Client Alert | Financial Institutions / Sourcing & Technology Transactions / Data, Privacy & Cyber Security

CISA Guidance Clarifies How to Share Cyber Threat Information… but Issues Remain

April 2016

Authors: Kevin Petrasic, Trevor W. Nagel, Matthew Bornfreund

The Cybersecurity Information Sharing Act of 2015 ("CISA"), enacted on December 18, 2015, as part of the omnibus Consolidated Appropriations Act[1], 2016, creates a voluntary process that encourages public and private sector entities to share cyber information without the threat of litigation while simultaneously protecting privacy. Guidance recently issued by the Department of Homeland Security ("DHS") clarifies the types of information and the means for sharing to preserve liability protection under CISA. While the DHS guidance is instructive, a number of issues regarding CISA remain.

CISA requires DHS—along with the Director of National Intelligence, Secretary of Defense, and Attorney General, in consultation with the heads of the appropriate Federal entities—to develop and publish guidelines and procedures for sharing and receiving cyber threat indicators ("CTIs") and defensive measures ("DMs"). On February 16, 2016, DHS issued publications on federal agencies sharing information among themselves, handling the receipt of information, and protecting privacy and civil liberties.[2] DHS also issued Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under CISA ("Guidance"). The Guidance explains what constitutes CTIs and DMs, and clarifies how private companies can share CTIs and DMs in a way that receives liability protection under CISA, including under DHS's Automated Indicator Sharing ("AIS") initiative. On March 16, 2016, DHS issued an updated Privacy Impact Assessment regarding its AIS initiative under the Guidelines.[3]

Information Sharing Under CISA

The goal of CISA is to encourage cybersecurity information sharing to advance security. The sharing of cybersecurity information generally conflicts with corporate goals to protect intellectual property and avoid related legal risks. CISA is intended to overcome these obstacles and increase the sharing of information critical to enhancing cybersecurity protection.[4]

Related Practices

- Bank Regulatory
- Big Data Analytics
- Consumer Financial Services
- Cyber Currency
- Cyber Security
- Data Privacy & Protection
- EU & WTO
- Fintech
- Internet of Things
- Investment Advisory & Management
- Payments
- Security
- Technology Transactions

CISA creates a *voluntary* system of information sharing in which companies are authorized to share CTIs and DMs with federal and state governments, as well as with other companies and private entities. To encourage cybersecurity information sharing, CISA provides: (i) protection from liability for authorized cybersecurity information sharing; (ii) an antitrust exemption for sharing CTIs and DMs with competitors; (iii) protections from public disclosure laws; (iv) non-waiver of any privileges and protection of trade secrets; (v) protection of designated proprietary information; and (vi) protections against regulators using shared information in the supervision of, or in an enforcement action against, the sharing company. Whereas CISA protects companies in connection with the sharing of CTIs and DMs, it does not, however, shield companies from potential liability in the event of a data breach or cyber-attack.

There are four requirements for shared CTIs and DMs to receive full protection under CISA: (i) the information sharing must be for a cybersecurity purpose;[5] (ii) the information must fit the definition of a CTI or DM; (iii) the information should not include personal information of a specific individual or that identifies a specific individual ("PII"); and (iv) the information must be shared through means specified by DHS. Companies should keep a record of material decisions relating to any cyber information sharing exercise under CISA.

Cyber Threat Indicators

Pursuant to CISA § 102(6), a CTI is information that is necessary to describe or identify one of several threats, including malicious reconnaissance; efforts to defeat a security control or exploit a security vulnerability; anomalous activity indicating a security vulnerability, malicious cyber command and control; actual or potential harm from an incident; or any other aspect of a cybersecurity threat. To protect privacy, the Guidance emphasizes sharing only what is *necessary*.[6] The system implemented by DHS is designed to reduce the risk that a CTI contains PII. The Guidance provides examples of CTIs unlikely to include private information or PII, and thus may be shared.[7]

Defensive Measures

Under CISA § 102(7), a DM is defined as an action or measure applied to an information system or stored information that addresses a cybersecurity threat or vulnerability.[8] Generally, the DM definition is broadly construed,[9] but CISA *excludes* from this definition a measure that damages or destroys an information system or stored data not owned by the company applying the DM. As with CTIs, a DM should generally not include any PII.

