9110-9P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate; Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents – Notice of Availability

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice of availability.

SUMMARY: DHS is announcing the availability of Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents jointly issued with the Department of Justice (DOJ) in compliance with the Act (CISA), which authorizes the voluntary sharing and receiving of cyber threat indicators and defensive measures for cybersecurity purposes, consistent with certain protections, including privacy and civil liberty protections.

ADDRESSES: The CISA guidance documents may be found on www.us-cert.gov/ais.

FOR FURTHER INFORMATION CONTACT: If you have questions about this notice, email Matthew Shabat at matthew.shabat@hq.dhs.gov or telephone on (703) 235-5338. Questions may also be directed by mail to Matthew Shabat, 245 Murray Lane, S.W., Mail Stop 0610, Washington, DC 20528-0610.

SUPPLEMENTARY INFORMATION: The CISA requires the Secretary of DHS and the Attorney General to jointly develop and make publicly available –

- guidance to assist non-Federal entities and promote sharing of cyber threat indicators with the Federal Government;
- interim and final guidelines for the protection of privacy and civil liberties; and
- interim and final procedures related to the receipt of cyber threat indicators and defensive measures by the Government, which happen principally through the

real-time DHS process, the existing DHS-operated Automated Indicator Sharing (AIS) initiative and may also occur through direct submissions to Federal agencies.

The CISA also requires the Secretary of DHS, the Attorney General, the Director of National Intelligence, and the Secretary of Defense, to jointly develop interim procedures to facilitate and promote the sharing of cyber threat indicators and defensive measures by the Federal Government.

Authority and Background

On December 18, 2015, the President signed into law the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, which included at Division N, Title I the Cybersecurity Information Sharing Act of 2015 (CISA). Congress designed CISA to establish a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators and defensive measures while protecting privacy and civil liberties. The CISA requires various Executive Branch agencies to coordinate and create, within 60 days of enactment (i.e., not later than February 16, 2016), four guidance documents to facilitate this voluntary cybersecurity information sharing process. The CISA requires two of these interim documents to be made publicly available. See generally Pub. L. No. 114-113, Div. N, Title I secs. 103, 105).

Overview of the 60 Day Guidance Required under CISA

The CISA sec. 103 requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation

with the heads of designated Federal entities,[1] to jointly develop and issue procedures to facilitate and promote the sharing by the Federal Government of classified and unclassified cyber threat indicators, defensive measures, and other information and best practices related to mitigating cyber threats. The CISA sec. 103(b) requires these procedures to include a real-time sharing capability (namely the DHS Automated Indicator Sharing (AIS) initiative); incorporate existing Federal information sharing processes, procedures, roles, and responsibilities to the greatest extent possible; account for sharing done in error; and protect against unauthorized access to cyber threat information. Further, the procedures must account for the review of cyber threat indicators to identify personal information not related to the threat, a technical capability to remove such personal information, and a notification process to alert any U.S. person whose personal information is improperly shared by a Federal entity.

The CISA sec. 105(a)(1) requires the Secretary of Homeland Security and the Attorney General, in consultation with the heads of designated Federal entities, to jointly develop and issue interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government. These internal operational procedures describe general rules applicable to DHS and other Federal agencies and the operative processes of the DHS AIS system, including the statutory requirement for Federal agencies that receive cyber threat indicators and defensive measures to share them with other appropriate agencies.

The CISA sec. 105(a)(4) requires the Secretary of Homeland Security and the

[1] The CISA defines Appropriate Federal Entities as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence. See CISA sec. 102(3).

Attorney General to jointly develop and make publicly available guidance to assist non-Federal entities with sharing cyber threat indicators with Federal entities. This guidance includes explanations of how non-Federal entities can identify and share cyber threat indicators and defensive measures with the Federal Government in accordance with CISA and describes the protections non-Federal entities receive under CISA for sharing cyber threat indicators and defensive measures, including targeted liability protection and other statutory protections.

Finally, CISA sec. 105(b) requires the Secretary of Homeland Security and the Attorney General, in consultation with the Department Heads and Chief Privacy and Civil Liberties Officers of the designated Federal entities, to jointly develop and make publicly available interim guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity. These privacy and civil liberties guidelines are consistent with the Fair Information Practice Principles (FIPPs) set forth in Appendix A of the "National Strategy for Trusted Identities in Cyberspace," published by the President in April 2011.

Issuance of Agency Guidance required under CISA

The CISA guidance documents may be found on www.us-cert.gov/ais.

Dated: February 11, 2016. .

