The Department of Homeland Security
The Department of Justice

Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015

June 15, 2016

Table of Contents

1 Purpose 3
2 Applicability 3
3 Background 3
4 Guiding Principles 4
5 Federal Entity Activity 7
5.1 Defensive Measures 7
5.2 Receipt 7
5.3 Notification Procedures 8
5.4 Notification of a United States Person 9
5.5 Use 10
5.6 Safeguarding 11
5.7 Retention 11
5.8 Dissemination 12
6 Sanctions 13
7 Protection of Classified/National Security Information 14
8 Audit 14
9 Periodic Review 15
Appendix A: Glossary 16

1 Purpose

This document establishes privacy and civil liberties guidelines governing the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity[1] obtained in connection with the activities authorized by the Cybersecurity Information Sharing Act of 2015 (CISA), consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats, any other applicable provisions of law, and the Fair Information Practice Principles (FIPPs) set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace. Federal entities engaging in activities authorized by CISA shall do so in full compliance with the Constitution and all other applicable laws of the United States, Executive Orders and other Executive Branch directives, regulations, policies and procedures, court orders and all other legal, policy and oversight requirements. Nothing in these guidelines shall affect the conduct of authorized law enforcement or intelligence activities or modify applicable authority of a department or agency of the Federal Government, including, but not limited to, the protection of classified information and sources and methods and the national security of the United States.

2 Applicability

These guidelines are applicable to federal entities, as that term is defined in CISA, receiving, retaining, using, or disseminating cyber threat indicators, and where appropriate defensive measures, under CISA.

3 Background

On December 18, 2015, the President signed CISA into law. Congress designed CISA to create a voluntary cybersecurity information sharing process that will encourage public and private entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties. CISA required the Attorney General and the Secretary of Homeland Security to jointly develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with activities authorized in CISA. On February 16, 2016, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) fulfilled this interim requirement by jointly issuing Privacy and Civil Liberties Interim Guidelines: Cybersecurity Information Sharing Act of 2015.[2]

Similarly, CISA requires the Attorney General and the Secretary of Homeland Security, in coordination with their privacy and civil liberties officers and in consultation with heads of the appropriate Federal entities, with such entities' privacy and civil liberties officers, and with such private entities with industry expertise as the Attorney General and the Secretary consider

[1] Non-federal entities should refer to 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, found at: https://www.us-cert.gov/ais.
[2] Found at: https://www.us-cert.gov/ais.

relevant, to jointly develop, submit to Congress, and make publicly available final guidelines. This document fulfills this requirement.

DHS and DOJ have consulted with the following appropriate federal entities, as defined in CISA, in preparing this document:

- Department of Commerce
- Department of Defense
- Department of Energy
- Department of the Treasury
- Office of the Director of National Intelligence

In addition, as required by CISA, DHS and DOJ have consulted with private entities with industry expertise related to cybersecurity through multiple avenues, including meetings, conference calls, webinars, and various outreach events. Consulted organizations included those with specific privacy and civil liberties expertise. In addition to these events, DHS and DOJ established a dedicated e-mail address for receiving comments and further facilitating continued correspondence with the consulted organizations.

4 Guiding Principles

Federal entities' activities authorized by CISA, including the receipt, retention, use, and dissemination of cyber threat indicators and through the voluntary cybersecurity information sharing process outlined in the Section 105(a)(1)-(3) Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government, shall follow procedures designed to limit the effect on privacy and civil liberties of federal activities under CISA. Cyber threat indicators provided to the Federal Government under CISA may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of federal law, any federal agency or department, component, officer, employee, or agency of the Federal Government solely for authorized activities as outlined in CISA. A federal entity shall review cyber threat indicators, prior to sharing them, to assess whether they contain any information not directly related to a cybersecurity threat that such federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual[3] and remove such information. Furthermore, as specifically directed by CISA, and consistent with other Federal Government cybersecurity initiatives, a primary guiding principle for all federal entity activities related to the receipt, retention, use and dissemination of cyber threat indicators as authorized by CISA is the FIPPs set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace. The FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect

[3] Federal entities are permitted to assess cyber threat indicators or defensive measures for information that would qualify as "personal information" or "personally identifiable information," as defined by the federal entity, so long as the definition would, at a minimum, include personal information of a specific individual, or information that identifies a specific individual.

individual privacy. Table 1 identifies how the FIPPs have shaped these guidelines that govern the receipt, retention, use, and dissemination of cyber threat indicators shared under CISA.

Principle	Privacy and Civil Liberties Guidelines Implementation
Transparency	By making publicly available and following these Privacy and Civil Liberties Guidelines, as well as the procedures developed in accordance with Sections 103(b)(1) and 105(a)(1)-(3) of CISA, federal entities are transparent about their receipt, retention, use and dissemination of cyber threat indicators under CISA. In addition, federal entities should complete and publish privacy compliance documentation, such as Privacy Impact Assessments (PIAs) in accordance with the E-Government Act of 2002 and an agency's privacy policies, as appropriate, to fully describe their receipt, retention, use, and dissemination of cyber threat indicators, under CISA. Further, per Section 103(b)(1)(F) of CISA, procedures have been developed for notifying, in a timely manner, any United States person[4] whose personal information is known or determined to have been shared by a federal entity in violation of CISA.
Individual Participation	Given the nature of a cyber threat indicator, an individual whose personal information is directly related to a cybersecurity threat does not have the ability to consent, be involved in the process used to collect that information, access, or correct that information. This would be counter to the utility of the cyber threat indicator. However, by limiting the receipt, retention, use, and dissemination of cyber threat indicators that contain any information not directly related to a cybersecurity threat that such federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual, federal entities are limiting the impact to an individual's privacy and civil liberties.
Purpose Specification	CISA authorizes federal entities to receive, retain, use, and disseminate cyber threat indicators. Cyber threat indicators received under CISA may only be used for purposes authorized in Section 105(d)(5)(A) of CISA.
Data Minimization	Federal entities are required to limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals in accordance with the Section 105(a)(1)-(3) Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government and these Privacy and Civil Liberties Guidelines. These minimization requirements include, but are not limited to, the timely destruction of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals known not to be

[4] For the purposes of Section 103(b)(1)(F), a "United States person" means a citizen of the United States or an alien lawfully admitted for permanent residence.

Principle	Privacy and Civil Liberties Guidelines Implementation
	directly related to uses authorized under CISA.
Use Limitation	Federal entities may only use cyber threat indicators received under CISA, including personal information of a specific individual or information that identifies a specific individual that may be part of the cyber threat indicator, for purposes authorized in Section 105(d)(5)(A) of CISA.
Data Quality and Integrity	Cybersecurity threats change and evolve over time, sometimes almost as quickly as the threat is identified. Because of these factors, the usefulness and timeliness of an individual cyber threat indicator may be limited to a short period of time. To mitigate the usage of stale or poor quality information, cyber threat indicators are retained only for a specific period of time or until they are no longer directly related to a use authorized under CISA.
Security	Federal entities should follow requirements to safeguard cyber threat indicators, including those containing personal information of specific individuals or information that identifies specific individuals that is directly related to a cybersecurity threat or a use authorized under CISA, from unauthorized access or acquisition. In addition, appropriate sanctions will be implemented for activities by officers, employees, or agents of the Federal Government in contravention of these guidelines.
Accountability and Auditing	Federal entities are accountable for complying with the Privacy and Civil Liberties Guidelines, as well as the procedures developed in accordance with Sections 103(b)(1) and 105(a)(1)-(3) of CISA. In addition, federal entities must ensure there are audit capabilities put in place around the receipt, retention, use and dissemination of cyber threat indicators. Finally, the Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate federal entities and in consultation with the officers and private entities as the Attorney General and the Secretary of Homeland Security consider relevant, periodically, but not less frequently than once every 2 years after issuance of the final guidelines, jointly review the guidelines contained within this document. These guidelines shall be updated, as appropriate, and made publicly available following such periodic reviews. Periodic reviews shall take into account the findings and recommendations of the agency Inspector General biennial reports on compliance required under Section 107(b) of CISA, and the Government Accountability Office's independent report on removal of personal information under Section 107(c) of CISA.