Sharing CTIs and DMs

Prior to sharing CTIs or DMs, a company must assess whether such information contains PII not directly related to the cybersecurity threat. This review may be conducted manually or via technical processes. A significant issue is ensuring that this "scrubbing" procedure has been conducted satisfactorily prior to sharing a CTI or DM, particularly as potential liability could result from failing to do so. A related issue involves whether a privacy notice issued by a bank or other financial institution anticipates the possibility of information sharing that could include PII directly related to a cybersecurity threat. If not, then institutions should consider updating their privacy notices to avoid potential class action litigation or an enforcement action based on the inadequacy of the privacy notice disclosures.

Moreover, the manner in which information is shared affects the protections companies receive for sharing CTIs and DMs. DHS provides four means for information sharing with liability protection: (i) the AIS initiative; (ii) through the National Cybersecurity and Communications Integration Center website; (iii) via an email sent to DHS; or (iv) through an Information Sharing and Analysis Center or Information Sharing and Analysis Organization.[10] The AIS initiative is DHS's preferred method because it "enables the timely exchange of [CTIs] and [DMs] among the private sector, state, local, tribal, and territorial governments and the Federal government."[11] The fourth option listed above, however, authorizes the sharing of cybersecurity information directly between companies without the federal government acting as an intermediary.

CISA allows a company to communicate further about a previously shared CTI or DM without losing existing liability protection.[12] Post-sharing communication allows a company to provide additional descriptions or to assist in the development of appropriate DMs. In addition, a regulated company may also communicate with its Federal regulatory authority about CTIs and DMs without losing liability protection. DHS also clarifies that

CISA information sharing is not a substitute for required reporting to federal entities, such as reporting known or suspected cybercrimes directly to prudential regulators and law enforcement agencies.[13]

Other CISA Protections

An important additional protection for companies that share information under CISA is provided by the AIS initiative itself. The Guidance notes that "AIS will not provide the identity of the submitting entity to other AIS participants unless the submitter consents to share its identity as the source of the [CTI] submission."[14] DHS's updated Privacy Impact Assessment on the AIS is more explicit, noting "DHS will only reveal the identity of the [CTI] submitter as long as the AIS participant has provided consent to do so."[15]

If properly submitted, companies are protected from a court action for sharing or receiving CTIs or DMs.[16] Unclear is exactly how a company protects itself from such a court action, which could, in itself, remain a disincentive to information sharing. Another more fundamental disincentive may be the reluctance of certain companies to share any information relating to cybersecurity, particularly with the federal government. Exacerbating this reluctance is a continuing perception that information sharing with the federal government under CISA may not be a reciprocal exercise. Of particular concern is that privately shared information may be collected and analyzed by the government for purposes not solely related to assessing cybersecurity risks. This concern is heightened to the extent personal information is included out of necessity in such collected information. Interestingly, DHS's Privacy Impact Assessment underscores this concern, noting "there remains a residual privacy risk that [PII removal] processes may not always identify and remove unrelated PII, thereby disseminating more PII than is directly related to the cybersecurity threat."[17]

Limits on Hacking Back

Beyond the CISA definition, the Guidance provides only a few details about the potential scope of DMs. Because CISA restricts a DM that would adversely impact or access an information system or stored information, it appears to foreclose DMs that neutralize a cybersecurity threat at its source, or more colloquially, hacking back. The Guidance emphasizes that companies developing DMs should ensure that they do not unlawfully access or damage information systems or data.[18] Specifically, CISA does not permit "unauthorized access to or execution of computer code on another entity's information systems or other actions that would substantially harm another entity's information systems."[19] As hacking back techniques become more sophisticated, the distinction between what is permitted and not permitted under the Guidance may become problematic. Does this prohibition against unauthorized access to another's information systems prevent the use of "tracer" technologies? In the digital world, the "boundary" of any information system is not always as clear as the term colloquially implies.

