



**The Department of Homeland Security**
**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

**February 16, 2016**

# Table of Contents

On December 18, 2015, Congress passed and President Obama signed into law the Cybersecurity Act of 2015. Title I of the Cybersecurity Act, entitled the Cybersecurity Information Sharing Act (CISA or the Act), provides increased authority for cybersecurity information sharing between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government. Section 105(a)(4) of the Act directs 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. Accordingly, this document provides information that will assist non-federal entities who elect to share cyber threat indicators with the Federal Government to do so in accordance with the Act.[1] It will also assist non-federal entities to identify defensive measures and explain how to share them with federal entities[2] as provided by CISA. Lastly, it describes the protections non-federal entities receive under CISA for sharing cyber threat indicators and defensive measures in accordance with the Act, including targeted liability protection and other statutory protections.[3]

## 1. Scope of Guidance

As required by Section 105(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.[4]

It also explains how to identify and share defensive measures, even though section 105(a)(4) does not require the guidance to do so.[5]

---

[1] This document does not provide guidance on reporting crimes to law enforcement. See section II for a discussion of sharing information for law enforcement, regulatory, and other purposes.

[2] Pursuant to CISA, "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 102(14)(A)-(C).

[3] This document focuses on providing guidance to non-federal entities concerning how they may properly share cyber threat indicators with the government pursuant to CISA. 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 Interim Guidance at https://www.us-cert.gov/ais.

[4] 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.

[5] Although section 105(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 104(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.

In addition to covering how to identify and share cyber threat indicators and defensive measures, this guidance also explains how to share that information with federal entities through the Federal Government's capability and process that is operated by DHS (See section 2.B.) This guidance also explains how to share such information 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 (See sections 2.C. and 3).

## a. Key Concepts

The Act authorizes sharing of specific information that is used to protect information systems and information. Section 104(c) allows non-federal entities to share cyber threat indicators and defensive measures with any other entity—private, federal, state, local, territorial, or tribal—for a "cybersecurity purpose." The Act defines a "cybersecurity purpose" 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. Section 102(4). The terms "cyber threat indicator" and "defensive measure" also have specific meanings under the Act. These key concepts and associated terms are discussed below.

### i. Cyber Threat Indicator

The Act 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 gathering technical information related to a cybersecurity threat or security vulnerability; [6]
- A method of defeating a security control or exploitation of a security vulnerability;

[6] 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 under section 102(5) 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.

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 are not cybersecurity threats under CISA.

The definition of a cybersecurity threat includes activities that may have unauthorized and negative 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 by section 102(17) 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.

- 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.[7]

The Act promotes the goal of sharing while simultaneously providing privacy protections in two ways: first, by specifying the types of cyber threat information that can be shared under the Act between and among non-federal and federal entities; and, second, by limiting sharing under the Act only to those circumstances in which such information is necessary to describe or identify threats to information and information systems. Effectively, the only information that can be shared under the Act is information that is directly related to and necessary to identify or describe a cybersecurity threat.

Information is not directly related to a cybersecurity threat if it is not necessary to assist others detect, prevent, or mitigate the cybersecurity threat. For example, a cyber threat indicator could be centered on a spear phishing email. For a phishing email, personal information about the sender of email ("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, could be considered directly related to a cybersecurity threat. The name and e-mail address of the targets of the email (i.e., the "To" address), however, would be personal information not directly related to a cybersecurity threat and therefore should not typically be included as part of the cyber threat indicator.

The following are additional examples of information that would contain cyber threat indicators that a private entity could submit to DHS and other federal entities under CISA:

- A company could report that its web server log files show that a particular IP address has sent web traffic that appears to be testing whether the company's content management system has not been updated to patch a recent vulnerability.
- A security researcher could report on her discovery of a technique that permits unauthorized access to an industrial control system.
- A software publisher could report a vulnerability it has discovered in its software.
- A managed security service company could report a pattern of domain name lookups that it believes correspond to malware infection.

[7] Section 102(6).

- A manufacturer could report unexecuted malware found on its network.
- A researcher could report on 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 report the IP addresses that are sending malicious traffic.

To help ensure consistency with CISA's definitions and requirements, standardized fields in structured formats can be used to establish a profile that limits the type of information in a cyber threat indicator. Much of the information within an indicator is centered on an observable fact about the cyber threat. For example, a cyber threat indicator has a variety of 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 content or information inappropriate to share. DHS's AIS initiative uses this means of controlling the type of information that may be shared using the automated system discussed in section 2.B.1.

### ii. Defensive Measure

The Act 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.