Table 1: FIPPs Implementation

5 Federal Entity Activity

The following provisions apply to federal entity activities authorized by CISA. These include a discussion on defensive measures, the receipt, retention, use, and dissemination of cyber threat indicators, and notification and safeguarding requirements.

5.1 Defensive Measures

Defensive measures, as a technical matter, typically should not need to contain personal information of a specific individual or information that identifies a specific individual. However, they may contain such information if determined necessary to the defensive measure. While these guidelines generally govern only the receipt, retention, use, and dissemination of cyber threat indicators, these guidelines discuss several CISA requirements relating to the receipt, retention, use, and dissemination of both defensive measures and cyber threat indicators.[5] When discussing a CISA requirement that applies to defensive measures in addition to cyber threat indicators, these guidelines will note that fact. In addition, a defensive measure may contain a cyber threat indicator. In such an instance, these guidelines would apply in any event to the portion of the defensive measure that is a cyber threat indicator.[6]

Federal entities are strongly encouraged, where not explicitly required and to the extent appropriate, to apply the requirements found in these guidelines to defensive measures. CISA provides that, not later than 3 years after the date of the enactment of CISA, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to CISA. Accordingly, federal entities are encouraged to review defensive measures, prior to sharing them, to assess whether they contain any information (1) not directly related to a cybersecurity threat (2) that such 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. Any recipients of defensive measures should also exercise due diligence to ensure that the effects of implementing a recommended defensive measure do not cause subsequent harm to systems or individuals.

5.2 Receipt

Federal entities must destroy information, in a timely manner, that is (1) personal information of specific individuals or information that identifies specific individuals and (2) that is known not to be directly related to uses authorized under CISA.

---

[5] For example, Section 103(b)(1)(C) (requiring specific procedures for timely notifying federal entities and nonfederal entities that have received cyber threat indicators or defensive measures 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)(D) (requiring federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures); and Section 105(d)(5)(D) (limiting the disclosure, retention, and use of cyber threat indicators and defensive measures to only those authorized uses permitted under CISA).

[6] For example, a signature or technique for protecting against targeted exploits such as spear phishing may include a specific email address (cyber threat indicator) from which malicious emails are being sent.

Upon receipt of a cyber threat indicator under CISA, each federal entity will ensure that any such information described above is deleted. Agencies should do this through a technical capability when possible.

The Federal Government's principal mechanism for receipt of cyber threat indicators and defensive measures is the Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS) capability.[7] DHS will receive cyber threat indicators and defensive measures through that portal in a standard, automated format; apply rules to remove information as described above; and apply unanimously agreed upon controls as described in the Section 105(a)(1)-(3) procedures. Federal entities that receive cyber threat indicators or defensive measures from DHS through AIS may assume that any personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat has been removed. However, federal entities should still follow all other applicable procedures, guidelines, and requirements, to the extent consistent with and in addition to these Privacy and Civil Liberties Guidelines to ensure appropriate handling of cyber threat indicators and defensive measures.

5.3 Notification Procedures

Section 103(b)(1)(C) of CISA requires procedures for notifying, in a timely manner, 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. In addition, Section 105(b)(3)(E) of CISA requires procedures for notifying 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. Under both of these scenarios, the federal entity that makes the determination shall notify the disseminating entity of that determination as soon as practicable and the disseminating entity shall notify all entities and federal entities who have received the information as soon as practicable. If the disseminating entity was not the originator of the cyber threat indicator or defensive measure, then the disseminating entity shall also notify the original submitting entity as soon as practicable. These notifications shall all be provided consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats.

