The Department of Homeland Security
The Department of Justice

Privacy and Civil Liberties Final Guidelines:

Cybersecurity Information Sharing Act of 2015

January 4. 2021

Table of Contents

Action Log

Upon issuance, the Attorney General and the Secretary of Homeland Security are required to periodically, but not less frequently than once every two years, jointly review the Privacy and Civil Liberties Final Guidelines. A notation of actions taken during the periodic review period will be included in this Action Log, and a brief summary and explanation of changes, if any, will appear in a summary of changes addressing the revisions. Previous summaries of changes prepared during these periodic reviews will be appended to the Guidelines in Appendix B.

Review	Date	Actions Taken
Interim Guidelines	February 16, 2016	Interim Guidelines Issued
Final Guidelines	June 16, 2016	Final Guidelines Issued
2018 Periodic Review	June 15, 2018	Final Guidelines, 2018 Edition, Issued
2020 Periodic Review	January 4, 2021	Final Guidelines, 2020 Edition, Issued

Summary of Changes, 2020 Edition

This section summarizes the revisions made to the Cybersecurity Information Sharing Act of 2015 (CISA 2015)[1] Privacy and Civil Liberties Final Guidelines, during the 2020 joint review conducted by the United States Department of Homeland Security (DHS) and the United States Department of Justice (DOJ).

CISA 2015 requires that the Attorney General and the Secretary of Homeland Security periodically, but not less frequently than once every 2 years, jointly review the CISA 2015 Privacy and Civil Liberties Final Guidelines, last published on June 15, 2018. The changes made throughout the 2020 Edition of the CISA 2015 Privacy and Civil Liberties Final Guidelines are a result of this periodic review. Overall, the 2020 joint review of the CISA 2015 Privacy and Civil Liberties Final Guidelines resulted in only minor administrative and clarifying changes to the Privacy and Civil Liberties Final Guidelines issued in 2018. In particular:

- In Sections 4, "Guiding Principles," 5, "Federal Entity Activity," and 9, "Audit," DHS and DOJ updated the text to clarify that not all information that a federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual needs to be removed, prior to sharing. Rather, after such information is identified, even if it is or is part of a cyber threat indicator or, where applicable, a defensive measure, a federal entity must still assess whether the information is "directly related to a cybersecurity threat," and if not, remove such information prior to sharing.
- DHS and DOJ reordered Section 5 to more clearly align with 6 USC § 1504(b)(3) and the typical chronological steps recipient federal entities will undertake as they interact with shared information.
- In Section [5.1], "Defensive Measures," DHS and DOJ added further clarifying text explaining why it is prudent to apply to defensive measures those CISA 2015 requirements that are only expressly applicable to cyber threat indicators.
- In Section [5.8], "Dissemination and Marking Requirements," DHS and DOJ revised the example under renumbered subsection 2 to better explain whether information that a federal entity knows at the time of sharing is personal information of a specific individual or information that identifies a specific individual is directly related to a cybersecurity threat.

[1] CISA 2015 was enacted as Title I of the Cybersecurity Act of 2015, and is codified at 6 U.S.C. §§ 1501–1510. For ease of reference, these Guidelines generally cite to the sections as codified in title 6 of the U.S. Code.

Lastly, DHS and DOJ made minor and clarifying revisions throughout to, among other things, refer to the statute as "CISA 2015" to account for the establishment of the Cybersecurity and Infrastructure Security Agency (CISA); cite to incorporated United States Code provisions instead of CISA 2015 section numbers; refer to guidance, procedures, and guidelines by their titles rather than by the associated CISA 2015 section number; clarify that, if it is necessary to remove personal information prior to sharing, only the personal information itself, and not necessarily the entire cyber threat indicator that contains such personal information, would need to be removed; account for the Comptroller General's December 2018 report and the fact that this is a one-time reporting requirement; and correct outdated footnotes and web links, where necessary.

