The Department of Homeland Security

and

The Department of Justice

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

October 2020

Table of Contents

In December 2015, Congress enacted the Cybersecurity Act of 2015. Title I of the Cybersecurity Act of 2015, entitled the Cybersecurity Information Sharing Act of 2015 (CISA 2015 or the Act),[1] provides increased authority for cybersecurity information sharing between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government.[2] Section 105(a)(4) of the Act, 6 U.S.C. § 1504(a)(4), directed the Attorney General and the Secretary of the Department of Homeland Security (DHS) to jointly develop guidance to promote sharing of cyber threat indicators with Federal entities pursuant to CISA 2015 no later than 60 days after CISA 2015 was enacted. That guidance was first published on February 16, 2016, as required by statute.

Since then, the Department of Justice (DOJ) and DHS issued a final version of the CISA 2015 guidance and a collection of "Frequently Asked Questions" (FAQs) regarding the application of CISA 2015. Both of those documents incorporated input from the private sector that DOJ and DHS gathered during industry outreach. This amended version of the CISA 2015 guidance includes additional examples of information that may be shared under CISA 2015 and incorporates an updated version of the previously published FAQs as an annex.[3] Like its predecessors, this amended document is intended to assist non-Federal entities[4] in identifying cyber threat indicators and defensive measures and explain how to share them with Federal entities as authorized by CISA 2015 so that non-Federal entities may enjoy the protections afforded by the Act while engaged in such sharing.[5]

1. Scope of Guidance

As required by Section 1504(a)(4), this guidance addresses:

1. Identification of types of information that would qualify as a cyber threat indicator under the Act that would be unlikely to include information that is not directly related to a cybersecurity threat and is personal information of a specific individual or information that identifies a specific individual; and
2. Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

[1] CISA 2015 is codified at 6 U.S.C. §§ 1501–1510. For ease of reference, this Guidance generally cites to the sections as codified in title 6 of the U.S. Code.

[2] Section 1503(c)(1) authorizes both the sharing and receipt of cyber threat indicators and defensive measures. In most cases, references throughout this document to the authority to share such information pursuant to section 1503(c) also include the authority to receive the same information in accordance with section 1503(c).

[3] This 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. *See United States v. Caceres*, 440 U.S. 741 (1979). Further, the sharing of a cyber threat indicator or defensive measure with a non-Federal entity under the Act shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity. Section 1503(f).

[4] Pursuant to CISA 2015, "non-Federal entity" means any private entity, non-Federal government agency or department, or state, tribal, or local government (including a political subdivision, department, or component thereof) and includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States, but does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801). Section 1501(14)(A)-(C).

[5] This document focuses on providing guidance to non-Federal entities concerning how they may properly share cyber threat indicators and defensive measures with the government pursuant to CISA 2015. For policies and procedures specifically addressing the protection of individual rights for activities conducted under the Act, please refer to the jointly published Privacy and Civil Liberties Final Guidelines at https://www.us-cert.cisa.gov/ais.

It also explains how to identify and share defensive measures, even though section 1504(a)(4) does not require the guidance to do so.[6]

In addition to covering how to identify and share cyber threat indicators and defensive measures, this guidance also explains how to share those categories of information with Federal entities through the Federal Government's capability and process that is operated by DHS.[7] Furthermore, it explains how to share cyber threat indicators and defensive measures with DHS and other Federal entities— including law enforcement—through other means authorized by the Act and discusses the various legal protections the Act provides for such authorized sharing.[8]

2. Key Concepts

Congress enacted CISA 2015 to encourage robust sharing of useful cybersecurity information among all types of entities—private, Federal, state, local, territorial, and tribal. At the same time, CISA 2015 balances its authorization to share relevant cybersecurity information with the need to safeguard privacy. Accordingly, the Act incorporates three forms of privacy protections into its sharing authority: CISA 2015 (1) defines the types of cyber threat information that may be shared pursuant to the Act; (2) only authorizes sharing by non-Federal entities for a "cybersecurity purpose," which is a defined term; and (3) requires the removal of certain information prior to sharing that the sharer knows to be personal information or information that identifies a specific person that is not directly related to a cybersecurity threat.[9] These key concepts are discussed below. Sharing that does not meet the three requirements is not per se unlawful or subject to sanction, but such sharing would not be authorized or receive the protections provided by the Act, as described in Sections 3 and 4 below. Sharing not conducted pursuant to CISA 2015 may be eligible for protection under other law or regulations.

a. Shareable Information: Cyber Threat Indicators and Defensive Measures

CISA 2015 authorizes entities to share two categories of information: "cyber threat indicators" and "defensive measures." Each of these terms are defined by the Act.

i. Cyber Threat Indicators

CISA 2015 defines a cyber threat indicator to mean information that is necessary to describe or identify:

- Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of

[6] Although section 1504(a)(4) omits any reference to defensive measures, we have elected to include them in this guidance because the Act authorizes non-Federal entities to share defensive measures. Section 1503(c). Furthermore, providing guidance to non-Federal entities on sharing defensive measures is important because improperly shared information is not eligible for the Act's protections.

[7] See *infra* at pp. 13-15.

[8] See *infra* at p. 16.

[9] As used in this guidance, each instance of transmitting information to another entity or entities is considered a distinct act of "sharing"; each entity that transmits information (even if it received that information originally from another entity) to another entity is a "sharer"; and each entity sharing information is required to comply with the requirements of CISA 2015 to receive the protections afforded by the Act.

gathering technical information related to a cybersecurity threat or security vulnerability;[10]

- 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;
- The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- Any combination thereof.[11]

Congress intended a cyber threat indicator to constitute the type of technical data used in common cybersecurity activities.[12] By definition, a cyber threat indicator includes only information that is "necessary to describe or identify" an attribute of a cybersecurity threat or security vulnerability and, therefore, excludes many categories of sensitive personal and business information. The following are examples of information that contain cyber threat indicators that a private entity may share under CISA 2015:

---

[10] The definition of cyber threat indicator references a "cybersecurity threat" and "security vulnerability," which are terms defined by the Act. A cybersecurity threat is defined to mean:

> An action, not protected by the First Amendment to the Constitution of the United States, 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 or information that is stored on, processed by, or transiting an information system. The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Section 1501(5).

Many terms of service agreements prohibit activities that satisfy the definition of a "cybersecurity threat." However, activities that are "solely" violations of consumer agreements but do not otherwise meet the definition of a cybersecurity threat do not fall within section 1501(5)'s definition and, therefore, are not a cybersecurity threat under CISA 2015.

The definition of a cybersecurity threat includes activities that may have unauthorized and adverse results, but excludes authorized activities, such as extensive use of bandwidth that may incidentally cause adverse effects. S. Rep. No. 114-32, at 4. This definition clearly allows the sharing of information related to criminal hacking actions like theft of information or destruction of property.

A "security vulnerability" is defined to mean "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control." In contrast to a cybersecurity threat, it does not require adverse impact to an information system or information. Section 1501(17).

[11] Section 1501(6).

[12] *Cf.* S. Rep. No. 114-32, at 4 ("[T]his definition limits the information that can be shared under this Act to the techniques and 'malware' used by malicious actors to compromise the computer networks of their victims, not sensitive personal and business information contained in such networks.").

- A company could share 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 not been updated to patch a recent vulnerability.
- A security researcher could share her discovery of a technique that permits unauthorized access to an industrial control system.
- A software publisher could share a vulnerability it has discovered in its software.
- A managed security service company could share a pattern of domain name lookups that it believes correspond to malware infection.
- A manufacturer could share unexecuted malware found on its network.
- A researcher could share the domain names or IP addresses associated with botnet command and control servers.
- 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 other companies with similar assets.
- A newspaper suffering a distributed denial of service attack to its web site could share the IP addresses that are sending malicious traffic.
- A company could share a description of the anomalous pattern of operations and associated system data for an industrial control system that appears to be related to malicious reconnaissance or to the existence of a security vulnerability.[13]

Information that provides background that is necessary to describe or identify a cybersecurity threat—which is sometimes called "contextual information"—may also be a cyber threat indicator that may be shared under CISA 2015, so long as it falls into any of the categories of information enumerated in section 1501(6) and is shared consistent with CISA 2015's other sharing requirements.[14] For example, a description of the steady-state operation of a system before it is compromised may be necessary to describe or identify the method used to defeat a security control or exploit a vulnerability and, therefore, may be a cyber threat indicator that may be shared under section 1501(6)(B).[15]

To help ensure consistency with CISA 2015's definitions and requirements, particularly in connection with automated sharing, standardized fields in structured formats can be used to establish a profile that limits the type of information in a cyber threat indicator (or defensive measures, as discussed further below). Much of the information that constitutes a cyber threat indicator is centered on an observable fact about the cyber threat. For example, a cyber threat indicator has a variety of possible observable characteristics: a malicious email, internet protocol (IP) addresses, file hashes, domain names, uniform resource locators (URLs), malware files, and malware artifacts (attributes about a file). The specificity and nature of the observable facts are designed to reduce the risk that a cyber threat indicator contains personal information not directly related to a cybersecurity threat. DHS's Automated Indicator Sharing (AIS) initiative uses this means of controlling the type of information that may be shared using the automated system discussed in section 3.b.i.

[13] For additional discussion of sharing cyber threat indicators involving industrial controls systems and operational technology systems, see Annex 2, FAQ #22.
[14] See Annex 2, FAQ #1 for a discussion of CISA 2015's requirements.
[15] See Annex 2, FAQ #21 for more discussion of sharing contextual information.

ii. Defensive Measures

CISA 2015 defines a defensive measure to mean:

> An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure; or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.[16]

For example, a defensive measure could be something as simple as a security device that protects or limits access to a company's computer infrastructure or as complex as sophisticated software tools used to detect and protect against anomalous and unauthorized activities on a company's information system.[17]

Similar to cyber threat indicators, defensive measures are composed of an "action, device, procedure, signature, technique, or other measure" that is commonly associated with cybersecurity activities.[18] Some examples of defensive measures include but are not limited to:

- 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 firewall rule that disallows a type of malicious traffic from entering a network.
- An algorithm that can search through a cache of network traffic to discover anomalous patterns that may indicate malicious activity.
- A technique for quickly matching, in an automated manner, the content of an organization's incoming Simple Mail Transfer Protocol (SMTP, a protocol commonly used for email) traffic against a set of content known to be associated with a specific cybersecurity threat without unacceptably degrading the speed of email delivery to end users.