Andy Ozment,
Assistant Secretary,
Department of Homeland Security.
[FR Doc. 2016-03430 Filed: 2/17/2016 8:45 am; Publication Date: 2/18/2016]

The Office of the Director of National Intelligence
The Department of Homeland Security
The Department of Defense
The Department of Justice

Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015

February 16, 2016

This Page Intentionally Left Blank

Table of Contents

1 Purpose 4
1.1 Consultation 6
2 Definitions 6
3 Background 6
4 Timely Sharing of Classified Cyber Threat Indicators and Defensive Measures (Section 103(a)(1)) 7
5 Timely Sharing of Declassified Cyber Threat Indicators and Defensive Measures (Section 103(a)(2)) 9
6 Timely Sharing of Unclassified Cyber Threat Indicators and Defensive Measures (Section 103(a)(3)) 10
7 Timely Sharing of Information Relating to Cyber Threats (Section 103(a)(4)) 13
8 Periodic Sharing of Cybersecurity Best Practices (Section 103(a)(5)) 14
9 General Procedures Supporting the Sharing of Cyber Threat Indicators/Defensive Measures 17
9.1 Sharing in Real-time (Section 103(b)(1)(A)) 17
9.2 Roles and Responsibilities -- Federal Entities/Non-Federal Entities/ISACs and ISAOs (Section 103(b)(1)(B)) 17
9.2.1 Federal Entities 17
9.2.2 Non-Federal Entities 18
9.3 Notification of Cyber Threat Indicators/Defensive Measures Error (Section 103(b)(1)(C)) 19
9.4 Protection of Unauthorized Access to Cyber Threat Indicators/Defensive Measures (Section 103(b)(1)(D)) 19
9.5 Personal Information Review and Removal (Section 103(b)(1)(E)) 19
9.6 Privacy/Civil Liberties Violation Notification (Section 103(b)(1)(F)) 20
Appendix A: Acronyms 21

1 Purpose

Section 103 of the Cybersecurity Information Sharing Act of 2015, Pub. L. 114-113, 129 Stat.694 (2015), directs the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate federal entities set forth in Subsection 1.1, to jointly develop and issue procedures to facilitate and promote:

1. Timely sharing of classified cyber threat indicators (CTIs) and defensive measures (DMs) in the possession of the Federal Government with representatives of relevant federal entities and non-federal entities that have appropriate security clearances;
2. Timely sharing with relevant federal entities and non-federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government that may be declassified and shared at an unclassified level;
3. Timely sharing with relevant federal entities and non-federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;
4. Timely sharing with federal entities and non-federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and
5. Periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in Section 3 of the Small Business Act (15 U.S.C. 632)).

The procedures outlined in this document describe the current mechanisms through which the appropriate federal entities, as named in Section 102(3), share information with non-federal entities.[1] Examples of non-federal entities are private sector entities and state, local, tribal and territorial (SLTT) governments, including owners and operators of private and public critical infrastructure. These procedures are implemented today through a series of programs, which are described below and provide the foundation of appropriate federal entities' cybersecurity information sharing capability. These programs are dynamic and are expected to grow or evolve over time.[2] That said, some programs may be discontinued and new programs may begin. In addition, these programs work together to identify useful information available through their unique information sources and to share that information with their respective partners. Wherever possible, appropriate federal entities coordinate with each other through these programs to ensure that the information they share is timely, actionable, and unique.

[1] Section 103 stipulates that procedures should "incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers."

[2] However, the documentation of these procedures, in line with Section 103, does not imply the commitment of additional resources by these federal entities.

Federal entities are encouraged to share CTIs and DMs as broadly and as quickly as possible. Whether CTIs and DMs are classified, declassified or unclassified, federal entities should continuously identify and implement programs to share such CTIs and DMs with each other and with non-federal entities.

Federal entities engaging in activities authorized by CISA, including those referenced within this document, 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.

In furtherance of this general encouragement to share broadly and quickly, federal entities shall establish and maintain procedures; and consistent with those procedures, maintain programs that:

1. Facilitate the timely sharing of classified CTIs and DMs in the possession of the Federal Government with representatives of relevant federal entities and non-federal entities that have appropriate security clearances.
2. Share with other relevant federal entities and non-federal entities CTIs, DMs, and information relating to cybersecurity threats in their possession that may be declassified and shared at an unclassified level. Such sharing is consistent with the emphasis placed by the President and the Director of National Intelligence on the need to ensure the timely and efficient flow of CTIs and DMs to appropriate federal and non-federal entities and shall be conducted consistent with all applicable Executive Orders and directives.
3. Support the timely sharing with relevant federal entities and non-federal entities, or the public if appropriate, of unclassified, including controlled unclassified, CTIs and DMs in the possession of the Federal Government.
4. Support the timely sharing with federal entities and non-federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under CISA, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats.
5. Support the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of CTIs, DMs, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns.

This document sets forth relevant procedures, or otherwise references exemplar activities that have implemented such procedures. In addition, this document provides that federal entities will share with each other as a means of also sharing more broadly with non-federal entities since many federal entities maintain unique relationships with different cross-sections of the Nation, such as critical infrastructure sectors, regulated industries or State and local governments. Finally, this document recognizes that broad sharing within components of a federal entity can be just as important as broad sharing between federal entities.