DHS and DOJ will continue to review these Privacy and Civil Liberties Final Guidelines for necessary updates no less than every 2 years, as required by CISA 2015, to appropriately govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with the activities authorized by CISA 2015, 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.

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[2] obtained in connection with the activities authorized by the Cybersecurity Information Sharing Act of 2015 (CISA 2015), 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 2015 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 2015, receiving, retaining, using, or disseminating cyber threat indicators, and, where appropriate, defensive measures, under CISA 2015.

3 Background

On December 18, 2015, the President signed CISA 2015 into law.[2] Congress designed CISA 2015 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 2015 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 2015. 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[3].

Similarly, CISA 2015 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 of Homeland Security consider relevant, to jointly develop, submit to Congress, and make publicly available final guidelines. On June 15, 2016, DHS and DOJ fulfilled this requirement by jointly issuing Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015.

Upon issuance, the Attorney General and the Secretary of Homeland Security are required to periodically, but not less frequently than once every 2 years, jointly review these guidelines. During these periodic reviews, DHS and DOJ will consult with the following appropriate federal entities, as defined in CISA 2015:

- 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 2015, DHS and DOJ will consult with the officers designated under section 1062 of the National Security Intelligence Reform Act of 2004[4] and private entities with industry expertise related to cybersecurity through multiple avenues, which may include meetings, conference calls, webinars, and various outreach events. Consulted organizations will include, but are not limited to, those with specific privacy and civil liberties expertise.

---

[2] 6 U.S.C. §§ 1501–10.

[3] 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 (the "Non-Federal Entity Sharing Guidance"), found at: https://www.us-cert.cisa.gov/ais.

[4] See 42 U.S.C. § 2000ee-1.

4 Guiding Principles

Federal entities' cybersecurity information sharing activities, including the receipt, retention, use, and dissemination of cyber threat indicators through the voluntary cybersecurity information sharing process outlined in the Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government (the "Final Operational Procedures")[5], shall follow procedures designed to limit the effect on privacy and civil liberties of federal activities under CISA 2015. Cyber threat indicators provided to the Federal Government under CISA 2015 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 2015.

A federal entity shall review cyber threat indicators, prior to sharing them, to assess whether they contain any information 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[6]. Not all personal information identified in this review will need to be removed prior to sharing. On occasion, information known at the time of sharing to be personal information of a specific individual or information that identifies a specific individual will be "directly related to a cybersecurity threat" and, therefore, shareable under CISA 2015. Other personal information will not be directly related to a cybersecurity threat and therefore would not be shareable under CISA 2015 and should be removed prior to sharing. Personal information directly related to a cybersecurity threat includes personal information that is necessary to detect, prevent, or mitigate a cybersecurity threat.

Furthermore, as specifically directed by CISA 2015, 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 2015 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 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 2015.

[5] Section 1504(a)(1)–(3) directs the Attorney General and the Secretary of Homeland Security to issue policies and procedures relating to the receipt of cyber threat indicators and defensive measures by all federal entities. The Final Operational Procedures can be found at: https://www.us-cert.cisa.gov/ais.

[6] 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.

Principle	Privacy and Civil Liberties Final Guidelines Implementation
Transparency	By making publicly available and following these Privacy and Civil Liberties Final Guidelines, the Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015 procedures (the "Federal Government Sharing Guidance")[7], and the Final Operational Procedures, federal entities are transparent about their receipt, retention, use and dissemination of cyber threat indicators under CISA 2015. 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 agency policies, as appropriate, to fully describe their receipt, retention, use, and dissemination of cyber threat indicators under CISA 2015. Further, per section 1502(b)(1)(F), procedures have been developed for notifying, in a timely manner, any United States person[8] whose personal information is known or determined to have been shared by a federal entity in violation of CISA 2015.
Individual Participation	Given the nature of a cyber threat indicator, an individual whose personal information is contained within a cyber threat indicator and is directly related to a cybersecurity threat does not have the ability to consent to the receipt, retention, use, or dissemination of their information, be involved in the process used to collect that information, access, or correct that information. Such an ability would be counter to the utility of the cyber threat indicator. However, by limiting the receipt, retention, use, and dissemination, of a cyber threat indicator or part of a cyber threat indicator, that is information 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 that is not directly related to a cybersecurity threat, federal entities are limiting the impact to an individual's privacy and civil liberties.
Purpose Specification	CISA 2015 authorizes federal entities to receive, retain, use, and disseminate cyber threat indicators. Cyber threat indicators received under CISA 2015 may only be used for purposes