[16] Section 1501(7).

[17] When developing and implementing defensive measures pursuant to section 1503(b), due diligence should be exercised to ensure that they do not unlawfully access or damage information systems or data. CISA 2015's definition of and authorization to use a defensive measure (sections 1501(7) and 1503(b), respectively) do 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. Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015, at 8847. Cognizant of the fact that defensive measures deployed on one entity's network could have effects on other networks, Congress defined a defensive measure to only include measures on an entity's information systems that do not cause substantial harm to another entity's information systems or data. Even if a defensive measure does not cause substantial harm, it is still not within CISA 2015's definition if it enables unauthorized access to another entity's information systems. See section 1501(7)(B).

[18] Section 1501(7).

b. A Cybersecurity Purpose

CISA 2015 only authorizes non-Federal entities to share and receive cyber threat indicators and defensive measures for a "cybersecurity purpose," which is defined as 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.[19] While a cybersecurity purpose encompasses a broad range of activities taken to protect information and information systems from cybersecurity threats,[20] it imposes some limits on the purposes for which cyber threat indicators and defensive measures may be shared and receive CISA 2015's protections.[21] If cyber threat indicators or defensive measures are shared for other purposes, they are not shared in accordance with CISA 2015 and, therefore, will not receive CISA 2015's legal protections. Such sharing, however, may be authorized by other statutes and eligible for protection, as provided by those statutes.

c. Removal of Personal Information not Directly Related to a Cybersecurity Threat

Information that meets the definition of a cyber threat indicator or a defensive measure and is shared for a cybersecurity purpose will generally consist of technical data that typically will not contain personal information. Nevertheless, as an additional privacy protection, CISA 2015 imposes an express obligation on a non-federal entity sharing a cyber threat indicator under the Act to take affirmative steps to identify and remove extraneous personal information the sharer knows at the time of sharing is not directly related to a cybersecurity threat, before such sharing occurs.[22]

i. Identifying "Personal Information" and Determining Whether it is Subject to Removal Before Sharing

Section 1503(d) imposes a requirement on a sharer to remove extraneous personal information from a cyber threat indicator before sharing it. Specifically, section 1503(d)(2) requires a sharer to remove any information from a cyber threat indicator that is not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.[23] This can be accomplished by either (a) reviewing cyber threat indicators and removing identified information or (b) implementing and utilizing a "technical capability configured to remove" such information.[24]

Not all personal information identified in this review will need to be removed prior to sharing. On occasion, information known at the time of sharing to be personal information of a specific individual or information that identifies a specific individual will be "directly related to a

[19] Section 1501(4).
[20] "Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015" *Congressional Record* 161:185 (December 18, 2015) p. 8847. Available at https://www.govinfo.gov/content/pkg/CREC-2015-12-18/html/CREC-2015-12-18-pt1-PgS8844.htm.
[21] See *supra* p. 3 and note 12.
[22] Section 1503(d)(2).
[23] Section 1503(d)(2).
[24] Sections 1503(d)(2)(a), (b).

cybersecurity threat" and, therefore, shareable under CISA 2015.

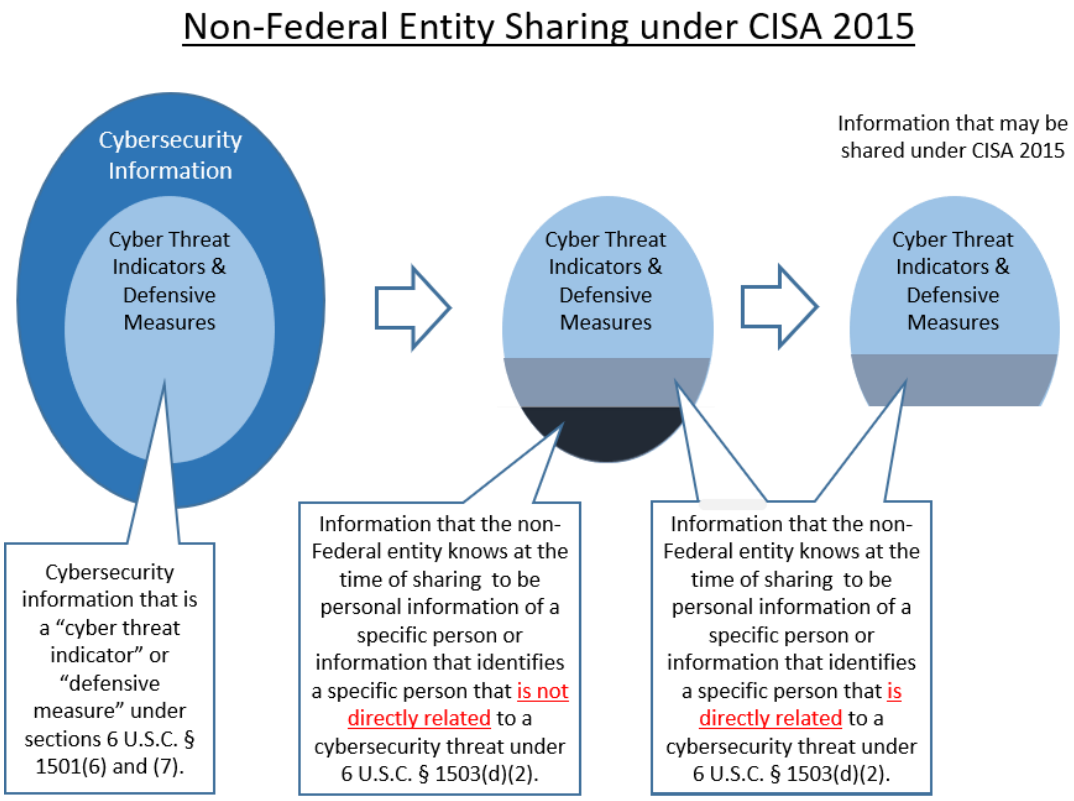
Personal information directly related to a cybersecurity threat includes personal information that is necessary to detect, prevent, or mitigate a cybersecurity threat. In some circumstances, a cyber threat indicator (i.e., information necessary to identify or describe a cybersecurity threat or security vulnerability) may contain personal information, but still may be sharable if that personal information is also directly related to a cybersecurity threat. For example, personal information may be necessary to identify or describe a spear phishing email. For a phishing email, information about the sender of email (such as "From"/"Sender" address), a malicious URL in the e-mail, malware files attached to the e-mail, the content of the e-mail, and additional email information related to the malicious email or potential cybersecurity threat actor (such as Subject Line, Message ID, and X-Mailer) all typically meet the definition of a cyber threat indicator. While some of this information could be information a sharer knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual, that personal information could be necessary to identify or describe a cybersecurity threat ***and*** be directly related to a cybersecurity threat. It, therefore, would be shareable for a cybersecurity purpose under CISA 2015.

Other information known at the time of sharing to be personal information of a specific individual or information that identifies a specific individual, such as the names and e-mail addresses of the recipients of the email (i.e., the "To" address), would typically be personal information not directly related to a cybersecurity threat, and therefore would usually not be sharable under CISA 2015.[25] For instance, while sharing the medical condition of a particular individual targeted for a phishing attack is unlikely to be directly related to a cybersecurity threat, sharing an anonymized characterization of a cyber threat (e.g., describing a phishing tactic as emails that included medical information about the recipient) may have utility.

As with cyber threat indicators, information known at the time of sharing to be personal information of a specific individual or information that identifies a specific individual may occasionally be part of a defensive measure. While section 1503(d)(2) requires removal of certain personal information from a cyber threat indicator, it does not expressly require that personal information be removed from a defensive measure before it is shared under CISA 2015. Regardless, non-Federal entities are encouraged to treat defensive measures no differently than cyber threat indicators in regard to the review of personal information under section 1503(d)(2) to provide an added degree of privacy protection. Such an approach is also prudent because a defensive measure may include a cyber threat indicator that contains information that a sharer knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual. If so, and the personal information is not directly related to the cyber threat, that personal information must be removed before the defensive measure is shareable under CISA 2015.

[25] In some cases, knowing the specific recipient of a communication (as opposed to the general category or title(s) of employees being targeted) may be a necessary facet of identifying and preventing future attacks. For instance, knowing that specific personnel, such as specific managers or officials, were targeted by a phishing campaign may help identify future targets and take appropriate preventative measures. In such a case, the identities of recipients of a phishing email may be considered directly related to a cybersecurity threat. In addition, a general category of targets (e.g., "senior management") or titles of targets (e.g., "threat analysts"), which generally do not include personal information of a specific individual or information that identifies a specific individual, may be directly related to a cybersecurity threat and shareable under CISA 2015.

For example, a signature for protecting against targeted exploits such as spear phishing attacks may be used to identify or block messages from a specific email address that is the source of malicious emails. Because this signature is applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability, it would typically meet the definition of a defensive measure. While the defensive measure may contain information that the sharer knows at the time to be personal information of a specific individual or information that identifies a specific individual, that information could be directly related to the cyber threat. Therefore, it could be shared for a cybersecurity purpose under CISA 2015.[26]



ii. Information Protected under Otherwise Applicable Privacy Laws that is Unlikely to Be Directly Related to a Cybersecurity Threat

Under section 1503(c), a non-Federal entity may share a cyber threat indicator or defensive measure for a cybersecurity purpose "notwithstanding any other provision of law." Consequently, otherwise conflicting laws, including privacy laws, do not restrict sharing under CISA 2015. To assist in the task of identifying information that should still be removed based on the manual or technical review described above, section 1504(a)(4)(B)(ii) requires this guidance to help entities identify certain types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat. As explained above, cyber threat indicators and defensive measures will typically consist of technical information that describes attributes of a cybersecurity threat that generally need not

[26] See annex 2, FAQ #8 for further discussion.

include information in many of the categories of information that are protected by privacy laws. Information that is generally protected under privacy laws and is unlikely to be directly related to a cybersecurity threat may include:[27]

- Protected Health Information (PHI), which is defined in the HIPAA Privacy Rule (45 C.F.R. § 160.103 (2019)) as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium. PHI is information, including demographic information, that relates to:

    - the individual's past, present, or future physical or mental health or condition,
    - the provision of health care to the individual, or
    - the past, present, or future payment for the provision of health care to the individual,

    and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

    For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content.