1.1 Consultation

In developing the procedures required under this section, the DNI, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General have consulted with the following appropriate federal entities, including the Small Business Administration and the National Laboratories (as defined in Section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of CTIs by the Federal Government in a timely manner.

- The Department of Commerce
- The Department of Energy
- The Department of the Treasury
- The Small Business Administration
- The National Laboratories
    1. Ames Laboratory
    2. Argonne National Laboratory
    3. Brookhaven National Laboratory
    4. Fermi National Accelerator Laboratory
    5. Idaho National Laboratory
    6. Lawrence Berkeley National Laboratory
    7. Lawrence Livermore National Laboratory
    8. Los Alamos National Laboratory
    9. National Energy Technology Laboratory
    10. National Renewable Energy Laboratory
    11. Oak Ridge National Laboratory
    12. Pacific Northwest National Laboratory
    13. Princeton Plasma Physics Laboratory
    14. Sandia National Laboratories
    15. Savannah River National Laboratory
    16. Stanford Linear Accelerator Center
    17. Thomas Jefferson National Accelerator Facility

2 Definitions

The definitions in Section 102 of the Cybersecurity Information Sharing Act of 2015 (CISA) shall apply to the same terms contained in this document. Any additional defined terms are set forth in the provisions below.

3 Background

On December 18, 2015, the President signed the Cybersecurity Information Sharing Act of 2015 (CISA) into law. Congress designed CISA to create a voluntary cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties. CISA requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of appropriate federal entities, to jointly develop and issue procedures to facilitate and promote the sharing of classified and unclassified CTIs and DMs by the Federal Government and other information and best practices related to mitigating cyber threats. This document fulfills that requirement.

4 Timely Sharing of Classified Cyber Threat Indicators and Defensive Measures (Section 103(a)(1))

It is the policy of the U.S. Government to make every reasonable effort "to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity."[3] Sharing of cyber threat information that is classified, however, is dependent upon the recipient's security clearance level and must be performed in accordance with applicable policy and protection requirements for intelligence sources, methods, operations, and investigations, which are not superseded by this document. Any federal entity sharing classified information must continue to conform to existing classification standards and adhere to handling restrictions, like Originator Controlled (ORCON) markings or specific originator instructions on use of downgraded information, when determining what information can be shared with any entity. Given the protections for and sensitive nature of classified information, additional emphasis must be placed on coordination early in the process, with originators of specific classified information deemed necessary to share with an entity.

When appropriate, agency heads are expected to continue using the emergency authority granted in 32 CFR Section 2001.52, promulgated pursuant to Executive Order 13526 – *Classified National Security Information*, to disseminate and transmit classified information during certain emergency situations, in which there is an imminent threat to life or in defense of the homeland, to those who are otherwise not routinely eligible for access.

The following programs are a non-exhaustive set of examples that use current procedures to support the timely sharing of classified CTIs and DMs in the possession of the Federal Government with representatives of relevant federal entities and non-federal entities that have appropriate security clearances.

- Department of Homeland Security (DHS) Enhanced Cybersecurity Services (ECS) Program -- http://www.dhs.gov/enhanced-cybersecurity-services

  The DHS ECS program is a voluntary information sharing program that assists U.S.-based public and private entities as they improve the protection of their computer systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the Federal Government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops CTIs based on this information and shares them with qualified commercial service providers (CSPs), thus enabling them to better protect their customers. ECS augments, but does not replace, entities' existing cybersecurity capabilities.

  The ECS program does not involve government monitoring of private networks or communications. Under the ECS program, information relating to cyber threats and malware activities detected by the CSPs is not directly shared between CSP customers and the Federal Government. However, when a CSP customer voluntarily agrees, the CSP may share limited and anonymized information with DHS.

[3] EO 13636 Section 4(a), Cybersecurity Information Sharing.

In February 2013, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, expanded ECS to each of the 16 critical infrastructure sectors. As a result of increased demand and need for cybersecurity protection across the nation, the ECS program has since expanded further and now allows approved CSPs to extend their ECS customer base to all U.S.-based public and private entities.

- Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity (CS) Program –32 CFR Part 236, http://dibnet.dod.mil/

  The DIB CS Program was initiated in 2007 and established as a permanent DoD program in 2013 under 32 Code of Federal Regulations, Part 236, to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified networks or information systems. Under the voluntary DIB CS program, DoD and DIB participants share cyber threat information in order to enhance the overall security of unclassified DIB networks, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness.

  The DoD Cyber Crime Center (DC3) serves as the operational focal point for the DIB CS program, sharing cyber threat information with DIB participants in near real-time at both the classified and unclassified levels. Participating companies receive analytic support, incident response, mitigation and remediation strategies, malware analysis, and other cybersecurity best practices.