[7] Section 1502 directs the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General to jointly develop and issue procedures describing the current mechanisms through which the appropriate federal entities share cyber threat indicators and defensive measures. The Federal Government Sharing Guidance can be found at: https://www.us-cert.cisa.gov/ais.

[8] For the purposes of section 1502(b)(1)(F), a "United States person" means a citizen of the United States or an alien lawfully admitted for permanent residence.

	authorized in section 1504(d)(5)(A).
Data Minimization	Federal entities are required to limit the receipt, retention, use, and dissemination, as part of cyber threat indicators, of personal information of specific individuals or information that identifies specific individuals in accordance with the Final Operational Procedures. These minimization requirements include, but are not limited to, the timely destruction of personal information of specific individuals or information that identifies specific individuals not directly related to uses authorized under CISA 2015.
Use Limitation	Federal entities may only use cyber threat indicators received under CISA 2015, including personal information of a specific individual or information that identifies a specific individual that may be or is part of the cyber threat indicator, for purposes authorized in section 1504(d)(5)(A).
Data Quality and Integrity	Cybersecurity threats change and evolve over time, sometimes 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 2015.
Security	Federal entities 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 2015, 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 Final Guidelines, as well as the Federal Government Sharing Guidance and the Final Operational Procedures. 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.
Principle	**Privacy and Civil Liberties Final Guidelines Implementation**
	required under section 1506(b), and the Government Accountability Office's independent report on removal of personal information under section 1506(c).

5 Federal Entity Activity

The following provisions apply to the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with CISA 2015. These provisions also include a discussion on defensive measures, notifications, and safeguarding requirements.

Certain federal entities may find it necessary to develop supplemental guidelines to these activities, specific to the policies or rules that are unique to their handling of cyber threat indicators and defensive measures—however, federal entities should be mindful that supplemental guidelines may only add to or provide federal entity-specific clarification to these guidelines, and may not circumvent, or otherwise supersede, these guidelines.

5.1 Defensive Measures

Information that meets the definition of a defensive measure and is shared for a cybersecurity purpose will generally consist of technical data that typically will not contain personal information of a specific individual or information that identifies a specific individual. However, as with cyber threat indicators, they may contain such information, and such defensive measures may be shared with that information included if the personal information is determined to be "directly related to a cybersecurity threat."

While these guidelines, consistent with the requirements of section 1504(b), generally expressly govern only the receipt, retention, use, and dissemination of cyber threat indicators, these guidelines discuss several CISA 2015 requirements relating to the receipt,

retention, use, and dissemination of both defensive measures and cyber threat indicators[9]. When discussing a CISA 2015 requirement that applies expressly to defensive measures in addition to cyber threat indicators, these guidelines will note that fact.

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. Such an approach is also prudent because a defensive measure may include a cyber threat indicator that contains personal information of a specific individual or information that identifies a specific individual[10]. In such instances, these guidelines would apply to the portion of the defensive measure that is a cyber threat indicator.

Accordingly, federal entities are encouraged to review defensive measures, prior to sharing them to assess whether they contain any information. 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. If so, and if that information is not directly related to a cyber threat, the federal entity should 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

Section 1504(b)(3)(B) requires procedures for limiting the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals. 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) known not to be directly related to uses authorized under CISA 2015.