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 using sophisticated software tools to detect and protect against anomalous and unauthorized activities on a company's information system.

Similar to a cyber threat indicator, a defensive measure under the Act typically will not include personal information of a specific individual or information that identifies a specific individual. Instead, it will generally consist principally of technical information that can be used to detect and counter a cybersecurity threat.[8] However, personal information of a specific individual or

[8] When developing and implementing defensive measures pursuant to section 104(b), due diligence should be exercised to ensure that they do not unlawfully access or damage information systems or data. CISA's definition of

information that identifies a specific individual may occasionally be necessary to describe a cybersecurity threat, as is also true of a cyber threat indicator. For example, a signature or technique for protecting against targeted exploits such as spear phishing may include a specific email address from which malicious emails are being sent.

Some examples of defensive measures include but are not limited to:

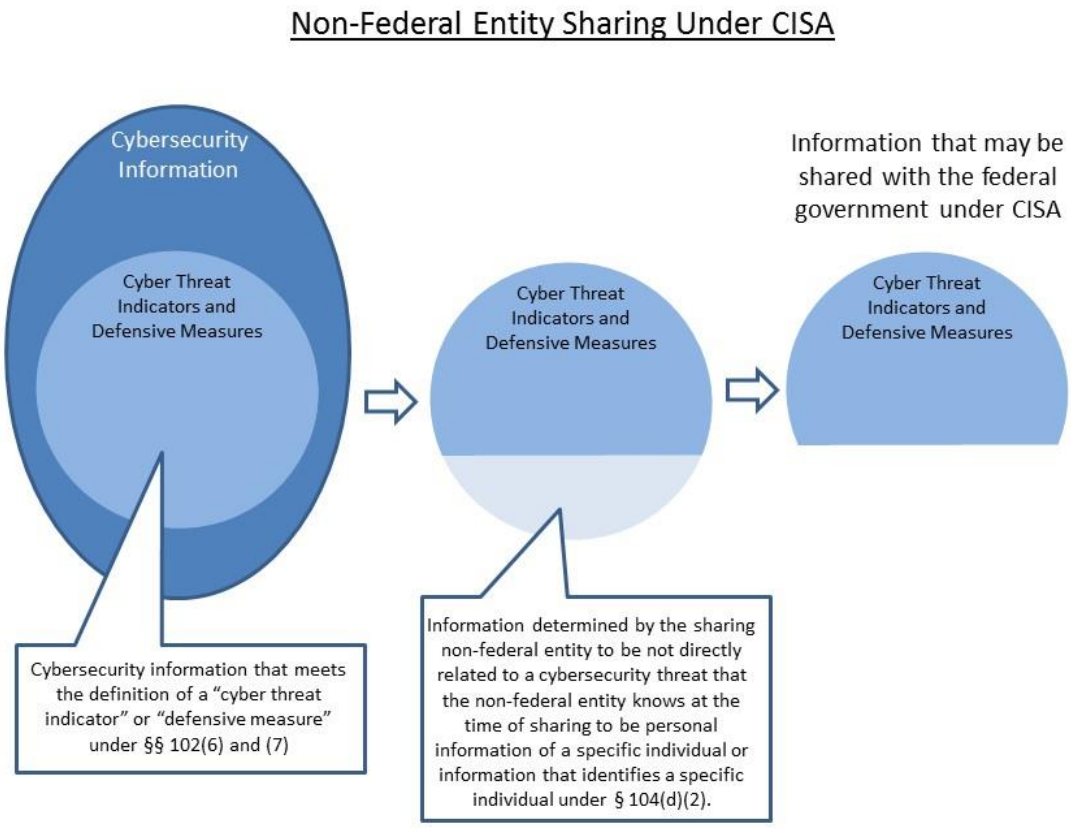
- A computer program that identifies a pattern of malicious activity in web traffic flowing into an organization.
- A signature that could be loaded into a company's intrusion detection system in order to detect a spear phishing campaign with particular characteristics.
- A firewall rule that disallows 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.

### iii. Information Protected under Otherwise Applicable Privacy Laws that are Unlikely to be Directly Related to a Cybersecurity Threat

Under CISA, a non-federal entity may share a cyber threat indicator or defensive measure for a cybersecurity purpose "notwithstanding any other provision of law," but to safeguard privacy while also promoting information sharing, CISA requires a non-federal entity to remove any information from a cyber threat indicator or defensive measure that it knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat before sharing it with a federal entity. Section 104(d)(2). Yet, some of the categories of information below may be used in connection with a cybersecurity threat, such as social engineering attacks and may, therefore, be shareable as part of a cyber threat indicator or defensive measure. Even so, sharing them in a form that constitutes personal information of a specific individual or information that identifies a specific individual may not be necessary. For instance, while sharing the health condition of a particular individual targeted for a phishing attack is unlikely to be useful or directly related to a cybersecurity threat, sharing an anonymized characterization of the cyber threat may have utility.