  Information shared between DoD and the DIB under the DIB CS Program strengthens the Nation's knowledge of the ever-growing cyber threat, increases the effectiveness of mitigating the risk, and meets the Administration's and DoD's strategic objective of enhancing voluntary government-private sector cyber threat information sharing.

- DHS Cyber Information Sharing and Collaboration Program (CISCP) -- http://www.dhs.gov/ciscp
  The Cyber Information Sharing and Collaboration Program (CISCP) is DHS's flagship program for public-private information sharing and complement ongoing DHS information sharing efforts. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities. To join CISCP, companies are required to sign a Cooperative Research and Development Agreement (CRADA). Along with governing participation in CISCP, a signed CRADA may permit access to the National Cybersecurity and Communications Integration Center (NCCIC) watch floor and allows for company personnel to be eligible for security clearances to view classified threat information.

- The National Cyber Investigative Joint Task Force (NCIJTF) is a Presidentially-mandated multi-agency cyber center that coordinates, integrates, and shares information related to cyber threat investigations and operations. The NCIJTF currently has signed memoranda of understanding (MOUs) with approximately 24 member agency representatives, which allow for sharing of cyber threat information—to include classified CTIs—at the NCIJTF. The appropriate federal entities identified under Section 102(3) are current members of the NCIJTF with signed MOUs.

The NCIJTF has several existing mechanisms for sharing classified CTIs to the appropriate federal entities, as members of the NCIJTF. CyWatch, the NCIJTF's 24/7 watch floor, serves as the primary mechanism for sharing classified CTIs with federal entities that are NCIJTF members. In addition, the NCIJTF's Office of Threat Pursuit analyzes collected cyber threat data and provides reports on exfiltrated data, which are shared with member agencies. Lastly, the Office of Campaign Coordination facilitates the sharing of classified CTIs and DMs related to campaign missions among participating agencies.

The NCIJTF also provides classified threat briefings to both federal entities and non-federal entities, to include cleared private sector representatives. Briefings are determined on an ad-hoc basis.

- In addition to sharing through the NCIJTF, the FBI utilizes on-site briefings to share classified indicators and defensive measures with industry and appropriate private sector entities. Coordinating with its other government agency partners, the FBI provides potential or known victim entities with temporary security clearances so they may have access to specific classified information and technical indicators that may be used to neutralize an ongoing threat. Oftentimes, the technical information exchanged is accompanied by a contextual briefing to emphasize the severity of the threat.

5 Timely Sharing of Declassified Cyber Threat Indicators and Defensive Measures (Section 103(a)(2))

To implement sharing CTIs, DMs, and information relating to cybersecurity threats in their possession that may be declassified and shared at an unclassified level, federal entities are encouraged to downgrade, declassify, sanitize or make use of tearlines to ensure dissemination of cyber threat information to the maximum extent possible. In addition, federal entities that are also members of the Intelligence Community, in accordance with their respective policies and procedures, should follow the guidance in Intelligence Community Directive 209 concerning tearline production and dissemination, as well as all other applicable procedures, as appropriate.

The following programs and efforts are a foundational set of examples that use current procedures to support timely sharing with relevant federal entities and non-federal entities of CTIs, DMs, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government that may be declassified and shared at an unclassified level.[4]

- DHS National Cybersecurity and Communications Integration Center (NCCIC) -- https://www.dhs.gov/nccic

  During the ordinary course of operations, the NCCIC may receive classified CTIs, DMs and information relating to cybersecurity threats from other federal entities. Through its own analysis, or in consultation with federal or non-federal entities with appropriate security clearances, the

[4] Originating agencies retain authority over classification decisions and each has its own procedures for handling downgrade/release requests.

NCCIC may identify a requirement to share the information more broadly than classification restrictions permit. In such cases, the NCCIC works with the originating federal entity to downgrade, sanitize, or otherwise declassify information for sharing with its stakeholders through indicator bulletins and other channels. The NCCIC establishes standing critical information requirements so that its federal entity partners have a sense of the CTIs, DMs, and information relating to cybersecurity threats that are of the greatest interest to the NCCIC and its federal and non-federal entity stakeholders.

- FBI Private Industry Notifications (PINs) and FBI Liaison Alert System (FLASH) Reports

  Working with its interagency partners and the Intelligence Community writ large, the FBI works to declassify both contextual and technical information for dissemination to private industry through Private Industry Notifications (PINs) and FBI Liaison Alert System (FLASH) reports. PINs and FLASHes convey industry-specific details about current or emerging cyber threats and trends, along with high-level analytical or technical information of use to the recipient to identify the threat. PINs provide contextual information regarding a threat and may contain information about tactics, techniques, and procedures or other information regarding a cyber threat. FLASH reports provide technical reporting to interagency and industry for immediate action against an ongoing threat and contribute to investigative efforts. Additionally, the FBI, along with other agencies, disseminates unclassified Joint Intelligence Bulletins (JIBs), which also provide cyber threat information.

