Cybersecurity Information Sharing Act – Frequently Asked Questions

On June 15, 2016, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) published 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*, which can be found at https://us-cert.gov/ais. Since then, DHS and DOJ have received numerous questions regarding the implementation of the Cybersecurity Information Sharing Act of 2015 (CISA),[1] and have compiled this document to provide further guidance and answers to frequently asked questions. This document 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, and methods of sharing with the DHS capability and process.[2]

1. Does CISA override federal and state laws that prohibit or restrict voluntary disclosure or sharing of information regarding cyber threats?

   Yes. CISA 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." CISA, §104(c)(1) (emphasis added). Therefore, CISA plainly overrides conflicting federal laws.

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

   - 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." *Id*. §102(4);
   - consisting of information that meets the definition of a "cyber threat indicator" or "defensive measures." (See frequently asked question (FAQ) #7 for a discussion of "cyber threat indicators" and "defensive measures.");
   - following the review and removal of any personal information of a specific person or information that identifies a specific person that the sharer knows is not directly related to a cyber threat. *Id*. § 104(d)(2); and
   - in compliance with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicators or defensive measures.

[1] Consolidated Appropriations Act of 2016, P.L. 114-113, Division N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2936, 6 U.S.C. §§ 1501-1510 (CISA).

[2] Like the other CISA 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 also includes a provision preempting any state law that restricts or otherwise regulates an activity that CISA authorizes. *Id*. § 108(k)(1). Thus, it is clear that CISA's authorization for sharing cyber threat indicators and defensive measures overrides conflicting federal and state civil and criminal laws.

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

   Yes. Section 104(c) of CISA 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 defines the term "non-federal entity" to include private entities. CISA, § 102(14). Section 106(b) of CISA protects any private entity from liability arising from sharing a cyber threat indicator or defensive measure in accordance with CISA. 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. CISA, § 106(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 106.

3. Do CISA'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?

   CISA'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 receives liability protection for that sharing under section 106(b). Consequently, ISAOs and ISACs that meet the definition of a private entity (*Id.*, § 102(15)), or the broader definition of a non-federal entity (*Id.*, § 102(14)), would qualify for protection, and private entities sharing information with ISAOs and ISACs in accordance with CISA would similarly receive liability protection. (See also Non-Federal Entity Sharing Guidance at 14 (June 2016)). 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, 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 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, 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's information sharing authorization and section 105(c)(1)(B). Section 106(b) of CISA provides liability protection to a private entity "for the sharing or receipt of a cyber threat indicator or defensive measure under section 104(c)," if such sharing is conducted consistent with CISA. Section 104(c) includes requirements for sharing under CISA, including requirements for the removal of personal information known to be not directly related to the cybersecurity threat. (See FAQ #1 for the requirements for sharing under CISA.)

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 105(c)(1)(B)." Private entities sharing information through the DHS capability and process receive liability protection under section 106, 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 105(c)(1)(B), they are not the only means.

Section 105 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 105(c)(1)(B)(i), provides for sharing, consistent with section 104, "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 106, including compliance with section 104(c). For example, a company could receive liability protection for sharing a cyber threat indicator or defensive measure with DHS consistent with sections 104(c) and 106, 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." § 105(c)(1)(B)(i).

So, as discussed below in FAQ #6, CISA is not primarily designed to address sharing cyber threat information with law enforcement. However, CISA 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 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

[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 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.

measure." Under Section 102(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 105(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. Further, as discussed above, a company could receive liability protection under section 105(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 104 for cybersecurity monitoring and information sharing, and the liability protections provided under section 106 of CISA?

Section 104 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 106 provides liability protection. Section 106 requires that any cause of action brought in any court be promptly dismissed if the alleged conduct was conducted in accordance with CISA. Section 106(a) applies to any cybersecurity monitoring conducted pursuant to section 104(a). Section 106(b)(1) shields any sharing conducted among private entities pursuant to section 104(c). (See FAQ #2.) However, as discussed in FAQ #4, section 106(b)(2) applies only to information sharing that a private entity conducts with the Federal Government in a manner consistent with section 105(c)(1)(B). Taken together, sections 104 and 106 provide strong legal protection to cybersecurity monitoring and information sharing activities undertaken in accordance with CISA.

6. Does CISA alter the manner in which non-federal entities report information to federal law enforcement? Must such reporting now be conducted through the DHS capability and process?

No. CISA does not require any change in reporting information to law enforcement. It is important to remember that CISA 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 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 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." *Id.* § 105(C)(1)(E). More broadly, CISA 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 title; 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 title." CISA, §108(a)(1)-(2). In short, CISA 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's definitions of a "cyber threat indicator" or "defensive measure" and that may be shared under CISA?

CISA 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." CISA § 102(6).

CISA 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." *Id*. § 102(7)(A). However, CISA 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." *Id*. § 102(7)(B).

CISA'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 provided examples of cyber threat indicators and defensive measures shareable under CISA. 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 104(c), these categories of information fall within CISA's liability protections when shared in accordance with CISA. (See FAQ #1.) Thus, liability protection would apply when sharing occurs among non-federal entities (CISA, § 106(b)(1)), and between a non-federal entity and a federal entity, when conducted in accordance with section 105(c)(1)(B). (*Id.* §§ 104(d)(2), 105(c)(1)(B) and 106(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?

