

Harvard Law School Forum on Corporate Governance

Federal Guidance on the Cybersecurity Information Sharing Act of 2015

Posted by Brad S. Karp, Paul, Weiss, Rifkind, Wharton & Garrison LLP, on Thursday, March 3, 2016

Tags: [CISA](#), [Compliance and disclosure interpretation](#), [Cybersecurity](#), [Director liability](#), [Disclosure](#), [DOJ](#), [Fiduciary duties](#), [Liability standards](#), [Privacy](#), [Risk](#), [Risk management](#), [Securities regulation](#)

More from: [Brad Karp](#), [Paul Weiss](#)

Editor's Note: [Brad S. Karp](#) is chairman and partner at Paul, Weiss, Rifkind, Wharton & Garrison LLP. This post is based on a Paul Weiss client memorandum.

The Cybersecurity Information Sharing Act of 2015 (“CISA”) was signed into law on December 18, 2015. The law has two main components. First, it authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats. Second, CISA provides certain protections to encourage companies voluntarily to share information—specifically, information about “cyber threat indicators” and “defensive measures”—with the federal government, state and local governments, and other companies and private entities. These protections include protections from liability, non-waiver of privilege, and protections from FOIA disclosure, although, importantly, some of these protections apply only when sharing with certain entities. To qualify for these protections, the information sharing must comply with CISA’s requirements, including regarding the removal of personal information.

On February 16, 2016, the Department of Homeland Security and the Department of Justice issued guidance to assist companies that share information under CISA with the federal government (the “Guidance”). [1] Additional guidance issued the same day addressed how federal agencies would protect the information they receive and how they would share that information with each other, state and local governments, and the private sector.

This post describes the key provisions of CISA and the Guidance with the aim of providing general counsels with a practical understanding of how companies can avail themselves of the law’s protections. We also identify some of the law’s key limitations and potential ambiguities, and we discuss the benefits and risks involved in a company’s decision to increase its voluntary cyber information sharing.

Key Provisions of CISA

Part of the December 2015 omnibus legislation (Pub. L. No. 114-113), CISA had support within both parties in Congress and from the Administration, but was opposed by privacy groups and some technology companies. [2] In authorizing companies to implement monitoring and defensive mechanisms on their information systems, the legislation responded to fears that certain such activities could result in liability, including under the Electronic Communications Privacy Act. The protections to encourage companies [3] to share information were meant to address concerns that sharing information with the government or other parties could risk litigation for violating privacy and antitrust laws, among others, as well as risk disclosure under FOIA and the waiver of privilege. The following is a non-exhaustive summary of CISA’s key provisions.

- **Monitor and Defend Information Systems.** Subject to certain requirements, a company is authorized, notwithstanding any other provision of law, to “monitor” and “operate defensive measures” on its own information

system—or, with written authorization, another party’s system—for cybersecurity purposes. Section 104(a)(1)(A)-(C), (b)(1)(A)-(C).

- **Protection from Liability for Monitoring.** CISA provides that “no cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed,” for “monitoring” conducted in accordance with CISA. Section 106(a). Note that there is no similar liability protection for operating defensive measures that go beyond monitoring.
- **Share or Receive Cyber Threat Indicators or Defensive Measures.** Subject to certain requirements, a company is authorized, notwithstanding any provision of law, to share with, or receive from, the federal government, state and local governments, and other companies and private entities “cyber threat indicators” and “defensive measures” for a “cybersecurity purpose.” Section 104(c)(1).
 - A “cyber threat indicator” means information that is “necessary to describe or identify” a variety of listed threats, including “malicious reconnaissance” and methods of exploiting a security vulnerability or causing a legitimate user to unwittingly enable such exploitation. Also included is information on the “actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat.” Section 102(6).
 - A “defensive measure” is something applied to an information system (or to information on that system) that “detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability,” but measures that destroy, render unusable, provide unauthorized access to, or substantially harm third-party information systems are expressly excluded from the definition. Section 102(7).
 - A “cybersecurity purpose” means the purpose of protecting an information system or information from a “cybersecurity threat” or “security vulnerability,” as those terms are defined in the statute. Section 102(4).
- **Scrub Personal Information Before Sharing.** A company intending to share a cyber threat indicator must remove—or implement a “technical capacity” configured to remove—any information “not directly related to a cybersecurity threat” that the company “knows” at the time of sharing to be “personal information of a specific individual or information that identifies a specific individual.” Section 104(d)(2)(A), (B).
- **Protections for Sharing and Receiving Information (As Applicable).** To qualify for protections, information sharing must be done in accordance with CISA’s requirements, including the requirement regarding removal of personal information.
 - **Protection from Liability.** CISA provides 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” for the sharing or receipt of a cyber threat indicator or defensive measure conducted in accordance with this title, subject to the proviso below. Section 106(b)(1).
 - **However, Federal Sharing Must Use DHS Process to Obtain Liability Protection.** With respect to sharing with the federal government, this liability protection generally applies only when the information is shared through the DHS process prescribed by CISA, though there is an exception that covers “communications by a regulated non-Federal entity with such entity’s Federal regulatory authority regarding a cybersecurity threat.” Section 105(c)(1)(B)(ii).**[4]** Within 90 days of enactment, DHS is required to establish and certify a process for receiving information shared by companies and disseminating it in an automated manner to several other federal agencies. Section 105(c)(1)(A)-(C).
 - **Antitrust Exemption.** CISA provides that it is not a federal or state antitrust violation for companies to share cyber threat indicators or defensive measures in order to prevent, investigate, or mitigate threats. Section 104(e)(1), (2); see also Section 108(e). **[5]**
 - **Non-Waiver of Privilege.** Sharing information with the federal government does not waive privileges and other legal protections, including trade secret protection. Section 105(d)(1). There is no analogous provision for sharing with state and local governments or other companies.
 - **Proprietary Information.** The federal government will consider cyber threat indicators and defensive measures shared with it to be the sharing entity’s commercial, financial, and proprietary information when so