---

and authorization to use a defensive measure (sections 102(7) and 104(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, p. 2, available at http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/JES%20for%20Cybersecurity%20Act%20of%202015.pdf. 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.




To assist in this task, section 105(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 which typically need not include various categories of information that are considered sensitive and, therefore, protected by privacy laws. Information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat falling into this category of protected information may include:[9]

- Protected Health Information (PHI) which is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45 CFR 160.103). PHI is information, including demographic information, which relates to:
    - the individual's past, present, or future physical or mental health or condition,
    - the provision of health care to the individual, or

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

- 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 is information contained within an employee's personnel file, such as hiring decisions, performance reviews, and disciplinary actions.

- Consumer Information/History may include information related to an individual's purchases, preferences, complaints and even credit. The Fair Credit Reporting Act (FCRA) 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 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 CFR 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 constitutes a vast category of information, which 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 require financial institutions – companies that offer consumers financial 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. Although some information about property ownership may be publicly available, such as property purchase records, other information such as Vehicle Identification Numbers are inherently more sensitive and typically governed by state laws.

- Identifying Information of children under the age of 13. The Children's Online Privacy Protection Act (COPPA) 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 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.

## 2. 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 104(c), and specifically through the Federal Government's capability and process for receiving cyber threat indicators and defensive measures under the Act, which is operated by DHS pursuant to section 105(c). The manner in which information is shared affects the protections private entities receive for sharing cyber threat indicators and defensive measures. Sharing conducted pursuant to section 104(c) using the DHS capability and process provided by section 105(c) receives liability protection under section 106, as well as other specified protections. However, sharing conducted in any other manner pursuant to section 104(c) with any federal entity does not receive liability protection under the Act, but does receive all of the other protections available under the Act. Sharing that is not conducted in accordance with the Act is not eligible for the Act's protections.

The Act only authorizes information sharing for a cybersecurity purpose.[10] It does not limit or modify any existing information sharing 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 105(c). Section 108(f).

Sharing conducted through the means discussed in this guidance that is conducted pursuant to CISA should not be construed to satisfy any statutory, regulatory, or contractual obligation. It is not a substitute for reporting other types of information to federal entities, such as known or suspected cybercrimes directly to appropriate law enforcement agencies, known or suspected cyber incidents directly to the National Cybersecurity and Communications Integration Center, or required reporting to regulatory entities. The sharing addressed in this guidance is intended to complement, not replace, the prompt reporting of 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

Under the Act, a non-federal entity must 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 identifies a specific individual and remove such information. Section 104(d)(2)(A). While not explicitly required by the Act, non-federal entities are encouraged to conduct a similar review prior to sharing defensive measures under the Act. A defensive measure may contain a cyber threat indicator. Consequently, even though CISA may

[10] CISA also does not prohibit or permit the sharing of information for any purpose other than a cybersecurity purpose. Sharing for any other purpose is governed by other legal authorities.

not require the removal of personal information for a defensive measure under section 104(d)(2)(A), removal may nevertheless be required for information within the defensive measure that is also a cyber threat indicator.

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. A non-federal entity may conduct its review for such information using either a manual or technical process; either is permissible under CISA. Section 104(d)(2)(A) and (B).[11]

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

Section 105(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 DHS will in turn relay that information to federal entities in an automated manner,[12] as required by the Act and consistent with the operational and privacy and civil liberties policies instituted under sections 105(a) and (b).[13] Upon certification by the Secretary of Homeland Security in accordance with section 105(c), the DHS capability and process shall be 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 only specific exceptions.[14]

Provided that sharing is conducted in accordance with the Act, sharing conducted using this DHS capability will receive liability protection under section 106. It will also receive the other protections provided by the Act discussed more fully below in section III. 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. Section 105(c)(1)(e). It also does not limit or prohibit voluntary or legally compelled participation a federal law enforcement investigation or affect the provision of cyber

---

[11] Although not directly relevant to this guidance on information sharing between non-federal and federal entities, non-federal entities should remain mindful that CISA requires non-federal entities to implement and utilize a security control to protect against unauthorized access to or acquisition of shared cyber threat indicator or defensive measure. Section 104(d)(1).