- Department of Energy (DOE) Cybersecurity Risk Information Sharing Program (CRISP)

  The DOE's CRISP is a unique public-private sector partnership that combines, 1) high fidelity (private sector) sensor devices, 2) government enrichment and analysis of the cyber threat (integrating Intelligence Community resources and analysis with the parallel generation of both classified and tear line information), 3) automated generation of machine consumable CTIs and DMs (leveraging Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)), with 4) a robust data sharing matrix that addresses the policy side of information sharing.

6 Timely Sharing of Unclassified Cyber Threat Indicators and Defensive Measures (Section 103(a)(3))

In general, federal entities should make unclassified CTIs and DMs broadly available to each other and to non-federal entities, subject to any specific handling instructions associated with a particular CTI or DM. To the extent a federal entity receives a CTI or DM from a non-federal entity in a manner other than the real-time process described in Section 105(c) of CISA, the recipient federal entity shall share such CTI or DM with each appropriate federal entity as quickly as operationally practicable, consistent with applicable law and the mission of those entities. This may be accomplished by sharing the CTI or DM through the DHS Automated Indicator Sharing initiative described below. To implement sharing of unclassified CTIs and DMs, federal entities are encouraged to declassify, sanitize or make use of tearlines in accordance with their respective policies and procedures.

The following programs are a foundational set of examples that use current procedures to support timely sharing with relevant federal entities and non-federal entities, or the public if appropriate, of unclassified, including controlled unclassified CTIs and DMs in the possession of the Federal Government.

- DHS Automated Indicator Sharing initiative (AIS) -- https://www.us-cert.gov/ais
  AIS is the Federal Government's primary mechanism to exchange unclassified CTIs and defensive measures with the private sector. DHS developed AIS to enable the automated exchange of CTIs between and among federal entities and non-federal entities in order to allow participants to quickly mitigate cyber threats.

  AIS connects participating organizations to a DHS-managed system that allows bi-directional sharing of CTIs, enhancing the ability of the Federal Government and its partners to block cyber adversaries before intrusions occur and identify ongoing cyber incidents. AIS not only shares DHS-developed CTIs and DMs, but also allows other federal entities and non-federal entities to share threat indicators they have observed in their own network defense efforts. This information sharing "ecosystem" helps DHS and other participating federal entities with cybersecurity responsibilities build a common, shared knowledge of current cyber threats, helping to protect our public health and safety, national security, and economic security.

  AIS leverages DHS-led standards for machine-to-machine communication and lessons learned from existing DHS information sharing programs to build the framework for this capability. DHS also utilizes feedback from participants to strengthen its ongoing implementation.

Other Federal Government programs also share CTIs with the private sector. The Federal Government shall ensure that unclassified indicators made available in these programs are also shared through AIS. Examples of such unclassified information sharing programs include:

- DHS Cyber Information Sharing and Collaboration Program (CISCP) via AIS -- http://www.dhs.gov/ciscp

  CISCP was established for information sharing and collaboration with DHS's critical infrastructure partners. CISCP shares cyber threat, incident, and vulnerability information in near-real time, and enhances collaboration in order to better understand the threat and improve network defense for the entire community. The key focus of this program is to establish a community of trust between the Federal Government and entities from across the different critical infrastructure sectors and then leverage these relationships for enhanced information sharing and collaboration.

  To join CISCP, partners such as Information Sharing and Analysis Centers (ISACs) and the stakeholder community—which consists of mature critical infrastructure owners and operators—sign a CRADA. The majority of sharing among CISCP participants is at the unclassified level.

- DHS National Cybersecurity and Communications Integration Center (NCCIC) -- https://www.dhs.gov/nccic

The NCCIC's United States Computer Emergency Readiness Team (US-CERT) publicly shares a series of unclassified alerts and bulletins to provide timely information about current security issues, vulnerabilities, and exploits, as well as weekly summaries of new vulnerabilities along with patch information when available. In addition, the US-CERT Portal provides a secure, web-based, collaborative system to share sensitive, cyber-related information and news with participants in the public and private sector, including Government Forum of Incident Response and Security Teams (GFIRST), the Chief Information Security Officer Forum, ISAC members, and various other working groups. Authorized users can visit the US-CERT Portal. Similarly, the NCCIC's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) publicly shares a series of unclassified alerts and advisories to provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks, as well as information about current security issues, vulnerabilities, and exploits.

- DOD Defense Industrial Base (DIB) Cybersecurity (CS) Program -- http://dibnet.dod.mil/

  Under the voluntary DIB CS program, DoD and DIB participants share cyber threat information in order to enhance the overall security of unclassified DIB networks, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness.

  Participating companies receive analytic support, incident response, mitigation and remediation strategies, malware analysis and other cybersecurity best practices.