- Human Resource Information, which may include information contained within an employee's personnel file, such as hiring decisions, performance reviews, and disciplinary actions.

- Consumer Information/History, which may include information related to an individual's purchases, preferences, complaints and even credit. The Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 et seq.) requires that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information.

- Education History, which is information that relates to an individual's education, such as transcripts, or training, such as professional certifications. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 C.F.R. Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

- Financial Information, which is composed of a wide variety of information that is highly sensitive and highly regulated. Financial information includes anything from bank statements, to loan information, to credit reports. Certain laws, such as the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.), require financial institutions – companies that offer consumers financial

[27] The discussion of potentially relevant privacy laws mentioned below is not intended to be exhaustive.

products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

- Identifying information about property ownership that is protected by privacy laws. Although some information about property ownership may be publicly available, such as property purchase records, other information, such as Vehicle Identification Numbers, is inherently more sensitive and typically governed by state laws.

- Identifying information of children under the age of 13 that is subject to certain requirements under the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501-6506), which imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

In particular, the content of user-generated communications may be more likely to contain sensitive or protected information such as those found in the categories listed above. Thus, non-Federal entities should exercise particular care when reviewing such information before sharing it with a Federal entity.

3. How to Share Cyber Threat Indicators and Defensive Measures with the Federal Government

The Act authorizes non-Federal entities to share cyber threat indicators and defensive measures with Federal entities—and non-Federal entities—as provided by section 1503(c).[28] In addition, section 1504(c) specifically provides for sharing such information through the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, which is operated by DHS pursuant to section 1504(c). That capability and process was certified as operational by the Secretary of DHS in March 2016, as required by CISA 2015.

How a non-Federal entity shares cyber threat indicators and defensive measures with the Federal Government affects the types of protections the non-Federal entity receives under CISA 2015. All sharing conducted in accordance with section 1503(c) receives certain protections under CISA 2015. Section 1503(c) authorizes sharing of cyber threat indicators and defensive measures with any Federal entity (or non-Federal entity) for a cybersecurity purpose and *notwithstanding any other provision of law*.[29] It, therefore, furnishes authority that overrides any conflicting law.[30] In addition, when such sharing is conducted with the Federal government through the DHS capability and process, or as otherwise provided for by section 1504(c)(1)(B), it also receives additional liability protection under section 1505(b)(2).

Sharing conducted pursuant to section 1503(c) but not through DHS's capability and process or any of the other means provided for in section 1504(c)(1)(B) does not receive section

[28] While not the focus of this guidance, private entities also receive liability protection under section 1505(b)(1) for sharing cyber threat indicators and defensive measures with other private entities in accordance with CISA 2015. See Chart in Annex 1.
[29] A non-Federal entity must also comply with otherwise lawful restrictions placed on the sharing or use of a cyber threat indicator or defensive measure imposed by the sharing non-Federal entity or Federal entity. Section 1503(c)(2).
[30] See Annex 2, FAQ #1 for more discussion on the legal protections provided by section 1503(c)'s "notwithstanding any other provision of law" clause.

1505(b)(2)'s additional liability protection (i.e., sharing with a Federal entity that is not conducted through the DHS capability and process in section 1504(c) or through one of the other means provided for in section 1504(c)(1)(B)).[31] However, it still receives the array of other protections that apply to all sharing conducted pursuant to CISA 2015. Those protections, which include exemptions from state and Federal disclosure laws and from antitrust liability, are further discussed in section 4.[32]

As described in Section 2.b above, CISA 2015 only authorizes information sharing for a cybersecurity purpose.[33] It does not limit or modify any existing information sharing or reporting relationship, prohibit an existing or require a new information sharing relationship, or mandate the use of the capability and process within DHS developed under section 1504(c).[34]

Sharing conducted through the means discussed in this guidance should not be construed to satisfy any statutory, regulatory, or contractual obligation.[35] It is not a substitute for voluntary or mandatory reporting of information to Federal entities, such as reporting known or suspected cybercrimes directly to appropriate law enforcement agencies; known or suspected cyber incidents directly to DHS, including to the Cybersecurity and Infrastructure Security Agency (CISA); or required reporting to regulatory entities. The sharing addressed in this guidance is intended to complement, not supplant, the prompt reporting of any criminal activity, cyber incidents, or reportable events to the appropriate authorities.

a. Requirements for Non-Federal Entities Sharing Cyber Threat Indicators and Defensive Measures with Federal Entities

CISA 2015's information sharing authorization and other legal protections for information sharing only attach to sharing cyber threat indicators and defensive measures, as those terms are defined by the Act. CISA 2015 does not cover the sharing of information that falls outside the definition of those terms. For example, the *entire* contents of a hard drive of a personal computer that has been compromised by a cyber threat actor would be unlikely only to contain information constituting a cyber threat indicator or defensive measure; therefore, sharing it in its entirety may fall outside the scope of CISA 2015. However, sharing cyber threat indicators extracted from the hard drive of a compromised computer would be eligible for CISA 2015's protections, if done in accordance with CISA 2015's requirements. The same limitations apply to bulk sharing of network logs, netflow data, or other similar artifacts gathered during incident response.

As described in Section 2.c above, under section 1503(d)(2)(A), a non-Federal entity must also review cyber threat indicators prior to sharing them to assess whether they contain any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that

[31] Even if a Federal entity receiving the information shares it with DHS immediately upon receipt, the sharing with the Federal entity--not conducted through the DHS capability and process or as otherwise authorized by 1504(c)(1)(B)—still would not receive liability protection under section 1505(b)(2). See Annex 2, FAQ #4 for a fulsome discussion of CISA 2015's liability protection provisions.
[32] See Annex 2, FAQ #5 for more information. See also Chart in Annex 1 on page 24.
[33] While sharing for other purposes is not per se unlawful, sharing that does not meet all three requirements of CISA 2015, including sharing for a cybersecurity purpose, would not fall under the Act's authorizations and would be ineligible for receiving the Act's protections. See *supra* p. 3.
[34] See section 1507(f).
[35] See Annex 2, FAQ #11.

identifies a specific individual. Any such information must be removed.

As described above, if a non-Federal entity does not "know at the time of sharing" that a cyber threat indicator contains personal information of a specific individual or information that identifies a specific individual, the non-Federal entity is not required to alter the shared information before sharing it. A non-Federal entity may conduct its review for such information using either a manual or technical process; either is permissible under CISA 2015.[36]

b. Non-Federal Entities Sharing Cyber Threat Indicators and Defensive Measures through the Real-Time DHS Capability and Process

Section 1504(c) of the Act directs the Secretary of DHS to develop a capability and process within DHS that will accept cyber threat indicators and defensive measures in real time from any non-Federal entity, including private entities. Non-Federal entities may share such information with DHS through this capability and process, and DHS will in turn relay that information to Federal entities in an automated manner,[37] as required by the Act and consistent with the operational and privacy and civil liberties policies instituted under sections 1504(a) and (b).[38] In March 2016, upon certification by the Secretary of Homeland Security in accordance with section 1504(c), the DHS capability and process became the process by which the Federal Government receives cyber threat indicators and defensive measures under the Act that are shared by a non-Federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems, with the specific exception of the other means of sharing discussed below in section 3.c of this document.

Provided that sharing is otherwise conducted in accordance with the Act, sharing conducted through this DHS capability will receive liability protection under section 1505(b). It will, like any other sharing conducted in accordance with CISA 2015, also receive the other protections provided by the Act discussed more fully below in section 4. The implementation of this capability does not, however, limit or prohibit otherwise lawful disclosures of communications, records, or other information, including the reporting of known or suspected criminal activity.[39] It also does not limit or prohibit voluntary or legally compelled participation in a Federal law enforcement investigation or affect the provision of cyber threat indicators or defensive measures as part of a contractual requirement.[40]

Non-Federal entities may share cyber threat indicators and defensive measures through the DHS capability and process created under section 1504(c) via the AIS initiative, web form, email, or other information sharing programs that use these means of receiving cyber threat

[36] See section 1503(d)(2)(A) and (B). In addition, although not directly relevant to this guidance on information sharing between non-Federal and Federal entities, non-Federal entities should remain mindful that CISA 2015 requires non-Federal entities to "implement and utilize a security control to protect against unauthorized access to or acquisition of such shared cyber threat indicator or defensive measure." Section 1503(d)(1).

[37] Section 1504(a)(3)(A) requires DHS to disseminate cyber threat indicators and defensive measures shared with DHS pursuant to section 1504(c) to the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence in an automated fashion. Section 1504(a)(3)(A)(i).

[38] The Privacy and Civil Liberties Final Guidelines and Operational Procedures are available at https://www.us-cert.cisa.gov/ais.

[39] Section 1504(c)(1)(e). See also Annex 2, FAQ #6.

[40] Section 1504(C)(1)(E).

indicators or defensive measures. Sharing conducted using any of these means is eligible for liability protection, as well as CISA 2015's other protections and exemptions. Instructions on utilizing each method can be found below.

i. Automated Indicator Sharing (AIS)

Non-Federal entities may share cyber threat indicators and defensive measures with Federal entities using DHS's AIS initiative, which enables the timely exchange of cyber threat indicators and defensive measures among the private sector, state, local, tribal, and territorial governments and the Federal government. AIS leverages a technical specification for the format and exchange of cyber threat indicators and defensive measures using Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), respectively. By using standardized fields (STIX) and communication methods (TAXII), DHS enables organizations to share structured cyber threat information in a secure and automated manner.

To share cyber threat indicators and defensive measures through AIS, participants acquire their own TAXII client that will communicate with the DHS TAXII server. AIS participants also execute the AIS Terms of Use and follow submission guidance that outlines the type of information that should and should not be provided when submitting cyber threat indicators and defensive measures through AIS.

Once a cyber threat indicator or defensive measure is received, analyzed, and sanitized, AIS will share the indicator or defensive measure with all AIS participants. AIS will not provide the identity of the submitting entity to other AIS participants unless the submitter consents to the sharing of its identity as the source of the cyber threat indicator or defensive measure submission.