designated by that entity. Section 105(d)(2).

- **Exemption from Federal and State FOIA Laws.** Information shared under CISA is exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552), as well as under any State or local provisions “requiring disclosure of information or records.” Section 105(d)(3).
- **Information Cannot Be Used to Regulate or Take Enforcement Actions Against Lawful Activities.** Information shared under CISA “shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities related to monitoring, operating defensive measures, or sharing cyber threat indicators.” The information may be used, however, to develop or implement new cybersecurity regulations. Section 105(d)(5)(D)(i), (ii).

- **Other Requirements and Provisions**

- **Restrictions on Sharing and Use.** When a company receives a threat indicator or defensive measure from another party, it must comply with any lawful restrictions the sharing entity imposes on sharing or using that information. Section 104(c)(2).
- **Security Control.** Companies that monitor and defend their information systems, or share or receive information, under CISA must implement a “security control” (a defined term) to protect threat indicators and defensive measures from unauthorized access or acquisition. Section 104(d)(1); Section 102(16).
- **Voluntary Participation.** CISA creates no duty to share information, nor does it create a duty to warn or act based on information received. Section 106(c)(1)(A), (B); Section 108(i). The federal government also may not condition the sharing of cyber threat indicators with a company on such company’s sharing of information with the federal government or another party. Section 108(h)(2).
- **Preservation of Contracts.** CISA provides that nothing in the law shall be construed to supersede any current or future contractual agreement or terms of service agreement or to abrogate trade secret or intellectual property rights. Section 108(g).
- **Uses of Information by Federal Government.** Cyber threat indicators and defensive measures shared with the federal government may be used by the federal government solely for a “cybersecurity purpose” or in enumerated circumstances, such as responding to or preventing a specific threat of bodily harm or a specific threat of serious economic harm. Section 105(d)(5)(A).
- **Sunset.** Subject to exceptions, CISA will sunset on September 30, 2025. Section 111.

Federal Guidance for the Private Sector

As required by CISA section 105(a)(4), on February 16, 2016, DHS and DOJ issued the Guidance to assist the private sector in better understanding what information may be shared with the federal government, what information may not be shared, and what procedures are available for sharing information. [6] The Guidance also suggests some additional safeguards and procedures that are not required by CISA. While the Guidance is focused on information sharing with the federal government, its discussion of what information may and may not be shared appears applicable to sharing with non-federal entities as well.

- **Information That May Be Shared Under CISA.** The Guidance states that, “[e]ffectively, the only information that can be shared under the Act is information that is directly related to and necessary to identify or describe a cybersecurity threat.” Guidance at 5.
 - **Examples of Cyber Threat Indicators.** The Guidance, using some caveat language, provides several examples of information that meets these standards and can thus be shared under CISA, including (see Guidance at 5-6):
 - For a phishing email, personal information about the sender, a malicious URL in the email, malware files attached to the email, the content of the email, and additional email information related to the malicious email or potential cybersecurity threat actor, such as subject line, message ID, and X-

Mailer, “could be considered directly related to a cybersecurity threat.” However, the name and email address of the targets of the email would be “personal information not directly related to a cybersecurity threat and therefore should not typically be included as part of the cyber threat indicators.”