- FBI National Cyber Investigative Joint Task Force (NCIJTF) -- https://www.fbi.gov/about-us/investigate/cyber/ncijtf

  The NCIJTF's CyWatch disseminates PINs and FLASH messages to private sector entities and state and local law enforcement. PINs and FLASHes are unclassified, but are released only to authorized recipients through secure channels. CyWatch also disseminates unclassified CTIs to NCIJTF member agencies. This includes the dissemination of products that aggregate data on victim notifications and identify cyber threat activity by sector.

  The NCIJTF Office of Campaign Coordination coordinates, on an ad hoc basis, the sharing of unclassified cyber threat indicators and defensive measures relevant to campaigns between federal campaign partners and private industry partners.

  The FBI also leverages its 56 field offices, internal outreach programs, other agency cyber centers, and the InfraGard portal to disseminate unclassified PINs and FLASH reports, based on TLP protocols to a wide variety of industry partners.

- DOE Cybersecurity Risk Information Sharing Program (CRISP) – See description above.

- DOE Cyber Fed Model (CFM) Program – The DOE CFM program provides machine-machine automated indicator sharing 1) internal to DOE, 2) externally with other federal departments and agencies, and 3) within and across the energy sector.

- Treasury's Financial Sector Cyber Intelligence Group (CIG) disseminates information about cybersecurity threats and vulnerabilities that is only available through law enforcement and other protected government channels. This information is shared with the financial sector at the unclassified level, in bulletins called Circulars. CIG Circulars contain information on sophisticated threat actors that could cause damage to the financial sector. The Financial Services Information Sharing and Analysis Center is a key partner to disseminate this information to the financial sector. The Circulars are also available on the DHS Homeland Security Information Network portal under Financial Services, and include STIX files to enable automated indicator sharing. The CIG also shares information in response to the financial sector Requests for Information (RFIs) and that it identifies through proactive searches of United States Government holdings.

7 Timely Sharing of Information Relating to Cyber Threats (Section 103(a)(4))

Under Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, Section 4(b) -- *Process for Dissemination of Cyber Threat Information to Specific Targeted Critical Infrastructure Entities*, the Federal Government developed a process to facilitate notifications to entities affected by malicious cyber activity. This process, consistent with the need to protect national security information, includes the dissemination of classified reports to critical infrastructure entities authorized to receive them. Consistent with Section 103(a)(4) of CISA, federal entities should similarly notify any non-federal entity known to be, or reasonably expected to be affected by malicious cyber activity, not only those that are critical infrastructure entities. Consistent with EO 13636 Section 4(b) processes, participating federal entities will coordinate to identify the entities with primary sharing responsibility for a particular event. Similarly, and as outlined below, participating federal entities will ensure coordination and de-confliction associated with outreach to targeted entities or victims.

Section 4(b) process includes four phases:

1. Pre-Event Activities – This describes the activities performed within a 4(b) participant organization prior to generating an event. This includes the development of a cybersecurity threat report and the decision to generate an event based on a risk prioritization assessment of the cybersecurity threat information.
2. Create Event – This describes the creation of a 4(b) event and the activities that are initiated by the support capability.
3. Notification Planning – This describes the activities from event creation up to the point of notification.
4. Notification and Disposition – This describes the activities directly associated with notification and the follow-on response activities as well as final disposition of the event.

The 4(b) process has two "timer windows" that help ensure that the notification decisions are executed in a timely manner based on the risk prioritization and 4(b) participant inputs. The two "timer windows" are:

1. Incident to Create Event – This is the time from receipt and assessment of the initial cybersecurity threat information, the development of a cybersecurity threat report, the decision to enter this report into the 4(b) process by generating a 4(b) event. The process can be exited if the decision is

made that the incident's cybersecurity threat information does not have sufficient specificity, or present sufficient risks, where entry in to the 4(b) process is warranted.

2. Create Event to Notify – This is the time from the creation of a 4(b) event to formal notification. The value is based on the reassessed risk assessment. A "No Notify" decision based on an operational equity concern, insufficient resources, or inability for secure communications would exit the process after the reasons are documented in the Disposition Record.

Federal Government entities using the 4(b) process include:

- DHS National Cybersecurity and Communications Integration Center (NCCIC) -- https://www.dhs.gov/nccic
- DOD Defense Cyber Crime Center (DC3) -- http://www.dc3.mil/
- FBI National Cyber Investigative Joint Task Force (NCIJTF) -- https://www.fbi.gov/about-us/investigate/cyber/ncijtf

  The NCIJTF's CyWatch maintains responsibility for managing Cyber Guardian, the designated EO 13636 4(b) tracking system used by the FBI, Federal Cyber Centers, and participating sector-specific agencies to coordinate information that is provided to organizations when they are identified as a targeted entity in cyber threat reports. Cyber Guardian encompasses a comprehensive platform for real-time intake and management of criminal and national security cyber threat reporting against sector-specific targeted entities. The system will have the capability to provide both classified and unclassified reports to affected private sector organizations.