The notice shall contain:

- Identifying information of the cyber threat indicator or defensive measure (e.g., unique identifier);
- Identification of the information 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 in accordance with Section 103(b)(1)(C) of CISA, including any information that does

[7] For more information on AIS, please see the AIS PIA, found at: www.dhs.gov/privacy. The AIS PIA will be updated as appropriate.

not constitute a cyber threat indicator in accordance with Section 105(b)(3)(E) of CISA; and

- Any other information that may be relevant to the disseminating entity in order to correct the error. For more guidance on identifying information that should not be submitted, please refer to the Section 105(a)(4) Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under CISA, which can be found at www.us-cert.gov/ais.

Following receipt of a notice, the disseminating entity shall provide an update by redistributing the updated cyber threat indicator or defensive measure using the same mechanism used for the original sharing. Upon receipt of the update, the receiving federal entity shall promptly apply the update to replace and delete, to the maximum extent practicable, any information 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, including any information that does not constitute a cyber threat indicator.

Under DHS's AIS initiative, discovery that a cyber threat indicator or defensive measure contains information 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, including any information that does not constitute a cyber threat indicator or defensive measure may either be made by DHS or another entity. If an entity receiving the information determines that the information is in error or in contravention of the requirements of CISA or another provision of federal law or policy, including determining that the information does not constitute a cyber threat indicator or defensive measure, the entity should notify DHS as soon as practicable by emailing TAXIIADMINS@US-CERT.GOV so that DHS can notify the submitting entity and issue an update. Once the update is received, entities shall promptly replace and delete, to the maximum extent practicable, the original information. DHS will provide a periodic submission disposition report to the submitter with a unique identifier for each submission and a list of the fields that are accepted for dissemination along with a list of fields that were not accepted for dissemination. This report will notify the submitter of any information that was known or determined to be in error or in contravention of the requirements of CISA or another provision of federal law or policy, including any information that was submitted that does not constitute a cyber threat indicator or defensive measure.

5.4 Notification of a United States Person

In addition, Section 103(b)(1)(F) of CISA requires procedures for a federal entity to notify, in a timely manner, any United States person whose personal information is known or determined to have been shared in violation of CISA.

It should be noted that most personal information exchanged as part of a cyber threat indicator or defensive measure may be incomplete, may not identify a specific individual, or may lack enough information to verify that it pertains to a United States person. To the extent that agencies have policies in place regarding verification of the United States person status of an individual, such policies may be used. Even if notification under Section 103(b)(1)(F) of CISA may not be required because there isn't enough information to identify a specific individual, or

because the federal entity cannot verify whether personal information disclosed in violation of the Act pertains to a United States person, the other notification requirements may still apply (i.e., if the federal entity responsible for sharing the information knows or determines the information to be in error or in contravention of the requirements of CISA or another provision of federal law or, or if the information includes any information that does not constitute a cyber threat indicator, the federal entity should follow the Notification Procedures required by Sections 103(b)(1)(C) and 105(b)(3)(E) of CISA, as outlined above).

When a federal entity knows or determines that it has shared personal information of a United States person in violation of CISA, the federal entity should notify the person in accordance with the federal entity's own breach/incident response plan.[8] The federal entity may make the determination of the violation on its own, or may receive reporting of the violation from another entity that received the information and made the determination. If the federal entity that shared personal information of a United States person in violation of CISA received the personal information from another federal entity (which may have also shared the personal information in violation of CISA), the receiving entity should contact the entity that initially shared the information to coordinate notification. In addition, the disseminating entity shall provide an update by redistributing the updated cyber threat indicator or defensive measure using the same mechanism used for the original sharing. Upon receipt of the update, the receiving federal entity shall promptly apply the update to replace and delete, to the maximum extent practicable, the information pertaining to a United States person that was shared in violation of CISA.