[12] Section 105(a)(3)(A) requires DHS to disseminate cyber threat indicators and defensive measures shared with DHS pursuant to section 105(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 105(a)(3)(A)(i).

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

[14] Section 105(c)(1)(B) provides the following exceptions:

> (i) consistent with section 104 of the Act, 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; and
> (ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat.

threat indicators or defensive measures as part of a contractual requirement. Section 105(a)(1)(E).

Non-federal entities may share cyber threat indicators and defensive measures through the DHS capability and process created under section 105(c) via the AIS initiative, web form, email, or other information sharing programs that use these means of receiving cyber threat indicators or defensive measures. 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 the Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), respectively. By using standardized fields (STIX) and communication (TAXII), DHS enables organizations to share structured cyber threat information in a secure and automated manner.

In order 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 share its identity as the source of the cyber threat indicator submission.

For more information on AIS, visit the AIS web page at https://www.us-cert.gov/ais.

### ii. Web Form

Non-federal entities may share cyber threat indicators and defensive measures with DHS by filling out a web form on a DHS National Cybersecurity and Communications Integration Center website (including us-cert.gov). For more information, non-federal entities may visit the web page at https://www.us-cert.gov/ais.

### iii. Email

Non-federal entities may share cyber threat indicators and defensive measures with DHS by sending an email to DHS. For more information, non-federal entities may visit the web page at https://www.us-cert.gov/ais.

#### iv. Information Sharing and Analysis Organizations and Centers

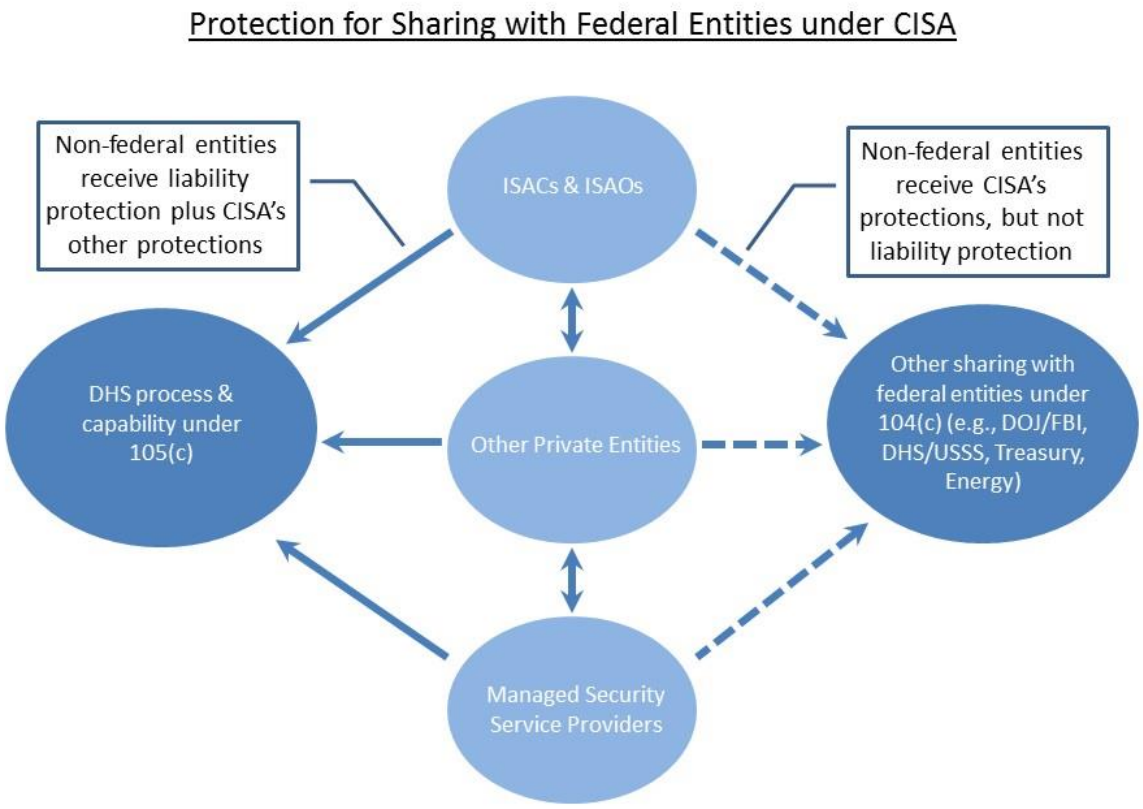
Non-federal entities may also share cyber threat indicators and defensive measures with federal entities through Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations, which will share them with federal entities through DHS on their behalf. Non-federal entities that share a cyber threat indicator or defensive measure with an Information Sharing and Analysis Center or Information Sharing and Analysis Organization—or any other non-federal entity—in accordance with the Act's requirements receive liability protection for such sharing under section 106(b) of the Act. See Section 106(b)(1).