  Cyber Guardian consists of three platforms: Cyber Guardian, iGuardian, and eGuardian. Cyber Guardian, and establishes a unified system of reporting, allowing synchronized victim contact and more effective and timely incident notification to targeted entities. The program ensures that more meaningful information is provided to victims, to include intruder as well as network activity where possible. Tracking of incident information in Cyber Guardian also allows for aggregated sector-specific incident data analysis.

  iGuardian provides trusted industry partners within the critical infrastructure sectors with a platform for reporting cyber intrusion incidents and submitting malware. Industry partners use an unclassified import form on a trusted Internet connection.

  eGuardian is a sensitive but unclassified system implemented in 2008, to allow for reporting and sharing of suspicious activity among SLTTs law enforcement partners and the FBI's Joint Terrorism Task Forces (JTTFs). The system was enhanced in 2013 to allow events and suspicious activity involving computer intrusions to be reported to the FBI's Cyber Task Forces (CTFs). eGuardian is accessible only to sworn law enforcement officers and support employees with a counterterrorism function.

8 Periodic Sharing of Cybersecurity Best Practices (Section 103(a)(5))

The following programs, activities, and offices support the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of CTIs, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in

the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in Section 3 of the Small Business Act (15 U.S.C. 632)).

Examples of periodic sharing of best practices include:

- Department of Commerce (DOC)'s National Institute of Standards and Technology (NIST) -- http://www.nist.gov/itl/csd/

  NIST Special Publications and Interagency Reports provide management, operational, and technical security guidelines for federal agency information systems, and cover a broad range of topics. Beyond these documents—which are peer-reviewed throughout industry, government, and academia—NIST conducts workshops, awareness briefings, and outreach to ensure comprehension of standards and guidelines, to share ongoing and future activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner. In addition, NIST maintains the National Vulnerability Database (NVD), a repository of standards-based vulnerability management reference data. The NVD makes available information on vulnerabilities, impact measurements, detection techniques, and remediation assistance. It provides reference data that enable government, industry and international security automation capabilities.

- Critical Infrastructure Cyber Community ($C^{3)}$ Voluntary Program -- https://www.dhs.gov/ccubedvp

  The C³ (pronounced "C Cubed") Voluntary Program assists the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the NIST's Cybersecurity Framework (the Framework), released in February 2014. The C³ Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework.

  The C³ Voluntary Program helps sectors and organizations that want to use the Framework by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector.

- DHS National Cybersecurity and Communications Integration Center (NCCIC) -- https://www.dhs.gov/nccic

  The NCCIC shares publications and tips, which include recommended practices, standards, and references for technical and non-technical users. Information is available for government users, as well as owners, operators, and vendors of control systems. In addition, the NCCIC includes information specifically focused on securing small business and home networks. The information is based on analyses conducted within the NCCIC and also analyses and recommendations produced across the public and private sectors.

  - Information for government users can be found at: https://www.us-cert.gov/government-users
  - Information for control system users and vendors can be found at: https://ics-cert.us-cert.gov/

- Information for small and medium businesses and home users can be found at: https://www.us-cert.gov/home-and-business

Through the US-CERT website, DHS also offers the Cyber Resilience Review (CRR), which is a no-cost, voluntary, non-technical assessment to evaluate an organization's resilience and cybersecurity practices. The CRR may be conducted as a self-assessment, or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of 10 domains, including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience, as well as provide a gap analysis for improvement based on recognized best practices. After a CRR, participants will receive a report that includes options for consideration that provide general guidance aimed at increasing an enterprise's cybersecurity posture and preparedness. This report may be used to support decision-making and help formulate cybersecurity investment justifications. The CRR report is for the enterprise's use only and DHS does not share the results. This information is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program http://dhs.gov/pcii. For additional information, visit http://www.us-cert.gov/ccubedvp/self-service-crr.

- DOD Defense Industrial Base (DIB) Cybersecurity (CS) Program -- http://dibnet.dod.mil/

  The DIB CS program shares actionable unclassified cyber threat information, including indicators, best practices and mitigation strategies with DIB participants through DoD's secure web portal. DoD also shares classified cyber threat contextual information electronically with DIB participants through a secret-level web portal accessible to participating DIB company representatives. DC3 receives cyber incident reporting from the DIB and analyzes the information leveraging both industry and Federal Government sources to provide information back to the DIB participants that can mitigate adversary activity. This program focuses on threat to the DIB.

- The FBI shares cybersecurity best practices with private industry and other government agencies through both unclassified and classified briefings and PINs, FLASHes, and JIBs. Additionally, through information sharing programs throughout headquarters, including InfraGard, in its 56 field offices, and internationally through its legal attaché offices, the FBI provides training to small businesses, state and local agencies, and international partners on best practices for securing networks, based on lessons learned through prior investigations and proactively disseminates both contextual and technical information.