- A security researcher could report on 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.
 - An engineering company that suffers a computer intrusion could describe the types of engineering files that appear to have been exfiltrated, as a way of warning others companies with similar assets.
 - A company suffering a distributed denial of service attack could report the IP addresses that are sending malicious traffic.
- **Examples of Defensive Measures.** The Guidance also provides examples of defensive measures that a company could share, including (see Guidance at 7):
 - A computer program that identifies a pattern of malicious activity in web traffic flowing into an organization.
 - A signature that could be loaded into a company’s intrusion detection system in order to detect a spear phishing campaign with particular characteristics.
 - A technique for automatically matching the content of email traffic against a set of content known to be associated with a specific cybersecurity threat.
- **Information That May Not Be Shared Under CISA.** CISA provides that a company must remove any information from a cyber threat indicator 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. Section 104(d)(2). The Guidance states that 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 at 5.
 - **Procedures for Removing Personal Information.** A company may conduct its review for such personal information using either a manual or a technical process. Guidance at 11; Section 104(d)(2)(A), (B). Additionally, the Guidance suggests that companies use “standardized fields in structured formats” as a means of limiting information to CISA’s requirements and avoiding the sharing of personal or otherwise inappropriate information. Guidance at 6.
 - **Review of Defensive Measures.** CISA does not explicitly require companies to review and remove such personal information from “defensive measures,” but the Guidance encourages companies to do so, and, importantly, takes the position that a defensive measure may itself contain a cyber threat indicator that is subject to CISA’s review and removal requirements. Guidance at 10.
 - **Examples of Personal Information That Likely Must Be Removed.** Notably, while CISA calls on DHS and DOJ to provide examples of types of information protected by “otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat,” section 105(a)(4)(B)(ii), CISA’s requirements concerning the removal of personal information do not reference, and thus do not appear limited to, information covered by privacy laws. The Guidance provides the following examples of information or types of information that likely must be removed (see Guidance at 5-9):
 - “Protected Health Information” such as an individual’s past, present, or future physical or mental health condition.
 - “Human Resources Information” such as performance reviews and disciplinary actions.
 - “Consumer Information/History” such as an individual’s purchases, preferences, complaints, or credit.
 - “Financial Information” such as bank statements, loan information, and credit reports.
 - As noted above, the name and email of a target of a phishing email “typically” must be removed.

- The Guidance notes as an example that a phishing attack could use “social engineering” that focuses on the target’s health condition, but states that sharing such information in a form that constitutes personal information of a specific individual “may not be necessary,” and instead suggests sharing an anonymized characterization of the cyber threat.
- **In Sharing with the Federal Government, Liability Protection Generally Applies Only to Sharing Through the DHS Process.** The Guidance acknowledges that the “manner in which information is shared affects the protections private entities receive.” Guidance at 10. Importantly, in sharing information with the federal government, the only way to receive the liability protection of section 106 is to share information through the “DHS capability and process” created under section 105(c), or through the exceptions covering follow-up communications and “communications by a regulated non-Federal entity with such entity’s Federal regulatory authority regarding a cybersecurity threat.” Section 105(c)(1)(B)(i), (ii). Otherwise sharing with other federal agencies does not trigger the liability protections of section 106, although it does trigger the other protections, such as non-waiver of privilege and non-disclosure under FOIA, assuming of course that the other requirements of CISA are satisfied. Guidance at 10, 13.
 - **Options for Using the DHS Process.** The Guidance contains information on the options for submitting information using the DHS process created under section 105(c), including through the Automated Indicator Sharing (AIS) system, through a web form on the DHS National Cybersecurity and Communications Integration Center website, and by sending an email to DHS. Guidance at 12.
 - **Guidance Warns That DHS Process is Not a Substitute for Other Federal Reporting.** While obtaining liability protection appears to be a seemingly strong reason to only share information with the federal government through the DHS process, the Guidance warns that sharing conducted through this process “should not be construed to satisfy any statutory, regulatory, or contractual obligation. It’s not a substitute for reporting other types of information to federal entities, such as known or suspected cybercrimes directly to appropriate law enforcement agencies, known or suspected cyber incidents directly to the National Cybersecurity and Communications Integration Center, or required reporting to regulatory entities. The sharing addressed in this guidance is intended to complement, not replace, the prompt reporting of criminal activity, cyber incidents, or reportable events to the appropriate authorities.” Guidance at 10.
- **Liability Protection Applies to Sharing with ISACs and ISAOs.** The Guidance notes that companies may share information under CISA with Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs), [7] which will in turn share information with federal agencies through DHS. Such sharing with an ISAC or ISAO brings with it the liability protections provided under section 106 because they are non-federal entities. Guidance at 13.

