Final Guidance, lays out the framework for private sector companies interested in sharing cybersecurity information.

A. Must Support a Cybersecurity Purpose. CISA only applies to information shared for a "cybersecurity purpose," meaning for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.[4] CISA does not pre-empt or substitute for any other legal, regulatory, or contractual obligations among parties, or between private sector companies and law enforcement. Sharing of information for any other reason is governed by other legal authorities.

B. Only Certain Categories of Information are Eligible. CISA provides for two categories of information that may be shared.

(1) Cyber Threat Indicators – The Final Guidance provides several examples of cyber threat indicators, including identifying information about the sender of a phishing email, internet protocol addresses associated with suspicious or malicious activity (*e.g.*, denial of service attacks, malicious reconnaissance efforts), methods by which security vulnerabilities are revealed (*e.g.*, by software publishers and security researchers), and types of files successfully exfiltrated in a computer intrusion. CISA defines "cyber

---

the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government (https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf); and (2) Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015 (https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec%20105%28b%29%29.pdf).

[4] "Cybersecurity threat" is broadly defined to include an action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system.

threat indicator" to include information that is necessary to describe or identify any of the following:

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of 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 the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control; or
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat.

(2) Defensive Measures – These include an action, device, procedure, signature, technique, or other measure that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. Examples from the Final Guidance include programs that are able to identify certain malicious activity, firewall rules that successfully block certain internet traffic, and techniques for screening incoming email traffic for suspicious content.

C. Personally Identifiable Information Must be Removed. Information shared pursuant to CISA must not include personal information of a specific individual or personally identifiable information ("PII") if that information is not directly related to a cybersecurity threat. This means that, prior to sharing information, participants must remove information that it knows at the time to be personal information of a specific individual, or information that identifies a specific individual, the sharing of which is not necessary to communicate the cybersecurity threat. While the Final Guidance does not define PII, it provides several exemplar categories including:

- Protected Health Information – This includes individually identifiable health information, including demographic information, that relates to an individual's physical or mental health or condition, the provision of health care, and the past, present, or future payment for health care (*e.g.*, medical records, lab reports, hospital bills).

- Human Resource Information – This includes information contained within an employee's personnel file, such as hiring decisions, performance reviews, and disciplinary actions.
- Consumer Information/History – This consists of information related to an individual's purchases, preferences, complaints and credit.
- Education History – This relates to an individual's education, such as transcripts, or training, such as professional certifications.
- Financial Information – This broad category includes bank statements, loan information, credit reports and other highly sensitive information related to banking, investment and insurance products and services.
- Information Regarding Property Ownership – This includes certain identifying information about property ownership that is protected by privacy laws and not otherwise publicly available.
- Information Regarding Minor Children – This includes certain identifying information of children under the age of 13.

D. Information Must be Shared via a DHS-Sanctioned Method. CISA protections will only apply to cybersecurity information shared pursuant to a DHS-sanctioned method, which currently includes:[5]

(1) Automated Indicator Sharing ("AIS") – The AIS initiative is designed to be the primary mechanism by which private sector companies will share information with DHS. Once a company enrolls and executes the AIS Terms of Use, it may submit cyber threat information using a specialized software program called a Trusted Automated eXchange of Indicator Information. There is no cost to sign up for AIS, and a sharer's identity may be withheld from other AIS participants if preferred. Companies that enroll in AIS will receive real-time information on cyber threat indicators and defensive measures provided by other entities that participate. The program is open to private sector participants as well as state, local, tribal and territorial governments, foreign governments and foreign private sector entities. Additional details about the AIS initiative are available at https://www.us-cert.gov/ais.

(2) Web Form Submissions – Participants may share information via a form on the DHS's National Cybersecurity and Communications Integration Center ("NCCIC") website. Additional information about NCCIC is available at https://www.us-cert.gov/nccic.

[5] The Final Guidance provides that information shared with DHS via other means, including certain systems established prior to the passage of CISA, may also qualify for liability and other protections.

(3) Email Submissions – Participants may share information with the NCCIC via email.

(4) Indirect Sharing – Companies may share information indirectly through Information Sharing and Analysis Centers ("ISACs") or Information Sharing and Analysis Organizations ("ISAOs"), which are private sector entities that then relay the information to DHS. However, the specific protections that apply will depend on whether the ISAC or ISAO complied with CISA's sharing requirements.