Cyber threat indicators and defensive measures submitted via automated means including AIS are considered part of the DHS capability and process created under section 1504(c) and, therefore, eligible for liability protection, as well as CISA 2015's other protections and exemptions. For more information on AIS, visit the AIS web page at https://www.us-cert.cisa.gov/ais. Entities wishing to connect to AIS may send an email to the address listed at https://www.us-cert.cisa.gov/ais.

ii. Web Form

Non-Federal entities may share cyber threat indicators and defensive measures with DHS's CISA by filling out a web form on a CISA website (including us-cert.cisa.gov). Cyber threat indicators and defensive measures submitted via web form to CISA are considered part of the DHS capability and process created under section 1504(c) and, therefore, eligible for liability protection, as well as CISA 2015's other protections and exemptions. For more information, non-Federal entities may visit the web page at https://www.us-cert.cisa.gov/ais.[41]

iii. Email

Non-Federal entities may share cyber threat indicators and defensive measures with DHS's CISA by sending an email to CISA. Cyber threat indicators and defensive measures submitted

[41] See Annex 2, FAQ #19.

via email are considered part of the DHS capability and process created under section 1504(c) and, therefore, eligible for liability protection, as well as CISA 2015's other protections and exemptions. For more information, non- Federal entities may visit the web page at https://www.us-cert.cisa.gov/ais.[42]

iv. Other DHS Programs through which Cyber Threat Indicators and Defensive Measures May Be Shared Using the DHS Capability and Process

Non-Federal entities may also share cyber threat indicators and defensive measures with DHS's CISA by sharing within programs that leverage automated machine-to-machine sharing, web forms or email. For example, CISA provides access to communities of interest (such as industrial control systems owners and operators) through a web-based portal, which allows sharing of indicators via web form or secure messaging capabilities within the portal. Stakeholders participating in CISA's Cybersecurity Information Sharing and Collaboration Program may share cyber threat indicators or defensive measures within that program, leveraging automated machine-to-machine sharing, web forms or email. Any sharing of cyber threat indicators or defensive measures with CISA using one of these methods for sharing is considered to be sharing with DHS's capability and process created under section 1504(c) and, therefore, eligible for liability protection, as well as CISA 2015's other protections and exemptions.

v. Information Sharing and Analysis Organizations and Centers

Under section 1503(c), non-Federal entities may also share cyber threat indicators and defensive measures with Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs), who may then share cyber threat indicators or defensive measures with Federal entities. In general, ISACs and ISAOs are private entities. Under section 1505(b)(1), private entities that share a cyber threat indicator or defensive measure with an ISAC or ISAO in accordance with the Act receive liability protection and other protections and exemptions for such sharing.[43] Similarly, ISACs and ISAOs that share information with other private entities in accordance with the Act also receive liability protection under section 1505(b)(1), as well as the other protections and exemptions discussed below.[44] Likewise, an ISAC or ISAO that shares cyber threat indicators or defensive measures with the Federal government in accordance with section 1503(c) through the DHS capability and process created under section 1504(c), or as otherwise consistent with section 1504(c)(1)(B), is also eligible for liability protection under section 1505(b)(2), in addition to CISA 2015's other protections and exemptions.[45] Each of these examples is a different instance of sharing, and each entity must comply with the requirements of CISA 2015 to receive the Act's protections for their respective information sharing.

c. Non-Federal Entities Sharing with Federal Entities through Means Other than the DHS Capability and Process

Consistent with CISA 2015, non-Federal entities may also share cyber threat indicators and defensive measures with Federal entities through means other than the Federal government's capability and process operated by DHS described in sections 3.b.i through iv above and receive

[42] *Id.*
[43] The topic of sharing between non-governmental entities is further addressed at Annex 1.
[44] See *infra* at pp. 17-19.
[45] See Annex 2, FAQ #3 for more on sharing with ISACs and ISAOs.

legal protections for doing so. Section 1503(c) authorizes, notwithstanding any provision of law, a non-Federal entity to share cyber threat indicators and defensive measures with a Federal entity—or any non-Federal entity—so long as the sharing is conducted in accordance with all of CISA 2015's sharing requirements.[46]

Section 1505(b)'s additional liability protection, however, only applies when a private entity shares cyber threat indicators or defensive measures with the Federal government "consistent with" section 1504(c)(1)(B). That section identifies two means of sharing that receive section 1505(b)'s statutory immunity other than by sharing through the DHS capability and process.

First, section 1504(c)(1)(B)(i) allows the sharing of "communications," consistent with section 1503, between a Federal and non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or to develop a defensive measure based on such cyber threat indicator. This section would apply when a non-Federal entity first shares a cyber threat indicator with the DHS capability and process or a regulator as permitted by section 1504(c)(1)(B)(ii) discussed below, and then engages in communications with a Federal entity regarding that previously shared indicator. Section 1503 only permits sharing of cyber threat indicators and defensive measures for cybersecurity purposes (section 1503(c)) and requires removal of certain irrelevant personal information prior to such sharing (section 1503(d)(2)).

Second, section 1504(c)(1)(B)(ii) also permits communications between a regulated non-Federal entity and its Federal regulatory authority regarding a cybersecurity threat. Unlike section 1504(c)(1)(B)(i), it is not expressly limited to communications about a previously shared communication.

While both sections 1504(c)(1)(B)(i) and (ii) discuss the sharing of "communications," only the sharing of cyber threat indicators and defensive measures receive liability protection under section 1505(b). Moreover, for sharing consistent with section 1504(c)(1)(B) to receive liability protection, section 1505(b)(1) requires that such sharing be conducted in accordance with CISA 2015. Accordingly, liability protection for sharing under both sections 1504(c)(1)(B)(i) and (ii) requires adherence to all of CISA 2015's requirements (e.g., removal of certain personal information pursuant to section 1503(d)(2), sharing cyber threat indicators or a defensive measure, and sharing for a cybersecurity purpose).[47]

4. Other Protections CISA 2015 Extends to Sharing Cyber Threat Indicators and Defensive Measures

In addition to the liability protections discussed above, the Act provides other protection to sharing entities and protects information shared in accordance with the Act. Sharing with the Federal government *other than* in a manner consistent with section 1504(c)(1)(B) does not receive section 1505(b)'s liability protection; however, such sharing is eligible for all of the other protections furnished by the Act, just the same as sharing conducted with DHS under section

[46] See Annex 2, FAQ #1 for a list of CISA 2015's requirements.
[47] See Annex 2, FAQ #4.

1504(c), so long as the sharing otherwise adheres to CISA 2015's requirements (e.g., removal of certain personal information pursuant to section 1503(d)(2), sharing cyber threat indicators or a defensive measure, and sharing for a cybersecurity purpose).

Other than section 1505(b) liability protection, CISA 2015 provides the following protections for sharing cyber threat indicators and defensive measures with any Federal entity conducted pursuant to section 1503(c):[48]

- Antitrust Exemption: The Act provides 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.[49] It supplements the policy statement issued by the Department of Justice's Antitrust Division and the Federal Trade Commission in May 2014 stating that sharing of cyber threat information would in the normal course be unlikely to violate Federal antitrust laws.[50] The Act also expressly prohibits conduct that would otherwise constitute an antitrust violation, notwithstanding the exception provided by section 1503(e) to prevent this exception from being used as the basis for committing antitrust violations under the guise of cybersecurity information sharing.[51]

- Exemption from Federal and state disclosure laws: The Act provides that cyber threat indicators or defensive measures shared with the Federal government under CISA 2015 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.[52] Shared information is also deemed "voluntarily shared," which assists in protecting appropriately shared information from disclosure under The Critical Infrastructure Information Act of 2002.[53]

- Exemption from certain state and Federal 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. However, a cyber threat indicator or defensive measure may, consistent with a Federal, state, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information

[48] See Annex 2, FAQ #5.
[49] Section 1503(e).
[50] The DOJ/FTC policy statement revisited a business review letter prepared by the Antitrust Division in 2000 in which it examined a proposed cybersecurity information sharing program. The policy statement reaffirmed the conclusions of the 2000 business review letter. It stated, "While this guidance is now over a decade old, it remains the Agencies' current analysis that properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns." Policy Statement at 1, *available at* http://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf.
[51] Section 1507(e); see also Annex 2, FAQ #12.
[52] Section 1504(d)(3); see also section 1503(d)(4)(B) for information shared by or with a state, tribal, or local government.
[53] Annex 2, FAQ #13.

systems. CISA 2015's legislative history states that congressional drafters viewed this as a narrow exception to ensure that government agencies with regulatory authority understand the current landscape of cyber threats and those facing the particular regulatory sector over which they have cognizance.[54]

- No waiver of privilege for shared material: Under the Act, 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.[55]