Based on the type of personal information shared in violation of CISA, and the potential harm the disclosure could cause, remedial actions or corrective measures should be considered for the affected United States person, based on the federal entity's existing policies.

5.5 Use

Consistent with Section 105(d)(5) of CISA, federal entities that receive cyber threat indicators and defensive measures under CISA will use them only for the purposes authorized under CISA. Specifically, cyber threat indicators and defensive measures provided to the Federal Government under CISA may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of federal law, any federal agency or department, component, officer, employee, or agent of the Federal Government solely for:

1. a cybersecurity purpose;
2. the purpose of identifying (i) a cybersecurity threat, including the source of such cybersecurity threat or (ii) a security vulnerability;

[8] Consistent with the Office of Management and Budget (OMB) Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007), or its successor, the head of each Federal agency is required to develop a breach notification policy and plan. Federal entities may rely on its breach notification policy and plan for timely notifying United States persons, so long as the policy and plan is consistent with the notice requirements in Section 103(b)(1)(F) of CISA. Federal entities should update their breach notification policy and plan as OMB M-07-16 is revised to ensure their plan is consistent with the latest OMB guidance.

3. the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;
4. the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety; or
5. the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in #3 above or any of the offenses listed in (i) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft), (ii) chapter 37 of such title (relating to espionage and censorship), and (iii) chapter 90 of such title (relating to protection of trade secrets).

5.6 Safeguarding

Federal entities shall apply appropriate controls to safeguard cyber threat indicators that contain personal information of a specific individual or information that identifies a specific individual that is directly related a cybersecurity threat or a use authorized under CISA, from unauthorized access or acquisition. Such controls shall also protect the confidentiality of cyber threat indicators that contain personal information of a specific individual or information that identifies a specific individual that is directly related to a cybersecurity threat or a use authorized under CISA to the greatest extent practicable. Recipients of such cyber threat indicators shall be informed that they may only be used for purposes authorized by CISA. Such controls will include:

- Internal User access controls;
- Consideration for physical and/or logical segregation of data;
- Required training; and
- Requirements as prescribed by the Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554).

Controls commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, including cyber threat indicators are required and described in FISMA. Standards and Guidelines for these controls are documented in NIST Special Publication 800-53 Revision 4.[9]

5.7 Retention

Federal entities may only retain cyber threat indicators and defensive measures provided to the Federal Government under CISA for the purposes authorized in Section 105(d)(5)(A) of CISA (as outlined above in the *Use* section). Federal entities will follow or modify applicable, or establish new, records disposition schedules to comply with the requirements in Section 105(b)(3)(B)(ii) for specific limitations on retention. In accordance with Section 105(b)(3)(B)(i) of CISA, federal entities will also establish a process for the timely destruction, including

[9] Found at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

immediate destruction or deletion, of specific information within the cyber threat indicator, when it becomes known to the federal entity that the cyber threat indicator contains personal information of specific individuals, or information that identifies specific individuals, that is not directly related to an authorized use under CISA. Such schedules must also provide instructions for the destruction of appropriately shared cyber threat indicators.

Retention schedules for cyber threat indicators and defensive measures should be consistent with the operational needs of each federal entity and in accordance with the Federal Records Act. Because each federal entity's need may be different from another, retention schedules should be appropriate to their mission while ensuring the appropriate destruction of a cyber threat indicator and defensive measure. Examples of such record schedules include DHS's National Cybersecurity Protection System (NCPS) DAA-0563-2015-0008[10] and DAA-0563-2013-0008-0001[11] records schedules.

5.8 Dissemination

Federal entities will disseminate cyber threat indicators only after following the procedures set forth below, consistent with Section 103(b)(1)(E) of CISA.