II. Benefits and Protections

The primary benefit for companies considering participation in CISA's cybersecurity information sharing program – and in particular those that enroll in the AIS initiative – is the real-time receipt of cyber threat information provided by other participants. The more companies that enroll and actively participate, the faster and more efficiently cybersecurity threats can be identified and successful defensive measures and best practices can be shared. In addition, private sector companies will benefit from the resources of federal, state, local, and international intelligence and law enforcement agencies who also participate. Proponents hope that as more government resources are dedicated to the program, it could develop a critical mass of participation and further improve the program's usefulness to all involved. Ideally, it will result in all data and systems being more secure and less prone to cyber-attacks.

Provided that information is shared in accordance with its framework, CISA provides protections against various liabilities that may otherwise attach to the release of information to law enforcement agencies and private sector companies. CISA provides targeted liability protection for participants, stating that "[n]o cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed" with respect to sharing of information with DHS. In addition, CISA provides additional statutory protections including:

- Antitrust Exemption – CISA provides a statutory exemption to federal antitrust laws for the sharing of cybersecurity information between and among private entities.
- Open Records Exception – Shared information is exempt from disclosure under the Freedom of Information Act, and other federal state, tribal, or local open government, open meetings, open records, and sunshine laws.
- Enforcement Limitation – Shared information cannot be used by any federal, state, tribal, or local government as the basis of a regulatory or enforcement action against the participant.
- No Privilege Waiver – Sharing information does not constitute the waiver of any applicable legal privilege or protection, nor does it surrender trade secret protections.

- Treatment of Commercial, Financial, and Proprietary Information – When so designated by the participant, shared information will be treated as commercial, financial, and proprietary information.
- *Ex Parte* Communications Waiver – Sharing information will 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 related to the Administrative Procedure Act.

III. Risks and Compliance Obligations

Companies considering participation in DHS's cybersecurity information sharing program must note that the liability and other statutory protections only apply if all the sharing requirements under CISA are complied with. For most participants, the most onerous requirement will be that of identifying and removing PII from any cybersecurity information prior to submission via the AIS program or other permitted methods. While some companies may be able to automatically tag PII for extraction prior to submission, for many it will no doubt require a manual effort. Inadvertent sharing of PII may result in the loss of liability and other protections under CISA, violations of federal, state and local privacy laws, and possibly the obligation to inform individuals that their information has been disclosed.

In addition, many of the protections provided by CISA are both untested and limited. For example, the liability and statutory protections apply only to U.S. litigants and regulators, so participants who share cybersecurity information with the DHS may wind up with litigation, regulatory, and enforcement exposure overseas. Despite the various protections, participants must still consider the risk that confidential business information and intellectual property shared through the program is improperly used by competitors and others. Companies may also need to address any contractual barriers to sharing confidential business information, as well as any disclosure obligations to investors, clients, or customers.

Companies should also note that while CISA provides protections against legal liability for properly sharing cyber-attack information with DHS, it does *not* protect against liability for a data breach itself. An issue to consider is whether reporting cyber threat indicators and defensive measures establishes knowledge of threats and, in the event of an actual breach, failure to address such risks could form the basis for civil liability. Companies should also consider whether cyber threat information shared with DHS rises to the level of a material risk that would trigger public disclosure requirements.

IV. Conclusion

As a threshold matter, companies must consider whether the benefit of receiving real-time notifications of cyber threat indicators and defensive measures outweighs the various risks and

burdens of CISA compliance. For some, participation with DHS in what may come to be viewed as an essential effort in the fight against cyber-attacks may bring a degree of goodwill that outweighs the potential liabilities. For others who view their cybersecurity program as a competitive advantage, they may determine that sharing defensive measures in particular has little benefit. In addition, early adoption may result in limited benefits until the program reaches critical mass in terms of private and public sector participation. Either way, with publication of the Final Guidance, companies can now make a more informed decision as to whether to participate in CISA's cybersecurity information sharing program.

* * * *

If you have any questions regarding the foregoing, please contact the authors below.

Joseph V. Moreno	+1 202 862 2262 +1 212 504 6262	joseph.moreno@cwt.com
Emily J. Rockwood	+1 202 862 2225	emily.rockwood@cwt.com
Peter Carey	+1 202 862 2339	peter.carey@cwt.com
Keith M. Gerver	+1 202 862 2381	keith.gerver@cwt.com