Furthermore, it is questionable whether hacking back an entity that exists solely for the purpose of launching cyber-attacks would be excluded as a permissible DM. Essential to this determination is the definition of "information system." CISA defines information system by reference to section 3502(8) of the Federal Information Policy,[20] which provides that an information system is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[21] It is arguable that computers and systems assembled for the sole purpose of stealing or destroying information do not meet this "information system" definition. If a company chooses to deploy a DM that accesses a malicious system, such action may be permissible where the target system is not used for *any* legitimate purpose that would bring it under this definition of information system. Thus, the ability to exercise aggressive counter measures as protected DMs may require further clarification.

How, Where and When Will CISA Be Used

CISA protections assume and require a legitimate "cybersecurity purpose." For protected information sharing purposes, an uncertain but critical issue is: what is, and how broadly to construe, a valid cybersecurity purpose. While the Guidance defines the term,[22] the scope and coverage of the term remain ambiguous.

The protections enumerated by CISA and explained in the Guidance indicate that Congress understands the reluctance and concerns that many companies may have in sharing CTIs and DMs. Protection from liability and the exemption from antitrust laws will alleviate some arguments against information sharing. In addition, the anonymization of the submitter when using the AIS initiative helps mitigate concerns that sharing

information could lead to subsequent regulatory scrutiny. Some companies, however, may believe that a more detailed submission relating to CTIs and DMs may provide sufficient clues for a skilled operative to reasonably guess the likely identity of the submitting party, or at least to limit that identity to a short list of prospects. Furthermore, some companies consider that the release of any information relating to CTIs and DMs may provide skilled operatives with insights as to how certain cybersecurity protections work or perceived vulnerabilities.

There remain, however, a number of reasons why companies may choose not to share information under CISA. First, companies may view their own cybersecurity competence and dexterity as a competitive advantage. If a company views hackers and cyber threats as merely part of the competitive market environment, it may see little or no benefit in helping its competitors prepare for and survive a cyber-attack. Second, CISA and its protections only apply in the US. Given that many companies are global in operation and cyber threats are inherently global in nature, many companies fear that cyber information shared in the US may fall into the hands of individuals outside the US and even inform legal actions in other jurisdictions. For example, competition authorities in EU jurisdictions may adopt a different perspective on large technology companies sharing cyber information, particularly with respect to absolute restraints that may be imposed on any use of PII.

Although CISA specifically prevents regulators from using shared CTIs or DMs as the basis for future enforcement actions, companies may still fear potential consequences. A regulated entity that identifies numerous CTIs and effective DMs may create an expectation that it will be able to prevent or effectively remediate a particular attack throughout its enterprise systems. If there is a subsequent breach of the company, the concern is whether the shared information could be used by the regulator, not as the basis for a regulatory action, but as evidence that the company should have known how to prevent the attack.

Similarly, while failure to effectively deploy a DM may not provide a basis for regulatory action, it is unclear to what extent a company that fails to implement or execute a DM would be shielded from private litigation, including a consumer class action. A particular concern is whether the company has provided a roadmap regarding its knowledge of one or more CTIs, as well as the appropriate DMs, but then failed to act appropriately based on such information to protect its customers.