Prior to the sharing of a cyber threat indicator, every federal entity shall review such cyber threat indicator to assess whether it contains any information (1) not directly related to a cybersecurity threat (2) that such 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. If both of these elements apply to a particular field of information, that field of information shall be removed before sharing. This review may be conducted manually, or the federal entity may implement and utilize a technical capability configured to conduct the same review.

1. When information is not directly related to a cybersecurity threat:

A cybersecurity threat is defined in part as an "action … that may result in an unauthorized effort to adversely impact [a computer system's] security, availability, confidentiality, or integrity …" 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 typically be

[10] Found at: https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2015-0008_sf115.pdf.
[11] Found at: https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0008_sf115.pdf.

information not directly related to a cybersecurity threat and therefore should not be included as part of the cyber threat indicator.

2. Whether the federal entity knows at the time of sharing that the information is personal information of a specific individual or information that identifies a specific individual.

This element is met only if the federal entity has reason to know that information, at the time of sharing, is personal information of a specific individual or information that identifies a specific individual. For example, the "To" line or victim of a spear phishing email or a username included in a file path may meet this standard.

When disseminating cyber threat indicators, federal entities will do so in a manner consistent with any markings associated with the subject cyber threat indicators denoting their sensitivity or other concerns. Federal entities will preserve these markings as appropriate when disseminating cyber threat indicators.

Under DHS' AIS initiative, brokering of cyber threat indicators and defensive measures between non-federal entities and appropriate federal entities will be done through existing Enhance Shared Situational Awareness (ESSA) Community arrangements within the ESSA Information Sharing Architecture (ISA). Further dissemination of, and access to, cyber threat indicators and defensive measures is controlled via data markings as referenced in the ESSA/ISA's Access Control Specification (ACS). Appropriate federal entities apply a fully articulated set of markings that unambiguously define the access and dissemination constraints for shared cyber threat indicators and defensive measures—which are translated by DHS to a marking language commonly used by the non-federal entities called the Traffic Light Protocol (TLP). TLP markings provided by non-federal entities will be translated to the ESSA/ISA ACS for consistency and to limit confusion in the federal receipt and distribution of cyber threat indicators and defensive measures.

AIS non-federal entities may apply certain types of markings for access and dissemination: TLP, AIS Consent marking, and CISA Proprietary. TLP was designed for ease of use and permits some degree of human judgment in the application of the rule sets. The particular type of AIS Consent marking will indicate whether the non-federal entity consents (or not) to sharing its identity with federal entities or with the entire AIS community. The CISA Proprietary marking can also be used by non-federal entities.

The technical procedures and requirements for these markings are defined in the ESSA/ISA Access Control Specification, and may be modified with updates to this document.[12]

6 Sanctions

Failure by an individual to abide by the usage requirements set forth in these guidelines will result in appropriate sanctions applied to that individual in accordance with their department or

[12] For more information on the ESSA/ISA ACS, federal users may visit: https://community.max.gov/display/CrossAgencyExternal/ISA+Access+Control.

agency's relevant policy on *Inappropriate Use of Government Computers and Systems*. Sanctions commonly found in such policies, depending on the severity of misuse, include: remedial training; loss of access to information; loss of a security clearance; and termination of employment.

7 Protection of Classified/National Security Information

If during the review of a cyber threat indicator it is determined that classified or other sensitive national security information is present, then appropriate steps will be taken in accordance with applicable Executive Orders and directives.

8 Audit

Section 105(a)(3)(C) of CISA requires procedures to ensure that audit capabilities are in place. CISA sets forth multiple auditing requirements, which are restated below. Agencies shall ensure they maintain records sufficient to enable the assessments described below.

Section 107(b) of CISA provides that, not later than 2 years after the date of the enactment of CISA and not less frequently than once every 2 years thereafter, the inspectors general of the appropriate federal entities, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the actions of the executive branch of the Federal Government to carry out CISA during the most recent 2-year period.