No. CISA 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 personal information of a specific individual, or information that identifies a specific individual. CISA, §104(d)(2). So, information that is directly related to a cybersecurity threat, even if it is personal information, may be shared in accordance with CISA. However, failure to remove personal information consistent with CISA before cyber threat indicators or defensive measures are shared would forfeit CISA's liability protection and the other protections that apply to sharing conducted in accordance with CISA as well. The review for such information may be conducted using either a manual process or technical capability. CISA, § 104(d)(2).

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

   No. CISA 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's requirements for sharing (see FAQ #1) would not receive liability protection under CISA. See FAQs #1 and #5. It is also noteworthy that section 106(c) provides that CISA 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's enactment need to alter their practices now that CISA has been passed?

    No. Private or governmental entities that were lawfully sharing information before CISA was enacted do not need to alter their practices in the wake of CISA's passage. CISA is not intended to affect sharing that has occurred or currently occurs outside of the statute. Section 108(a) explicitly provides that CISA does not limit or prohibit otherwise lawful sharing of information among private or governmental entities. Section 108(f) further provides that CISA does not limit or modify existing information sharing relationships or require the creation of new ones. In other words, CISA 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 provide any protection against claims that sharing cyber threat indicators and defensive measures violates antitrust laws?

Yes. CISA provides that activity authorized by CISA 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. CISA, § 104(e). CISA'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 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. *Id.* § 108(e).

CISA'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 exempt from disclosure under the Freedom of Information Act or other federal or state "sunshine laws"?

Yes. CISA provides that cyber threat indicators or defensive measures shared with the Federal Government under CISA are exempt from disclosure under the Freedom of Information Act. CISA, § 105(d)(3). CISA further provides that cyber threat indicators or defensive measures shared with a federal, state, tribal, or local government under CISA are also exempt from disclosure under any state, local, or tribal "sunshine law" or similar law requiring disclosure of information or records. *Id*. §§ 104(d)(4)(B) and 105(d)(3).

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

CISA's protection against a waiver of privilege is broad and covers common law privileges. CISA provides that "[t]he provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection." CISA § 105(d)(1). CISA's privilege protections apply to cyber threat indicators and defensive measures shared in accordance with CISA, 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?

Generally, no. With one exception, CISA prohibits any federal, state, tribal, or local government from using cyber threat indicators or defensive measures submitted to the Federal Government under CISA to regulate the lawful activities of any non-federal entity. CISA, § 105(d)(5)(D). CISA explicitly prohibits the Federal 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. These same restrictions apply to the use of such information by state, tribal, or local regulators. *Id.* § 104(d)(4)(C).

This prohibition contains an exception, however, that allows the limited use of such information pursuant to regulatory authority "specifically related to the prevention or mitigation of cybersecurity threats to information systems." In such circumstances, the information can be used only to inform the development or implementation of regulations relating to information systems.

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

No. As Congress explained in its Joint Explanatory Statement on CISA, the statute does not authorize a private entity to "hack back." Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015, p. 2. CISA'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 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. CISA, § 104(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. *Id*. § 102(7)(b).

17. How do CISA'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's protections for sharing cyber threat indicators and defensive measures in accordance with CISA. State, tribal, and local governmental entities, however, generally cannot invoke CISA's liability protections for sharing conducted pursuant to CISA because liability protection under section 106 is only available to "private entities." But state, tribal, and local governmental entities that provide utility services may invoke liability protection, because CISA's definition of private entities includes governmental entities that provide such services. CISA, § 102(15)(B). The protections available for sharing information *with* any state, local, or tribal government are unaffected by this limitation.

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

    CISA does not protect or authorize sharing by or with a "foreign power," as defined in section 1801 of Title 50. CISA 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. CISA, §§ 102(14)(C) and 102(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. CISA § 102(8). CISA's protections are available, however, for sharing by or with foreign corporations that do not fall within the definition of a foreign power.

    CISA does not limit or modify any existing information sharing relationship or prohibit any new information sharing relationship, including with foreign governments. *Id*., § 108(f). Thus, otherwise lawful sharing with a foreign government is not affected by CISA, although such sharing would not be undertaken pursuant to CISA and, thus, would not benefit from CISA's protections. Nonetheless, foreign governments may share with the Federal Government using the same mechanisms provided by CISA, including through the DHS capability and process.

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

    No. CISA does not require the use of a specific submission pathway. Entities that wish to benefit from CISA's protections must comply with CISA's requirements as outlined in FAQ #1 in the Non-Federal Entity Sharing Guidance; but cyber threat indicators that are shared with DHS's National Cybersecurity and Communications Integration Center 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, and thus are eligible for CISA's protections, including protection from liability. No specific language must be used (for example in an email) to invoke CISA 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?

    CISA 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 that is known or determined to be in error or in contravention of the requirements of CISA or another provision of federal law or policy of such error or contravention. (Section 103(b)(1)(C))
    - federal entities must notify non-federal entities and federal entities if information received pursuant to CISA is known or determined by a federal entity receiving such information not to constitute a cyber threat indicator. (Section 105(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. (Section 103(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 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), located at https://www.us-cert.gov/ais and return to nccicustomerservice@hq.dhs.gov. Once the signed ToU is returned, DHS staff will reach out with all the information necessary to establish a direct connection to the DHS server. DHS will also conduct conference calls or webinars with companies that have questions about the on-boarding requirements or receiving, using, or sharing indicators and defensive measures.