Only time will tell whether CISA and DHS have sufficiently reduced companies' concerns to encourage greater information sharing. In the meantime, DHS and other Federal law enforcement and regulatory agencies will be working to facilitate an effective, healthy, and robust cybersecurity information sharing environment. An important consideration both for industry participants and law enforcement and regulatory agencies is the need for a continuing dialogue regarding CISA and the Guidance itself, as well as the actual sharing and reporting of CTIs and DMs. For example, the Guidance is not clear regarding the standard of care for scrubbing data to remove unrelated PII. For the AIS initiative, while DHS expresses the view that AIS participants should use "reasonable efforts" in applying versioning updates of AIS protocols to avoid sharing PII,[23] there is not a clearly articulated standard for how information should be scrubbed at the outset. Further complicating the picture is that the efficacy of any standard to protect PII may be difficult to gauge in this emerging and fast changing area of the law.

The decision for a company to participate in cybersecurity information sharing under CISA is not a decision to be taken lightly. Companies should prudently assess the benefits and risks associated with participating in this sharing process. For many companies, particularly those who consider that they have sophisticated and effective cyber security systems, this may be a case-by-case analysis highly contingent upon the circumstances of the perceived threat at a particular point in time. Although most large technology companies may be reluctant ever to agree to participate in CISA as part of the general terms and conditions collected at the end of technology transaction documents, many may require their vendors and suppliers to provide information regarding CTIs and DMs via an industry information sharing analysis center. While a step forward, it may ultimately result in an asymmetrical rather than a "sharing" information exchange

[1] Consolidated Appropriations Act, 2016, Pub. L. 114-113 (2015). As of April 8, 2016, the Government Printing Office has not published the public law version. For textual references, *see* H.R. 2029 – Consolidated Appropriations Act, 2016, *available at*, https://www.congress.gov/bill/114th-congress/house-bill/2029/text.

[2] Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015, *available at* https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf; Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government, *available at* https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf; and Privacy and Civil Liberties Interim Guidelines: Cybersecurity Information Sharing Act of 2015, *available at* https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec%20105%28b%29%29.pdf.

[3] Privacy Impact Assessment for the Automated Indicator Sharing (AIS) Update ("Privacy Impact Assessment"), U.S. Department of Homeland Security, DHS/NPPD/PIA-029(a), March 16, 2016, *available at* https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_ais_update_03162016.pdf.

[4] Joint Explanatory Statement to Accompany the Cybersecurity Act Of 2015, issued by the Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence, Senate Committee on Homeland Security and Governmental Affairs, and House Committee on Homeland Security, p. 1 (2015), *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/JES%20for%20Cybersecurity%20Act%20of%202015.pdf.

[5] "Cybersecurity purpose" means protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. CISA § 102(4).

[6] "Effectively, the only information that can be shared under [CISA] is information that is directly related to and necessary to identify or describe a cybersecurity threat. Information is not directly related to a cybersecurity threat if it is not necessary to assist others detect, prevent, or mitigate the cybersecurity threat." Guidance, p. 5.

[7] Examples include:

A company could report that its web server log files show that a particular IP address has sent web traffic that appears to be testing whether the company's content management system has a particular vulnerability.

A security researcher could report the discovery of a technique that permits unauthorized access to an industrial control system.

A software publisher could report a vulnerability it has discovered in its software.

A manufacturer could report unexecuted malware found on its network.

[8] CISA § 102(7).

[9] DMs "will generally consist principally of technical information that can be used to detect and counter a cybersecurity threat." Guidance, p. 6.

[10] CISA § 106(b)(1).

[11] Guidance, p. 12.

[12] CISA § 105(c)(1)(B).

[13] Guidance, p. 10.

[14] Guidance, p. 12. See also, https://www.us-cert.gov/ais (stating that the initiative "Anonymizes the identity of the submitter of the information, unless the submitter has consented to sharing its identity").

[15] Privacy Impact Assessment p. 8.

[16] CISA § 106(b).

[17] Privacy Impact Assessment, p. 13.

[18] Guidance, p. 6, n. 8.

[19] *Id*.

[20] CISA § 102(9).

[21] 12 U.S.C. 3502(8).

[22] *See* note 4.

[23] Privacy Impact Assessment, p. 14.