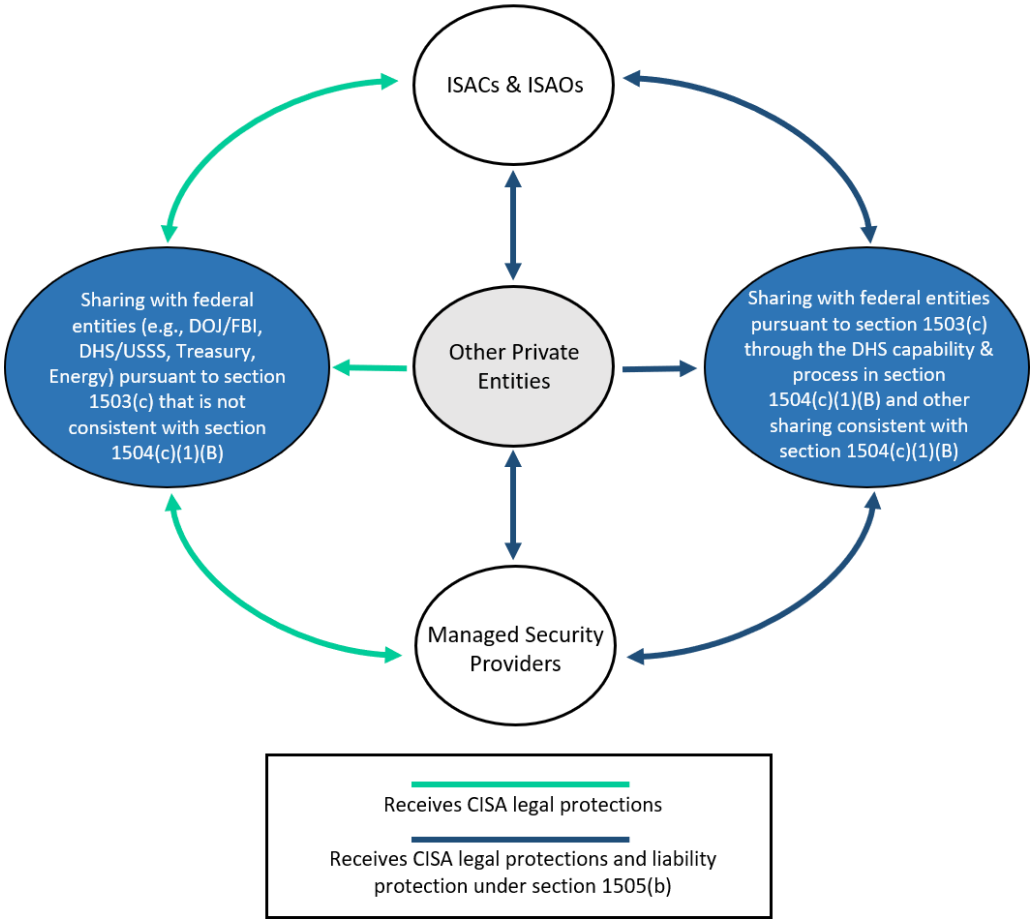
- Treatment as commercial, financial, and proprietary information: When so designated by the sharing entity, shared information shall be treated as commercial, financial, and proprietary information. The legislative history indicates that Congress expected the Federal government to further share and use such information for cybersecurity purposes consistent with the privileges, protections, and any claims of propriety on such information.[56]

- Ex parte communications waiver: Under the Act, 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. This provision addresses concerns about ex parte communications related to the Administrative Procedure Act (APA), 5 U.S.C. § 553.[57]

The availability of the protections described above varies depending on the nature of the entity sharing information with the Federal Government. All of CISA 2015's protections, including liability protection, are available to private entities, which CISA 2015 defines to include private companies and other private organizations, as well as "State, tribal, or local government performing utility services, such as electric, natural gas, or water services."[58] In addition to private entities, CISA 2015's definition of "non-Federal entities" includes other State, tribal, or local government entities. But such non-Federal entities are not eligible for liability protection or antitrust protection, which is reserved for "private entities."[59] They are, however, eligible for CISA 2015's other protections discussed above. Sharing cyber threat indicators and defensive measures with State, tribal, or local government entities is exempt from state disclosure laws.[60] Furthermore, CISA 2015 limits regulatory use of such shared information by a State, tribal, or local government.[61]

[54] Section 1504(d)(5)(D); see also section 1503(d)(4)(C) for information shared with a state, tribal, or local government.
[55] Section 1504(d)(1); see also Annex 2, FAQ #14.
[56] Section 1504(d)(2).
[57] Section 1504(d)(4).
[58] Section 1501(15)(B).
[59] See sections 1505(b), 1503(e).
[60] Section 1503(d)(4)(B).
[61] Section 1503(d)(4)(C).

Protections for Sharing with Federal Entities Under CISA 2015



Sharing Cyber Threat Indicators and Defensive Measures with a Federal Entity					
Means of Sharing	Authority for Sharing	Liability Protection Provision	Receiving Federal Entity	Requirements	Protections Conferred for Sharing Under the Act
DHS Capability and Associated Programs and other sharing permitted under section 1504(c)(1)(B)	Sections 1503(c) and 1504(c)(1)(B)	Section 1505(b)(2)	DHS	• Sharing for a cybersecurity purpose. Section 1503(c) • Sharing cyber threat indicators or defensive measures. Sections 1503(c) and 1505(b)(2) • Implement and utilize a security control to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures. Section 1503(d)(1) • Removal prior to sharing using a manual or technical means of information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific person or information identifying a specific person. Section 1503(d)(2)(A) and (B) • When receiving cyber threat indicators from the government observe lawful restrictions placed by the sharing entity. Section 1503(c)(2) • Compliance with procedures for submission to DHS	• Liability protection for sharing of cyber threat indicators or defensive measures. Section 1505(b) ** • Exemption from state disclosure laws. Section 1503(d)(4)(B) * • Exemption from state regulatory use. Section 1503(d)(4)(C) * • No waiver of privilege for shared material. Section 1504(d)(1) • Treatment as commercial, financial, and proprietary information. Section 1504(d)(2) • Deemed voluntarily shared. Section 1504(d)(3)(A) • Exemption from Federal disclosure laws. Section 1504(d)(3) • Ex parte communications waiver. Section 1504(d)(4) • Exemption from Federal regulatory use. Section 1504(d)(5)(D)

* This exemption applies to indicators and defensive measures shared with a State, tribal, or local government entity rather than with a Federal entity; however, it is included here in the interest of completeness.

** This protection applies only to private entities, not other non-Federal entities.

Sharing Cyber Threat Indicators and Defensive Measures with a Federal Entity (Continued)					
Means of Sharing	Authority for Sharing	Liability Protection Provision	Receiving Federal Entity	Requirements	Protections Conferred for Sharing Under the Act
Any other sharing conducted under the Act	Section 1503(c)	N/A	Any Federal entity (e.g., FBI, DHS, DOE, Treasury, DoD)	• Sharing for a cybersecurity purpose. Section 1503(c) • Sharing cyber threat indicators or defensive measures. Sections 1503(c) and 1505(b)(2) • Implement and utilize a security control to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures. Section 1503(d)(1) • Removal prior to sharing using a manual or technical means of information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific person or information identifying a specific person. Section 1503(d)(2)(A) and (B) • When receiving cyber threat indicators from the government observe lawful restrictions placed by the sharing. Section 1503(c)(2)	• Exemption from state disclosure laws. Section 1503(d)(4)(B) * • Exemption from state regulatory use. Section 1503(d)(4)(C) * • No waiver of privilege for shared material. Section 1504(d)(1) • Treatment as commercial, financial, and proprietary information. Section 1504(d)(2) • Deemed voluntarily shared. Section 1504(d)(3)(A) • Exemption from Federal disclosure laws. Section 1504(d)(3) • Ex parte communications waiver. Section 1504(d)(4) • Exemption from Federal regulatory use. Section 1504(d)(5)(D)

* This exemption applies to indicators and defensive measures shared with a State, tribal, or local government entity rather than with a Federal entity; however, it is included here in the interest of completeness.

Annex 1: Cyber Threat Indicator and Defensive Measure Sharing between Non-Governmental Entities under CISA 2015

Section 1504(a)(4) does not direct the Federal government to produce guidance covering how private entities may share cyber threat indicators and defensive measures with each other under CISA 2015. However, multiple private organizations have requested such guidance to facilitate their information sharing practices. Accordingly, the following chart furnishes a summary of the protections and exemptions that non-governmental entities receive for sharing cyber threat indicators and defensive measures with each other in accordance with CISA 2015.

CISA 2015 authorizes private entities to share cyber threat indicators and defensive measures with other private entities.[1] It also provides private entities with liability protection for conducting such sharing in accordance with CISA 2015.[2] In general, private entities include, but are not limited to, ISACs, ISAOs, and cybersecurity and managed security services providers. It is noteworthy that CISA 2015's definition of a private entity includes a State, tribal, or local government that performs utility services.[3] The chart below addresses protections and exemptions available for sharing between non-governmental entities, and so uses the term "non-governmental entity" in lieu of "private entity."

Sharing between private entities, regardless of whether they are non-governmental, is subject to the same requirements as sharing between private and Federal entities discussed above. For instance, under CISA 2015 only cyber threat indicators and defensive measures may be shared, the sharing must be for a cybersecurity purpose, and the removal of certain personal information pursuant to section 1503(d)(2) is required. Some of the protections discussed above do not apply to information sharing between non-governmental entities because those protections only cover information shared with governmental entities (e.g., Federal and state disclosure laws). In the event a non-governmental entity shares a cyber threat indicator or defensive measure with another non-governmental entity, and the receiving non-governmental entity subsequently shares that information with a Federal or state entity (consistent with any lawful restrictions placed by the original sharing entity), those additional protections would then apply to the information that was shared with the Federal or state entity, as discussed above.

[1] Section 1503(c).
[2] Section 1505(b)(1).
[3] Section 1501(15)(B).

Sharing Cyber Threat Indicators and Defensive Measures between Non-Governmental Entities			
Authority for Sharing & Receiving	Liability Protection Provision	Requirements	Protections Conferred for Sharing Cyber Threat Indicators and Defensive Measures Under the Act
Sections 1503(c)	Section 1505(b)(1)	• Sharing for a cybersecurity purpose. Section 1503(c) • Sharing cyber threat indicators & defensive measures. Section 1503(c) and 1505(b)(1) • Removal prior to sharing using a manual or technical means of information not directly related to a cybersecurity threat that the entity knows at the time of sharing to be personal information of a specific person or information identifying a specific person. Section 1503(d)(2)(A) and (B) • Implement and utilize a security control to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures. Section 1503(d)(1) • When receiving cyber threat indicators observe lawful restrictions placed by a non-Federal entity. Section 1503(c)(2)	• Liability protection for sharing and receiving cyber threat indicators or defensive measures. Section 1505(b) • Antitrust Exemption. Section 1503(e) * • Imposition of lawful restrictions on non-Federal entity on sharing and use of cyber threat indicators or defensive measures. Section 1503(c)(2)

* This protection applies only to private entities, not other non-Federal entities.

Annex 2: Cybersecurity Information Sharing Act of 2015 – Frequently Asked Questions

Since 2016, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) have received numerous questions regarding the implementation of the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the contents of the *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* (the Non-Federal Entity Sharing Guidance).[1] DHS and DOJ published responses to frequently asked questions (FAQs) in July 2017. In October 2020, DHS and DOJ issued an amended version of the Non-Federal Entity Sharing Guidance that included this updated FAQs document as an annex. This annex is intended to supplement and be read in conjunction with the Non-Federal Entity Sharing Guidance, which contains a more in-depth treatment of a number of topics, such as definitions of relevant terms, applying privacy protections required by CISA 2015, and methods of sharing with the DHS capability and process.[2]

1. Does CISA 2015 override Federal and state laws that prohibit or restrict voluntary disclosure or sharing of cyber threat indicators and defensive measures?