Each report submitted shall include, for the period covered by the report, the following requirements related to the protection of privacy and civil liberties:

- An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.
- An assessment of the cyber threat indicators or defensive measures shared with the appropriate federal entities under this title, including the following:
    - The number of cyber threat indicators or defensive measures shared through the capability and process developed under Section 105(c).
    - An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-federal government entity with the Federal Government in contravention of this title, or was shared within the Federal Government in contravention of the guidelines required by this title, including a description of any significant violation of this title.
    - The number of times, according to the Attorney General, that information shared under this title was used by a federal entity to prosecute an offense listed in Section 105(d)(5)(A).
    - A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to

a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by Section 105(b)(3)(E).

- The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this title on the privacy and civil liberties of United States persons.

In addition, CISA provides that, not later than 3 years after the date of the enactment of CISA the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant CISA. Such report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this title in addressing concerns relating to privacy and civil liberties.

9 Periodic Review

The Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate federal entities and in consultation with the officers designated under Section 1062 of the National Security Intelligence Reform Act of 2004 and such private entities with industry expertise as the Attorney General and the Secretary of Homeland Security consider relevant, periodically, but not less frequently than once every 2 years from the date of initial issuance, jointly review these guidelines. These guidelines shall be updated, as appropriate in accordance with statutory and policy changes, and made publicly available following such periodic reviews.

Periodic reviews shall take into account the findings and recommendations of the agency Inspector General biennial reports on compliance required under Section 107(b) of CISA and the Government Accountability Office's independent report on removal of personal information.

Appendix A: Glossary

AGENCY—The term ‘‘agency’’ has the meaning given the term in section 3502 of title 44, United States Code.

APPROPRIATE FEDERAL ENTITIES—The term ‘‘appropriate federal entities’’ means the following:

(A) The Department of Commerce.
(B) The Department of Defense.
(C) The Department of Energy.
(D) The Department of Homeland Security.
(E) The Department of Justice.
(F) The Department of the Treasury.
(G) The Office of the Director of National Intelligence.

CYBERSECURITY PURPOSE—The term ‘‘cybersecurity purpose’’ means 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.

CYBERSECURITY THREAT—

(A) IN GENERAL—Except as provided in subparagraph (B), the term ‘‘cybersecurity threat’’ means 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.
(B) EXCLUSION—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.

CYBER THREAT INDICATOR—The term ‘‘cyber threat indicator’’ means 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.

DEFENSIVE MEASURE—

(A) IN GENERAL—Except as provided in subparagraph(B), the term ‘‘defensive measure’’ means 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.

(B) EXCLUSION—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—

(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.

FEDERAL ENTITY—The term ‘‘federal entity’’ means a department or agency of the United States or any component of such department or agency.

INFORMATION SYSTEM—The term ‘‘information system’’—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

LOCAL GOVERNMENT—The term ‘‘local government’’ means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

MALICIOUS CYBER COMMAND AND CONTROL—The term ‘‘malicious cyber command and control’’ means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

MALICIOUS RECONNAISSANCE—The term ‘‘malicious reconnaissance’’ means a method for actively probing or passively monitoring an information system for the purpose of discerning

security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

MONITOR—The term ‘‘monitor’’ means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

NON-FEDERAL ENTITY—

(A) IN GENERAL—Except as otherwise provided in this paragraph, the term ‘‘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).

(B) INCLUSIONS—The term ‘‘non-federal entity’’ 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.

(C) EXCLUSION—The term ‘‘non-federal entity’’ does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

PRIVATE ENTITY—

(A) IN GENERAL—Except as otherwise provided in this paragraph, the term ‘‘private entity’’ means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION—The term ‘‘private entity’’ includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) EXCLUSION—The term ‘‘private entity’’ does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

SECURITY CONTROL—The term ‘‘security control’’ means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

SECURITY VULNERABILITY—The term ‘‘security vulnerability’’ means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

TRIBAL—The term ‘‘tribal’’ has the meaning given the term ‘‘Indian tribe’’ in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).