Upon receipt of a cyber threat indicator under CISA 2015, 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 DHS Automated Indicator Sharing (AIS) capability[11] DHS will receive cyber threat indicators and defensive measures through that portal in a standard,

[9] For example, section 1502(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 1502(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 1504(d)(5)(D) (limiting the disclosure, retention, and use of cyber threat indicators and defensive measures to only those authorized uses permitted under CISA).

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

[11] For more information on AIS, please see the AIS PIA, found at: us-cert.cisa.gov/ais. The AIS PIA will be updated, as appropriate.

automated format; apply rules to identify and remove information as described above; and apply unanimously agreed upon controls as described in the Final Operational Procedures before sharing with other Federal entities through the AIS capability. Federal entities that receive cyber threat indicators or defensive measures from DHS through the AIS capability may assume that any information that DHS knew 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 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 Final Guidelines to ensure appropriate handling of cyber threat indicators and defensive measures.

5.3 Notification Procedures

Section 1502(b)(1)(C) 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 2015 that is known or determined to have been shared in error or in contravention of the requirements of CISA 2015, or another provision of federal law or policy, of such error or contravention. In addition, section 1504(b)(3)(E) requires procedures for notifying entities and federal entities if information received pursuant to CISA 2015 is known or determined by a federal entity receiving such information not to constitute a cyber threat indicator. 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 from the disseminating entity 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 originator 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., AIS Submission ID number);
- Identification of the information that is known or determined to have been shared in error or in contravention of the requirements of CISA 2015 or another provision of federal law or policy in accordance with section 1502(b)(1)(C), including any information that does not constitute a cyber threat indicator in accordance with section 1504(b)(3)(E) of CISA 2015; 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 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.cisa.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 2015 or another provision of federal law or policy, including any information that does not constitute a cyber threat indicator.

If utilizing the AIS capability, DHS or another entity may discover 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 2015 or another provision of federal law or policy, including any information that does not constitute a cyber threat indicator or defensive measure. If an entity receiving the information determines that the information is in error or in contravention of the requirements of CISA 2015 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 e-mailing 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.

5.4 Notification to a United States Person

In addition, section 1502(b)(1)(F) 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 2015.

It should be noted that, with regards to the United States person notification requirements in CISA 2015, personal information known or determined to have been shared in violation of CISA 2015 may be incomplete, may not identify a specific individual, or may lack sufficient information to verify that it pertains to, and to contact, 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 1502(b)(1)(F) may not be required because there is insufficient 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 2015 or another provision of federal law, 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 1502(b)(1)(C) and 1504(b)(3)(E), 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 2015, the federal entity should notify the person in accordance with the federal entity's own breach/incident response plan[12]. The federal

[12] Consistent with the Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (January 3, 2017), the head of each Federal agency is required to develop a breach notification policy and plan. Federal entities may rely on their respective breach notification policy and plan for timely notifying United States persons, so long as the policy and plan is

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 2015 received the personal information from another federal entity (which may have also shared the personal information in violation of CISA 2015), the receiving entity should contact the entity that initially shared the information to coordinate notification.

In addition, the disseminating entity shall provide an update to its original submission and redistribute 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 2015.

Based on the type of personal information shared in violation of CISA 2015, 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 1504(d)(5), federal entities that receive cyber threat indicators and defensive measures under CISA 2015 will use them only for the purposes authorized under CISA 2015. 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 (as defined in CISA 2015), including the source of such cybersecurity threat or (ii) a security vulnerability (as defined in CISA 2015);
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).

consistent with the notice requirements in section 1502(b)(1)(F).

5.6 Safeguarding

Section 1502(b)(1)(D) requires procedures for federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures. Further, section 1504(b)(3)(C) requires procedures for safeguarding cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals from unauthorized access or acquisition.

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 to a cybersecurity threat or a use authorized under CISA , from unauthorized access or acquisition. Such controls shall also, to the greatest extent possible, 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 . Recipients of such cyber threat indicators shall be informed that they may only be used for purposes authorized by CISA 2015.