   Yes. CISA 2015 provides that, "*notwithstanding any other provision of law*, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure." Section 1503(c)(1) (emphasis added). Therefore, CISA 2015 plainly overrides any conflicting Federal criminal and civil laws.

   To be in conflict with CISA 2015, a Federal law would have to restrict or permit activities contrary to CISA 2015. In general, CISA 2015 authorizes the sharing of cyber threat indicators and defensive measures, subject to the following requirements:

   - information shared must meet the definition of a "cyber threat indicator" or a "defensive measure." Section 1503(c)(1). (See FAQ #7 for a discussion of "cyber threat indicators" and "defensive measures.");
   - sharing must be for a "cybersecurity purpose," defined to mean "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." Sections 1501(4), 1503(c)(1);
   - sharing must follow a review for and removal of any information that the sharer knows at the time of sharing to be personal information of a specific person or information that identifies a specific person that is not directly related to a cyber threat. Section 1503(d)(2); information must be protected through security controls to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures. Section 1503(d)(1); and
   - sharing must comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicators or defensive measures. Section 1503(c)(2).

[1] Consolidated Appropriations Act of 2016, P.L. 114-113, 129 Stat 2242, Division N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), P.L. 114–113, 129 Stat. 2936 (codified at 129 Stat. 2936, 6 U.S.C. §§ 1501-1510) (CISA 2015). For ease of reference, this document generally cites to the sections as codified in title 6 of the U.S. Code.

[2] Like the other CISA 2015 guidance documents published by DHS and DOJ, this document is intended as assistance, not authority. It has no regulatory effect, confers no rights or remedies, and does not have the force of law. *See United States v. Caceres*, 440 U.S. 741 (1979).

CISA 2015 also includes a provision preempting any statute or other provision of law of a state or political subdivision of a state that restricts or otherwise expressly regulates an activity that CISA 2015 authorizes. Section 1507(k)(1). Thus, CISA 2015's authorization for sharing cyber threat indicators and defensive measures overrides conflicting state civil and criminal laws. For example, to the extent that a state data privacy law restricts or otherwise expressly regulates an activity authorized by CISA 2015, CISA 2015 preempts such state law. And to the extent that the sharing of cyber threat indicators qualifies for liability protection, as explained in FAQs #2-5 below, CISA 2015 should protect such sharing from liability under any otherwise applicable state data privacy law.

2. Does CISA 2015 authorize a private entity to share cyber threat indicators and defensive measures with other private entities? Does CISA 2015 also provide liability protection for such private-to-private sharing?

   Yes, as long as the sharing is conducted in accordance with the requirements of CISA 2015. Section 1503(c) states that a non-Federal entity may, notwithstanding any other law, share with (or receive from) any other non-Federal entity a cyber threat indicator or defensive measure. CISA 2015 defines the term "non-Federal entity" to include private entities. Section 1501(14). Section 1505(b) protects any private entity from liability arising from sharing a cyber threat indicator or defensive measure in accordance with CISA 2015. This includes sharing a cyber threat indicator or defensive measure with (or receiving such information from) another private entity in accordance with the requirements for sharing under CISA 2015. Sections 1505(b) and (c); see also FAQ #1 for a discussion of the requirements. Sharing that does not meet those requirements is not eligible for the liability protection provided by section 1505.

3. Do CISA 2015's liability protections for private entities apply to sharing cyber threat indicators or defensive measures with Information Sharing and Analysis Organizations (ISAOs), including Information Sharing and Analysis Centers (ISACs)? Does the private entity lose liability protection if the ISAO or ISAC does not subsequently share that information with DHS? Does it lose liability protection if the ISAO or ISAC shares the information with DHS in a manner that does not comply with CISA 2015?

   CISA 2015's liability protections generally apply to sharing conducted with ISAOs and ISACs. As explained in FAQ #2, any private entity that shares cyber threat indicators or defensive measures with another non-Federal entity in accordance with CISA 2015 receives liability protection for that sharing under section 1505(b). Consequently, ISAOs and ISACs that meet the definition of a private entity (Section 1501(15)), or the broader definition of a non-Federal entity (Section 1501(14)), would qualify for protection, and private entities sharing information with ISAOs and ISACs in accordance with CISA 2015 would similarly receive liability protection. (See also Non-Federal Entity Sharing Guidance at 15). Such liability protection does not depend on whether the ISAO/ISAC subsequently shares the information with DHS. Should the ISAO or ISAC proceed to share a private entity's information with DHS in a manner contrary to CISA 2015, only the ISAO or ISAC would lose its liability protection; the private entity would retain its liability protection despite the ISAO/ISAC's actions.

4. I know that CISA 2015 provides a private entity with liability protection for sharing cyber threat

indicators and defensive measures with—or receiving such information from—DHS in accordance with CISA 2015, but can a private entity also receive liability protection for sharing cyber threat indicators and defensive measures with other Federal agencies, including law enforcement agencies?

Yes, so long as the sharing is conducted in a manner consistent with CISA 2015's information sharing authorization and section 1504(c)(1)(B). Section 1505(b) provides liability protection to a private entity "for the sharing or receipt of a cyber threat indicator or defensive measure under section 1503(c)," if such sharing is conducted consistent with CISA 2015. Section 1503(c) includes requirements for sharing under CISA 2015, including requirements for the removal of information known by the sharer to be personal information of a specific individual or information that identifies a specific individual that is not directly related to the cybersecurity threat. (See Non-Federal Entity Sharing Guidance at 7-9; see also FAQ #1 for the requirements for sharing under CISA 2015.)

To receive liability protection for sharing with the Federal Government, a private entity must share cyber threat indicators and defensive measures "in a manner that is consistent with section 1504(c)(1)(B)." Section 1505(b)(2). Private entities sharing information through the DHS capability and process receive liability protection under section 1505, provided that such sharing satisfies the requirements described in FAQ #1.[3] While the DHS capability and process serve as the principal means of sharing cyber threat indicators and defensive measures with the Federal Government consistent with section 1504(c)(1)(B), they are not the only means.

Section 1504 contains two exceptions that authorize sharing cyber threat indicators or defensive measures with Federal agencies other than through the DHS capability and process. Liability protection is available for private entities that share information directly with other Federal agencies under those provisions. The first exception, section 1504(c)(1)(B)(i), provides for sharing, consistent with section 1503, "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 cyber threat indicator." Sharing such information can therefore receive liability protection so long as the sharing is consistent with the other requirements in section 1505, including compliance with section 1503(c). For example, a company could receive liability protection for sharing a cyber threat indicator or defensive measure with DHS consistent with sections 1503(c) and 1505, and also receive liability protection for subsequently sharing with another Federal agency, including a law enforcement agency "communications . . . regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure." Section 1504(c)(1)(B)(i).

So, as discussed below in FAQ #6, CISA 2015 is not primarily designed to address sharing cyber threat information with law enforcement. However, CISA 2015 does provide liability protection for sharing cyber threat indicators or defensive measures with law enforcement, if the indicator or defensive measure is shared with law enforcement as part of a communication regarding a cyber threat indicator that was previously shared by the private entity through the DHS capability and

[3] As further detailed in the Non-Federal Entity Sharing Guidance, DHS operates the Federal Government's capability and process for receiving cyber threat indicators and defensive measures under CISA 2015 that are shared by a non-Federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems.

process, as described above.

Importantly, however, in order to receive liability protection, the information shared or received must fall within the statutory definitions of a "cyber threat indicator" and "defensive measure." Under section 1501(6) the information qualifies as a cyber threat indicator if it is "necessary to describe or identify" six categories of cyber threats, or "any other attribute of a cybersecurity threat, if disclosure is not otherwise prohibited by law," or any combination of the threats set out in the definition. Information that falls outside that definition would not receive liability protection.

Under the second exception, section 1504(c)(1)(B)(ii) provides for sharing "communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat." Thus, a non-Federal entity may receive liability protection for sharing a cyber threat indicator directly with its regulatory authority regarding a cybersecurity threat, whether or not a related cyber threat indicator was previously shared consistent with CISA 2015. Further, as discussed above, a company could receive liability protection under section 1504(c)(1)(B)(i) for sharing a cyber threat indicator with another Federal entity after sharing communications with its Federal regulatory authority.

5. What are the differences between the protections provided under section 1503 for cybersecurity monitoring and information sharing, and the liability protections provided under section 1505?

Section 1503 authorizes monitoring of information systems and information, and sharing cyber threat indicators and defensive measures, "notwithstanding any other provision of law," thereby overriding contrary Federal and state law. (See FAQ #1.) By clearly authorizing and protecting appropriate cybersecurity monitoring and information sharing, Congress intended to encourage those activities. As further incentive to conduct these activities, section 1505 provides explicit liability protections. Section 1505 requires that any cause of action brought in any court be promptly dismissed if the alleged conduct was monitoring or information sharing conducted in accordance with CISA 2015. Section 1505(a) applies to any cybersecurity monitoring conducted pursuant to section 1503(a). Section 1505(b)(1) shields any sharing conducted among private entities pursuant to section 1503(c). (See FAQ #2.) However, as discussed in FAQ #4, section 1505(b)(2) applies only to information sharing that a private entity conducts with the Federal Government in a manner consistent with section 1504(c)(1)(B). Taken together, sections 1503 and 1505 provide strong legal protection to cybersecurity monitoring and information sharing activities undertaken in accordance with CISA 2015.

6. Does CISA 2015 alter how non-Federal entities report information to Federal law enforcement? Must such reporting now be conducted through the DHS capability and process?

No. CISA 2015 does not require any change in reporting information to law enforcement. It is important to remember that CISA 2015 does not interfere in any way with voluntary or legally compelled participation with a Federal agency's investigation of a cybersecurity incident. Non-Federal entities routinely share cyber threat information with Federal investigators; nothing in CISA 2015 prevents or otherwise affects those activities, which the Federal Government encourages.