### c. Non-Federal Entities Sharing with Federal Entities through other Means

Consistent with CISA, 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 B.1 through 4 above. Section 104(c) authorizes a non-federal entity to share cyber threat indicators with a federal entity—or any non-federal entity—so long as sharing is conducted for a cybersecurity purpose. However, as noted below, the protection from liability of Section 106(b)(1) does not attach.

## 3. Protections Received by Sharing Entities

The Act both provides certain protection to sharing entities and protects information shared in accordance with the Act. Section 106 extends liability protection to private entities for sharing of a cyber threat indicator or defensive measure conducted through the Federal government's capability and process operated by DHS under section 105(c), provided that sharing is conducted in accordance with the Act. Sharing through other means does not receive liability protection under the Act; 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 105(c).




Other than liability protection, CISA provides the following protections for sharing cyber threat indicators and defensive measures with any federal entity conducted pursuant to section 104(c):

- Antitrust Exemption: The Act provides a statutory exemption to federal antitrust laws that 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.[15] Section 104(e). However, the Act also expressly prohibits conduct that would otherwise constitute an antitrust violation, notwithstanding the exception provided by section 104(e)(1) to prevent this exception from being used as the basis for committing antitrust violations under the guise of cybersecurity information sharing. Section 108(e).

- Exemption from federal and state disclosure laws: The Act provides an exemption from federal state, tribal, or local government freedom of information law, open government

[15] 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 .

law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. Section 104(d)(4)(B); section 105(d)(3). Shared information is also deemed "voluntarily shared," which assists in protecting appropriately shared information from disclosure under The Critical Infrastructure Information Act of 2002.

- Exemption from certain state and federal regulatory uses: Cyber threat indicators and defensive measures shared under the Act shall not be used by any state, tribal, or local government to regulate, including 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 systems. CISA'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. Section 104(d)(4)(C); section 105(d)(5)(D).

- 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. Section 105(d)(1).

- Treatment of 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. Section 105(d)(2).

- Ex parte communications waiver: Under the Act, the sharing of cyber threat indicators and defensive measures 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. Section 105(d)(4).

| Sharing Cyber Threat Indicators and Defensive Measures with a Federal Entity | | | | |
|---|---|---|---|---|
| Means of Sharing | Authority for Sharing | Receiving Federal Entity | Requirements | Protections Conferred for Sharing Under the Act |
| DHS Capability and Associated Programs | Sections 104(c) and 106(b) | DHS | • Removal prior to sharing using a manual or technical means of information not directly related to a cybersecurity threat that the private entity knows at the time of sharing to be information. Section 104(d)(2)(A) and (B)<br>• Compliance with procedures for submission to DHS | • Liability protection for sharing of cyber threat indicators. Section 106<br>• Antitrust Exemption. Section 104(e)<br>• Exemption from state disclosure laws. Section 104(d)(4)(B)<br>• Exemption from state regulatory use. Section 104(d)(4)(C)<br>• No waiver of privilege for shared material. Section 105(d)(1)<br>• Treatment of commercial, financial, and proprietary information. Section 105(d)(2)<br>• Exemption from federal disclosure laws. Section 105(d)(3)<br>• Ex parte communications waiver. Section 105(d)(4)<br>• Exemption from federal regulatory use. Section 105(d)(5)(D) |
| Any other sharing conducted under the Act | Section 104(c) | Any federal entity (e.g., FBI, DHS, DOE, Treasury, DoD) | • Removal prior to sharing using a manual or technical means of information not directly related to a cybersecurity threat that the private entity knows at the time of sharing to be information. Section 104(d)(2)(A) and (B) | • Antitrust Exemption. Section 104(e)<br>• Exemption from state disclosure laws. Section 104(d)(4)(B)<br>• Exemption from state regulatory use. Section 104(d)(4)(C)<br>• No waiver of privilege for shared material. Section 105(d)(1)<br>• Treatment of commercial, financial, and proprietary information. Section 105(d)(2)<br>• Exemption from federal disclosure laws. Section 105(d)(3)<br>• Ex parte communications waiver. Section 105(d)(4)<br>• Exemption from federal regulatory use. Section 105(d)(5)(D) |