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[13].

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 and its successor publications[14].

5.7 Retention

Federal entities may only retain cyber threat indicators and defensive measures provided to the Federal Government under CISA 2015 for the purposes authorized in section 1504(d)(5)(A) (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 1504(b)(3)(B)(ii) for specific limitations on retention. In accordance with section 1504(b)(3)(B)(i) of CISA 2015, federal entities will also establish a process for the timely destruction, including 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 known not to be directly related to an authorized use under CISA 2015. 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 each federal entity's respective mission while ensuring the appropriate destruction of a cyber threat indicator and defensive measure. Examples of such record schedules include

[13] Pub. L. No. 113-283, 128 Stat 3073 (2014) (codified at 44 U.S.C. §§ 3551–58 et seq.)
[14] Found at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

DHS's National Cybersecurity Protection System (NCPS) DAA-0563-2015- 0008[15] and DAA-0563-2013-0008- 0001[16] records schedules.

5.8 Dissemination and Marking Requirements

Federal entities will disseminate cyber threat indicators only after following the procedures set forth below, consistent with section 1502(b)(1)(E).

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 that (1) 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 (2) is not directly related to a cybersecurity threat. If both of these elements apply to particular information, that 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. 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, at the time of sharing, that information is personal information of a specific individual or information that identifies a specific individual. For example, a federal entity may have reason to know that the "To" line or information on the victim of a spear phishing e-mail is personal information of a specific individual or information that identifies a specific individual (e.g., an individual's full name appearing in the e-mail address). As another example, a federal entity may have reason to know that a username included in a file path may be personal information of a specific individual or information that identifies a specific individual. That information should not be disseminated as part of the cyber threat indicator if it is not directly related to a cybersecurity threat, as described below.

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

Section 1501(5) defines a cybersecurity threat (in part) as an "action … that may result in an unauthorized effort to adversely impact [an information system's] security, availability, confidentiality, or integrity …" Personal information directly related to a cybersecurity threat includes information that is necessary to detect, prevent, or mitigate the cybersecurity threat.

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

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

Other information that the federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual, such as the names and e-mail addresses of the recipients of the e-mail (i.e., the "To" address), would typically be personal information not directly related to a cybersecurity threat, and therefore should usually not be disseminated as part of the cyber threat indicator[17].

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.

If utilizing the AIS capability, brokering of cyber threat indicators and defensive measures between non-federal entities and participating federal entities will be done through existing Enhance Shared Situational Awareness (ESSA)[18] Community arrangements[19] within the ESSA Information Sharing Architecture (ISA)[18]. 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)[20]. 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 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 2015 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 participating federal entities or with the entire AIS community. The CISA 2015 Proprietary marking can also be used by non-federal entities.

The technical procedures and requirements for these markings are defined in the ESSA/ISA ACS and may be modified with updates to this document[21].

6 Sanctions

Section 1504(a)(3)(C)(ii) requires that procedures ensure there are appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under CISA 2015 in an unauthorized manner. Further, section 1504(b)(3)(C) requires procedures for appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of the safeguarding guidelines discussed in Section [5.6], above. Failure by an individual to abide by the requirements set forth in these guidelines will result in appropriate sanctions applied to that individual in accordance with their

[17] The ESSA Program Management Team was stood down in 2016. Accordingly, governance of ESSA has been transferred to DHS to organize and manage a successor organization.

[18] ESSA community arrangements are agreed upon by an inter-agency process and enable cyber information sharing, handling, and protections as codified in the Multilateral Information Sharing Agreement (MISA).

[19] The ESSA ISA is the common architecture for sharing as documented in the ISA Shared Situational Awareness (SSA) Requirements Document v2.1.

[20] The ESSA/ISA ACS are the common access controls enabling sharing trust communities as documented in the ISA ACS v2.0, which supplements the ISA SSA Requirements Document.