Sharing cyber threat information with law enforcement generally does not raise liability issues, particularly in the context of reporting an actual or attempted crime. Moreover, CISA 2015 provides that the DHS capability and process "does not limit or prohibit otherwise lawful disclosures of communications, records or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or a Federal entity [that] includ[es] cyber threat indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation." Section 1504(c)(1)(E). More broadly, CISA 2015 specifies that nothing in the statute should be "construed … to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government under this subchapter; or … to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this subchapter." Section 1507(a)(1)-(2). In short, CISA 2015 supplements—but does not supplant—other measures that already protect private entities that report crimes, including restrictions on disclosing investigative material.

7. What are some additional examples of information that fall within CISA 2015' definitions of a "cyber threat indicator" or "defensive measure" and that may be shared under CISA 2015?

CISA 2015 defines a "cyber threat indicator" as "information that is necessary to describe or identify: (A) 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; (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (D) 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; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof." Section 1501(6).

CISA 2015 defines a "defensive measure" as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability." Section 1501(7)(A). However, CISA 2015 explicitly excludes from the definition of defensive measure "a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—(i) the private entity operating the measure; or (ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure." Section 1501(7)(B).

CISA 2015's definitions of cyber threat indicators and defensive measures reflect categories of information used to protect and safeguard computer networks while assessing a threat, tracing the threat across the user's network and other networks, and mitigating and assessing harm. These definitions also include categories of information that may be useful to law enforcement.

The Non-Federal Entity Sharing Guidance issued in June 2016 and amended in October 2020 provides examples of cyber threat indicators and defensive measures shareable under CISA 2015. Some additional examples include:

1. malware;
2. information regarding the intrusion vector and method of establishing persistent presence;
3. information regarding when unauthorized access occurred;
4. information regarding how the actor moved laterally within a network and how network protections were bypassed;
5. information regarding the type of servers, directories, and files that were accessed;
6. information regarding what was exfiltrated and the method of exfiltration; and
7. information regarding the damage or loss caused by the incident, including remediation costs.

In addition to being authorized for sharing under section 1503(c), these categories of information fall within CISA 2015's liability protections when shared in accordance with CISA 2015. See FAQ #1. Thus, liability protection would apply when sharing occurs among non-Federal entities, Section 1505(b)(1), and between a non-Federal entity and a Federal entity, when conducted in accordance with section 1504(c)(1)(B). Sections 1503(d)(2), 1504(c)(1)(B) and 1505(b)(2).

8. Must all "personal information" be removed from cyber threat indicators or defensive measures before they may be shared in accordance with CISA 2015?

No. CISA 2015 does not require that all personal information be removed, only information not directly related to a cybersecurity threat that the entity knows at the time of sharing to be either personal information of a specific individual or information that identifies a specific individual. Section 1503(d)(2). So, information that is directly related to a cybersecurity threat, even if it is information that the sharer knows to be personal information of a specific individual or information that identifies a specific individual, may be shared in accordance with CISA 2015. However, failure to remove information that the sharer knows to be personal information of a specific individual or information that identifies a specific individual, and which is not directly related to a cybersecurity threat before cyber threat indicators or defensive measures are shared would forfeit CISA 2015's liability protection as well as the other protections that apply to sharing conducted in accordance with CISA 2015. The review for such information may be conducted using either a manual process or technical capability. *Id.*

Examples of the types of information that typically may require removal prior to sharing are provided in the Non-Federal Entity Sharing Guidance and the Privacy and Civil Liberties Guidelines.

9. Does CISA 2015 impose criminal or civil liability if cyber threat indicators or defensive measures are shared inconsistent with CISA 2015?

No. CISA 2015 does not provide a civil cause of action or impose criminal liability for activities that are conducted inconsistent with the statute. However, sharing that is inconsistent with CISA 2015's requirements for sharing (see FAQ #1) would not receive liability protection under CISA 2015. See FAQs #1 and #5. It is also noteworthy that section 1505(c) provides that CISA 2015 does not create a duty to share a cyber threat indicator or defensive measure, a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure, or undermine or limit the availability of otherwise applicable common law or statutory defenses.

10. Do private or governmental entities that were lawfully sharing information with each other before CISA 2015's enactment need to alter their practices now that CISA 2015 has been passed?

No. Private or governmental entities that were lawfully sharing information before CISA 2015 was enacted do not need to alter their practices in the wake of CISA 2015's passage. CISA 2015 is not intended to affect sharing that has occurred or currently occurs outside of the statute. Section 1507(a) explicitly provides that CISA 2015 does not limit or prohibit otherwise lawful sharing of information among private or governmental entities. Section 1507(f) further provides that CISA 2015 does not limit or modify existing information sharing relationships or require the creation of new ones. In other words, CISA 2015 does not displace other avenues of information sharing. Instead, it provides congressionally authorized pathways for information sharing that offer unique advantages—including liability protection—to those who use them.

11. Can I satisfy a Federal regulatory requirement concerning the reporting of cyber incidents by submitting information through DHS's Automated Indicator Sharing (AIS) initiative?

No. AIS is intended to facilitate the voluntary exchange of cyber threat indicators and defensive measures for cybersecurity purposes, not to satisfy regulatory requirements. DHS's AIS is not configured to receive information that provides the level of detail regarding cyber incidents that regulators typically require. It enables entities to share cyber threat indicators and defensive measures with the Federal Government using a standard set of fields that do not allow other data elements to be submitted. Consequently, sharing through AIS typically does not satisfy Federal regulatory requirements concerning the reporting of cyber incidents. Regulatory reporting should be conducted in accordance with the requirements and method of submission specified by regulators.

12. Does CISA 2015 provide any protection against claims that sharing cyber threat indicators and defensive measures violates antitrust laws?

Yes. CISA 2015 provides that activity authorized by CISA 2015 does not violate Federal and state antitrust laws, including provisions of the Clayton Act (15 U.S.C. § 12), the Federal Trade Commission Act (15 U.S.C. § 45), and state laws consistent with or modeled on those laws. Section 1503(e). CISA 2015's antitrust protections apply to information exchanged or assistance provided to assist with: (1) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or (2) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system. *Id*. Nevertheless, CISA 2015 does not

authorize price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning. Section 1507(e).

CISA 2015's antitrust protections augment the policy statement issued by the Department of Justice's Antitrust Division and the Federal Trade Commission in May 2014 explaining that "a properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns." Policy Statement at 1, *available at* http://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf.

13. Are cyber threat indicators and defensive measures shared with the government under CISA 2015 exempt from disclosure under the Freedom of Information Act or other Federal or state "sunshine laws"?

Yes. CISA 2015 provides that cyber threat indicators or defensive measures shared with the Federal Government under CISA 2015 are exempt from disclosure under the Freedom of Information Act. Section 1504(d)(3). CISA 2015 further provides that cyber threat indicators or defensive measures shared with a Federal, state, tribal, or local government under CISA 2015 are also exempt from disclosure under any state, local, or tribal "sunshine law" or similar law requiring disclosure of information or records. Sections 1503(d)(4)(B) and 1504(d)(3).

14. What is the scope of CISA 2015's protection against a waiver of privilege for sharing cyber threat indicators and defensive measures with the Federal Government? Does it cover common law privileges?

CISA 2015's protection against a waiver of privilege is broad and covers common law privileges. CISA 2015 provides that "[t]he provision of cyber threat indicators and defensive measures to the Federal Government under this subtitle shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection." Section 1504(d)(1). CISA 2015's privilege protections apply to cyber threat indicators and defensive measures shared in accordance with CISA 2015, including the requirements identified in FAQ #1.

Because the waiver provision reaches "any applicable privilege or protection," it applies in all circumstances where state or Federal privileges and protections may be invoked, to the extent a claim of waiver is based on disclosure of the information to the Federal Government. This includes protections recognized under common law, such as the attorney-client and work product privileges.

15. Can a regulator bring a regulatory action against a private entity based upon cyber threat indicators or defensive measures that the entity has shared with the government pursuant to CISA 2015?

Generally, no. With one exception, CISA 2015 prohibits any Federal, state, tribal, or local government from using cyber threat indicators or defensive measures provided to the Federal Government under CISA 2015 to regulate the lawful activities of any non-Federal entity. Section 1504(d)(5)(D). CISA 2015 explicitly prohibits the Federal Government and any state, tribal or local

government from using such information in an enforcement action against a non-Federal entity. *Id*. This protection extends to enforcement actions in connection with activities undertaken by a non-Federal entity pursuant to mandatory standards, including those related to monitoring information systems, operating defensive measures, or sharing cyber threat indicators.

This prohibition contains an exception, however, that allows the limited use of such information pursuant to regulatory authority "specifically relating to the prevention or mitigation of cybersecurity threats to information systems." In such circumstances, the information can be used to inform the development or implementation of regulations relating to information systems. Section 1504(d)(5)(D)(ii)(I). These same exceptions (and the aforementioned restrictions) apply to the use by state, tribal, or local regulators of information shared with a state, tribal or local government. Section 1503(d)(4)(C).

16. Does CISA 2015's provision authorizing the application of defensive measures permit "hacking back"?

No. As Congress explained in its Joint Explanatory Statement on CISA 2015, the statute does not authorize a private entity to "hack back." Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015, p. 2. CISA 2015's defensive measures authorization "does not include activities that are generally considered 'offensive' in nature, such as unauthorized access of, or execution of computer code on, another entity's information systems, such as 'hacking back' activities." *Id.* Instead, CISA 2015 authorizes a private entity to apply a "defensive measure" (1) to its own information system for cybersecurity purposes to protect its rights or property; or (2) to another entity's information system, with that entity's written consent, to protect that entity's rights or property. Section 1503(b). The definition of a defensive measure expressly excludes any activity that would violate the Computer Fraud and Abuse Act. Specifically, the definition excludes activity that "destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting an information system not owned [by that private entity]." Section 1501(7)(B).

17. How do CISA 2015's protections apply to sharing of cyber threat indicators and defensive measures by or with state, local, or tribal government entities?

With one exception, state, tribal, and local governments (as well as U.S. territories) are eligible to receive all of CISA 2015's protections for sharing cyber threat indicators and defensive measures in accordance with CISA 2015. State, tribal, and local governmental entities, however, generally cannot invoke CISA 2015's liability protections for sharing conducted pursuant to CISA 2015 because liability protection under section 1505 is only available to "private entities." But state, tribal, and local governmental entities that provide utility services may invoke liability protection, because CISA 2015's definition of private entities includes governmental entities that provide such services. Section 1501(15)(B). The protections available for sharing information *with* any state, local, or tribal government are unaffected by this limitation.