Implications and Recommendations

For many companies, sharing cybersecurity information with public and private partners should be part of a comprehensive cybersecurity program. By sharing, companies broaden the pool of information that the government and other companies can use to defend against attacks, which redounds to everyone’s benefit. Although CISA likely does not fundamentally change the cybersecurity landscape, it does tip the scale toward greater information sharing by offering limited protections and creating more certainty as to how, why, and why not to share cyber threat and defensive measure information.


In situations in which a company would ordinarily be motivated, pre-CISA, to share cybersecurity information with the government or other companies, such as through participation in an ISAC or ISAO, there is probably a strong case for the company to follow CISA’s requirements and procedures in order to obtain the law’s protections. Most companies already employ procedures to remove personal information from the information they share, and while additional one-time and ongoing efforts and costs will be incurred to comply with CISA, the benefits seem likely to justify the costs.


The more difficult question for a company is whether CISA should lead it to increase its voluntary information sharing above its baseline levels.

In determining what information to share, a company should evaluate whether a cyber threat indicator or defensive measure implicates sensitive business information, and exercise particular care in evaluating the costs and benefits of sharing this information. It bears emphasis that CISA imposes no requirement to share cyber information, and if a company does choose to share it is free to distinguish between different types of information. As compared to more generic threat information, disclosing information about a company's own specific cyber vulnerabilities and incidents can carry legal, competitive, and reputational risks that are far greater if that information is learned by competitors and customers. In this regard, it will be important to understand the situations in which the federal government may share and make public information received under CISA, such as in the context of a criminal prosecution. For particularly sensitive information, companies will want to focus on the ability to share on an anonymous basis, such as through an ISAC or ISAO. Public companies will, among other things, need to assess how their decision to share information under CISA may interact with their disclosure decisions under the securities laws, given that sharing cyber information with the federal government could potentially be seen as an indicator of materiality requiring disclosure in a public filing.

In determining whether to share information under CISA, companies will need to make a realistic assessment of the strengths and limitations of the protections offered by the law. As noted above, the liability protection of section 106 generally does not apply when sharing with federal agencies other than DHS, except when a company communicates with its federal regulatory authority regarding a cybersecurity threat. And while there is a non-waiver of privilege protection that applies to information sharing with the federal government, there is no such provision that applies to sharing with state or local governments or other companies. CISA's protections also raise interpretive issues that bear further analysis, including the meaning of the protections against federal and state regulatory and enforcement action (including the reference to protection against enforcement actions for "lawful conduct"). As another example, CISA's preservation of contracts provision would need to be analyzed in relation to the liability protection.

A company that decides to share information under CISA should establish or adapt procedures and systems to collect, screen, and report the types of information the company deems appropriate to share—bearing in mind that the protections apply only when sharing is conducted according to the CISA's requirements, such as sharing only information that satisfies the definitions of "cyber threat indicator" and "defensive measures" and complying with the requirements for removal of personal information. Depending on the company's organization, its legal, IT, and compliance functions should coordinate to help ensure that information shared complies with CISA and, to the extent possible, is provided to the government in a way that will afford maximum protection, and that compliance with CISA is well documented.


Ultimately, whether and how to make use of CISA will be part of a company's larger cybersecurity strategy. For a more comprehensive discussion of the cybersecurity legal landscape and the decision points faced by companies, see the firm's memorandum, "Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks," available [here](#) .

CISA can be found [here](#)  (beginning at page 694), and links to the Guidance and other related documents can be found [here](#).

Endnotes:

[1] **[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](#)** .

([go back](#))

[2] CISA is one title among several in the broader Cybersecurity Act of 2015, which was itself the product of reconciling three separate bills—one introduced in the Senate and two in the House. See **[Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015](#)** .

([go back](#))


[3] While this post focuses on companies, CISA authorizes information sharing to and from "non-federal entit[ies]," a term that includes not only individuals, companies, and other private entities, but also state, tribal, and local governments and their agencies and departments. Section 102(14). The authorization to monitor and defend an information system,

however, is limited to “private entities.” Section 104(a)(1), (b)(1).

[\(go back\)](#)

[4] The law also allows “communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such a threat indicator” to receive liability protection. Section 105(c)(1)(B)(i).

[\(go back\)](#)

[5] DOJ and the Federal Trade Commission previously issued their own antitrust guidance to promote the sharing of cybersecurity information. See [Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, April 10, 2014](#).

[\(go back\)](#)

[6] The Guidance “is intended as assistance, not authority. It has no regulatory effect, confers no rights or remedies, and does not have the force of law.” Guidance at 3 n.4.

[\(go back\)](#)

[7] ISACs and ISAOs are bodies whose members share cyber information with each other and with the government, often on an anonymized basis. Whereas ISACs are tied to particular sectors, like the financial services industry, ISAOs are more flexible, facilitating sharing across sectors or industries.

[\(go back\)](#)

Both comments and trackbacks are currently closed.