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

department or 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, a federal entity determines that classified or other sensitive national security information is present, the federal entity must take appropriate steps to safeguard and protect such information against unauthorized access, use, and disclosure, in accordance with applicable Executive Orders and directives.

8 Audit

Section 1504(a)(3)(C)(i) requires procedures to ensure that audit capabilities are in place. CISA 2015 sets forth multiple auditing requirements, which are restated below. Agencies shall ensure they maintain records sufficient to enable the assessments described below.

Section 1506(b) provides that, not later than 2 years after the date of the enactment of CISA 2015 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 2015 during the most recent 2-year period.

In accordance with the provisions related to privacy and civil liberties in section 1506(b)(2), 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 CISA 2015, including the following:

    - The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 1504(c).
    - An assessment of any information that is personal information of a specific individual or information identifying a specific individual that is not directly related to a cybersecurity threat and was shared by a non-federal government entity with the Federal Government in contravention of CISA 2015, or was shared within the Federal Government in contravention of the guidelines required by CISA 2015, including a description of any significant violation of CISA 2015.
    - The number of times, according to the Attorney General, that information shared under CISA 2015 was used by a federal entity to prosecute an offense listed in section 1504(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 that was personal information of a specific individual or information that identified a specific individual and was not directly related to a cybersecurity threat in accordance with the procedures required by section 1504(b)(3)(E).

- The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under CISA 2015 on the privacy and civil liberties of United States persons.

In addition, CISA 2015 provides that, not later than 3 years after the date of the enactment of CISA 2015 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 2015. Such report was to include an assessment of the sufficiency of the policies, procedures, and guidelines established under CISA 2015 in addressing concerns relating to privacy and civil liberties. The Comptroller General submitted this report to Congress on December 6, 2018, and found federal agencies met legislative requirements for protecting privacy when sharing information under CISA 2015, including the requirements related to the development of policies, procedures, and guidelines[22].

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 1506(b) and the Government Accountability Office's independent report on removal of personal information.

[22] GAO, Federal Agencies Met Legislative Requirements for Protecting Privacy When Sharing Threat Information, GAO-19-114R (Dec. 6, 2018), www.gao.gov/products/GAO-19-114R.

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).

Appendix B: Previous Summaries of Changes

DHS and DOJ will continue to review these Privacy and Civil Liberties Final Guidelines for necessary updates no less than every 2 years, as required by CISA 2015. If the periodic review results in a new edition, the previous summary of changes will appear in this Appendix.

The following summarizes the changes to the original guidance that were made pursuant to the 2018 review:

Overall, the 2018 joint review of the CISA 2015 Privacy and Civil Liberties Final Guidelines resulted in only minor administrative changes to the Privacy and Civil Liberties Final Guidelines issued in 2016. In particular:

- In Section 5, "Federal Entity Activity," DHS and DOJ updated the text to clarify that federal entities receiving, retaining, using, or disseminating cyber threat indicators or, where applicable, defensive measures may develop supplemental guidance to the Privacy and Civil Liberties Final Guidelines specific to the policies or rules unique to their

  entities' handling of cyber threat indicators and defensive measures. These supplemental guidelines, however, may not circumvent, or otherwise supersede, the Privacy and Civil Liberties Final Guidelines.

- In Section 5.3, "Notification Procedures," DHS and DOJ removed text stating that DHS would send periodic submission disposition reports to federal entity submitters providing notification of what fields were and were not accepted for dissemination. During the review, it was determined that these reports are not provided in practice, as feedback to federal entity submitters is conducted agency by agency, rather than through the structured process previously described. Accordingly, the text was removed.

- In Section 5.8, "Dissemination and Marking Requirements," DHS and DOJ revised the example under subsection 2 to better explain whether a 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.

- Lastly, DHS and DOJ made minor revisions throughout to, among other things, correct outdated footnotes and web links, where necessary.