State, local, tribal, and territorial governments also receive a unique disclosure protection under CISA 2015. Cyber threat indicators or defensive measures shared by or with a state, local, tribal, or territorial governmental entity are exempt from disclosure under any provision of "State, tribal, or

local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records." Section 1503(d)(4)(B)(ii).[4] The state, local, tribal, or territorial governmental entity holds the responsibility and discretion for asserting this basis for withholding in response to any such requests under their own applicable state, local, tribal or territorial freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

18. How do CISA 2015's protections apply to sharing by or with foreign governments or corporations?

    CISA 2015 does not protect or authorize sharing by or with a "foreign power," as defined in section 1801 of Title 50, U.S. Code. CISA 2015 authorizes a "non-Federal entity" to share and receive cyber threat indicators and defensive measures, but defines a non-Federal entity to exclude foreign powers. Sections 1501(14)(C) and 1501(15)(C). A "Federal entity may receive such information from a non-Federal entity," but a Federal entity is limited to a United States department or agency or component thereof and, therefore, also excludes a foreign power. Section 1501(8). CISA 2015's protections are available, however, for sharing by or with foreign corporations that do not fall within the definition of a foreign power.

    CISA 2015 does not limit or modify any existing information sharing relationship or prohibit any new information sharing relationship, including with foreign governments. Section 1507(f). Thus, otherwise lawful sharing with a foreign government is not affected by CISA 2015, although such sharing would not be undertaken pursuant to CISA 2015 and, thus, would not benefit from CISA 2015's protections. Nonetheless, foreign governments may share with the Federal Government using the same mechanisms provided by CISA 2015, including through the DHS capability and process.

19. Before CISA 2015's enactment, my organization routinely emailed cyber threat indicators to DHS's Cybersecurity and Infrastructure Security Agency (CISA) or uploaded them to CISA using online forms. Do we need to follow a different procedure now to obtain CISA 2015 protections?

    No. CISA 2015 does not require the use of a specific submission pathway. Entities that wish to benefit from CISA 2015's protections must comply with CISA 2015's requirements as outlined in FAQ #1; but cyber threat indicators that are shared with DHS's CISA using automated machine-to-machine sharing, uploaded via a web form, or shared by email or electronic media are considered to have been shared in accordance with CISA 2015, and thus are eligible for CISA 2015's protections, including protection from liability. No specific language must be used (for example in an email) to invoke CISA 2015 protections.

20. What notification requirements apply to Federal entities if personal information that is not directly related to a cybersecurity threat is erroneously shared under CISA 2015?

[4] Similar protections from state, local, or tribal disclosure laws are afforded to information shared by or with the Federal Government. Section 1504(d)(3).

CISA 2015 requires Federal entities to conduct such notifications. The Privacy and Civil Liberties Guidelines provide guidance for the following scenarios:

- "Federal entities must notify, in a timely manner, other Federal entities and non-Federal entities that have received a cyber threat indicator or defensive measure from a Federal entity under [CISA 2015] that is known or determined to be in error or in contravention of the requirements of [CISA 2015] or another provision of Federal law or policy of such error or contravention." Section 1502(b)(1)(C)
- Federal entities must notify non-Federal entities and Federal entities "if information received pursuant to [CISA 2015] is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator." Section 1504(b)(3)(E)
- Federal entities must notify, in a timely manner, "any United States Person whose personal information is known or determined to have been shared in violation of [CISA 2015]". Section 1502(b)(1)(F). The Privacy and Civil Liberties Guidelines provide guidance to Federal entities to follow their own breach/incident response plan.

21. What are some additional examples of contextual information that can be shared as part of a cyber threat indicator or defensive measure under CISA 2015?

    As explained in the Non-Federal Entity Guidance, CISA 2015 permits contextual information to be shared as a cyber threat indicator or defensive measure when it is necessary to describe or identify a cybersecurity threat or security vulnerability. See Non-Federal Entity Sharing Guidance at 5. The following are specific scenarios in which a non-Federal entity could share information with Federal entities under CISA 2015 because it identifies contextual information that satisfies CISA 2015's definitions of cyber threat information or defensive measures. These examples presume that the sharing is conducted, in accordance with CISA 2015, as described above and in FAQ #1.

    - A company that describes a malicious technique that was used to access its network could share information regarding associated tactics, techniques and procedures used by the same actors as part of a campaign of related activity.
    - When sharing anomalous user behavior information that appears to indicate malicious activity such as login attempts from a Virtual Private Server system at times/IP addresses unusual for a particular user, a company could provide examples of normal behavior alongside the abnormal for adequate context.
    - A cyber defense team could share a defensive measure to block Secure Sockets Layer traffic showing a particular pattern of behavior associated with a cybersecurity threat, including additional information regarding how to detect and avoid blocking false positives, such as those generated by other security appliances that exhibit a similar pattern of behavior to the cybersecurity threat.
    - An organization sharing a defensive measure to block malicious traffic from a particular port could include an explanation that legitimate Virtual Private Network traffic may randomly be placed on that port.

22. What types of information related to industrial control systems, which appear to be impacted by malicious cyber activity but the cause has not yet been identified, may be shared as a cyber threat indicator under CISA 2015?

There are many examples of information related to industrial control systems (ICS) that can be shared pursuant to CISA 2015. As explained in the Non-Federal Entity Guidance, CISA 2015 permits information to be shared as a cyber threat indicator or defensive measure when it is necessary to describe or identify a cybersecurity threat or security vulnerability to an industrial control system. See Non-Federal Entity Sharing Guidance at 3-5. For example, IP addresses, unauthorized commands sent to an industrial control system, unexpected communications traffic, unexpected and unexplained industrial control system events, data reflecting operating conditions, device log entries, potential or actual harm to a system or operations, or some combination of this information may be shared under CISA 2015 as a cyber threat indicator or defensive measure,[5] assuming the activity appears to be associated with a cybersecurity threat,[6] and if information known to be personal information or information identifying a specific individual that is not directly related to a cybersecurity threat has been removed prior to sharing.[7]

In particular, anomalous events may provide necessary contextual information that describes or identifies a cybersecurity threat or security vulnerability in an industrial control system. CISA 2015 expressly contemplated that anomalous activity could be shared in specified circumstances. See Sections 1501(6)(A) and (C). Information that may be shared as cyber threat indicators as described above could include the following activities when they appear to be unauthorized conduct, tied to a cybersecurity threat: login attempts; network or system access; identification of software on a device or network, network accessible ports, network devices, enabled ports, services, or wireless signals; unusual software updates; and other system anomalous behaviors indicative of malicious conduct (e.g., process, computer, and/or network system behavior).

The following are specific scenarios in which a non-Federal entity could share information with DHS or other Federal entities under CISA 2015 because these scenarios identify potentially important contextual information, such as anomalous activity related to an industrial control system. These examples presume that the sharing is conducted, in accordance with CISA 2015, as described above and in FAQ #1.

1. A company could share information reflecting a pattern of unauthorized remote login attempts to an industrial control system network.
2. A company could share its access control log entries that show a particular IP address has gained unauthorized access to a network used by an industrial control system.
3. A company could share an unauthorized IP address that has been observed to be sending commands to an industrial control system. In addition, the company could share the commands sent to and the effect of the command on the industrial control system.
4. A municipal utility could share information about unexpected communications traffic that it detects from an industrial control system (e.g., amount of traffic, source or destination for communications).

[5] See sections 1501(6) and (7).
[6] See sections 1501(4) and (5).
[7] See FAQ #1 and #7 for more information on appropriate sharing parameters.

5. A company could share its alarm log entries for an unexpected and unexplained industrial control system event that appears to be caused by a security vulnerability that, if not remediated, could adversely impact the availability or integrity of the system.
6. A company could share data reflecting the operating conditions, device log entries, and associated communications traffic from an industrial control system that fails before it is expected to if the company suspects that the failure was caused by or associated with an exploitation of a security vulnerability.
7. A company could share the actual or potential harm to an industrial control system or operations caused by a cybersecurity incident originating outside or inside an industrial control system.
8. A company could share the actual or potential harm caused by an anomalous pattern of operation of a programmable logic controller that appears to be related to a cybersecurity threat.
9. An information sharing and analysis center could share information about an irregular, potentially harmful response pattern of a particular programmable logic controller under specific conditions reported by multiple companies that appears to reflect the existence of a security vulnerability as a way of warning other companies with similar assets.

23. What are the next steps for an interested company to sign up for DHS's AIS initiative and obtain more information?

    Companies interested in participating in AIS should sign the AIS Terms of Use (ToU), which can be found via https://www.cisa.gov/automated-indicator-sharing-ais and return to cyberservices@cisa.dhs.gov. Once the signed ToU is returned, DHS CISA staff will reach out with all the information necessary to establish a direct connection to the CISA server. CISA will also conduct conference calls or webinars with companies that have questions about the on-boarding requirements or receiving, using, or sharing machine-readable indicators and defensive measures.

24. Can a non-Federal entity also share CISA 2015-covered information through CISA's Protected Critical Infrastructure Information (PCII) program? How do PCII protections interact with the protections afforded by CISA 2015?

    Yes, both statutory regimes (and associated programs) can be utilized simultaneously. Submissions of information to either program would need to fulfill each program's unique requirements in order for the respective program's protections to apply. While PCII and CISA 2015 offer some overlapping protections, such as protections against disclosure (see sections 1504(d)(3) and 1504(d)(4)(B) (CISA 2015) and 6 U.S.C. § 673(a)(1)(A) (PCII)) and a prohibition on certain regulatory uses of submissions (see sections 1504(d)(5)(D) and 1503(d)(4)(C) (CISA 2015) and 6 U.S.C. § 673(a)(1)(B) (PCII)), there are some protections that are unique to each program. For example, in section 1505, CISA 2015 provides liability protection for the sharing, provided that sharing is otherwise conducted in accordance with CISA 2015's requirements. The PCII Program, while not addressing protection from liability, protects PCII from being used directly in any civil action absent the consent of the submitter. 6 U.S.C. § 673(a)(1)(C). For more information regarding the PCII Program, the protections it offers, and how to submit critical infrastructure information for validation as PCII, please visit https://www.cisa.gov/pcii-program.