- National Security Agency (NSA) Information Assurance (IA) Guidance -- https://www.nsa.gov/ia/mitigation_guidance

  NSA provides guidance on Information Assurance security solutions so that customers can benefit from NSA's unique and deep understanding of risks, vulnerabilities, mitigations, and threats.

- Small Business Administration Cybersecurity Landing Page -- https://www.sba.gov/cybersecurity

  SBA provides information to small business and small business network partners through SBA's landing page of government wide cybersecurity best practices. Additionally, the agency has required that a Business Development Specialist from each SBA District Office attend a webinar training, and then disseminate the information to their respective office and SBA Resource Partners through a combination of webinars, in-person trainings, and roundtables.

9 General Procedures Supporting the Sharing of Cyber Threat Indicators/Defensive Measures

9.1 Sharing in Real-time (Section 103(b)(1)(A))

The Federal Government shall develop and maintain the capability to share CTIs and DMs in real time consistent with the protection of classified information.

To accomplish this, the Federal Government uses DHS's Automated Indicator Sharing initiative (AIS) as the primary mechanism to share unclassified CTIs and DMs with federal entities and non-federal entities. AIS access procedures can be found at: https://www.us-cert.gov/ais.

9.2 Roles and Responsibilities -- Federal Entities/Non-Federal Entities/ISACs and ISAOs (Section 103(b)(1)(B))

The Federal Government's procedures incorporate existing processes and existing roles and responsibilities of federal entities and non-federal entities for information sharing by the Federal Government, including sector-specific information sharing and analysis centers. Executive Order 13691 – *Promoting Private Sector Cybersecurity Information Sharing*, recognizes the important roles and responsibilities of federal and non-federal entities engaged in the sharing of information related to cybersecurity risks and incidents. Specifically, it encourages the voluntary formation of organizations that support such sharing.

9.2.1 Federal Entities

A Federal entity is a department or agency of the United States or any component of such department or agency.

9.2.1.1 Role of Federal Entities

Federal entities collaborate with non-federal entities to provide situational awareness of cybersecurity threats, security vulnerabilities, and the potential or real consequences resulting from the defeat of a security control. Federal entities necessarily have a deep understanding of the nature, breadth and scope of the stakeholders within their sectors of operation, and as such can be an essential resource in disseminating CTIs, DMs, and best practices to those stakeholders. This function is particularly important for reaching the small and medium size businesses that may not have automated sharing capabilities but can make use of this information. Accordingly, federal entities, including those with regulatory and non-regulatory authorities, should identify and participate in opportunities to share with each other such that they can facilitate further sharing with the non-federal entities with which they regularly engage.

9.2.1.2 Responsibilities of Federal Entities

Federal entities should share CTIs and DMs amongst each other and with non-federal entities to the broadest extent practicable. Each federal entity should conduct its own review of CTIs and DMs prior to disclosure to assess whether it contains any information (1) not directly related to a cybersecurity threat or (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 (see Section 9.5). Federal entities should analyze CTIs, DMs, security vulnerabilities and cyber threat information in the context of their own operations and those of any non-federal entity sectors with which they have any specialized familiarity in order to enhance their own and a sector's situational awareness while identifying potential cybersecurity practice improvements. Such practices should be shared periodically as identified in Section 8.

9.2.2 Non-Federal Entities

A "non-Federal entity" is defined in Section 102(14) of CISA. Information sharing among non-federal entities and federal entities is enhanced through Information Sharing and Analysis Centers and other Information Sharing and Analysis Organizations.

9.2.2.1 Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs)

Presidential Decision Directive-63 (PDD-63) introduced the concept of ISACs. PDD-63 recognized the potential for the infrastructures of the United States to be attacked either through physical or cyber means with the intent to affect the military or economic power of the nation.

In PDD-63, the Federal Government asked each critical infrastructure sector to establish a sector-specific information sharing organization to share information within each sector about threats and vulnerabilities to that sector. In response, many sectors established Information Sharing and Analysis Centers (ISACs) to meet this need. ISACs generally are funded and organized by private sector membership, with no government role in their operations or processes.

An Information Sharing and Analysis Organization (ISAO) is a group created to gather, analyze, and disseminate critical infrastructure information. Unlike an ISAC, an ISAO need not be directly tied to a critical infrastructure sector, as outlined in Presidential Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst, for example, small businesses across sectors; or legal, accounting, and consulting firms that support cross-sector clients.

9.2.2.2 Role of ISACs and ISAOs

ISACs and ISAOs are trusted entities established by their membership to provide comprehensive all-hazards analysis, which is shared within the sector, within a profession, across a particular community of interest, with other sectors, and with the Federal Government. ISACs and ISAOs may provide their membership with risk mitigation, incident response, and alert and information sharing. The goal is to provide users with accurate, actionable, and relevant information.

9.2.2.3 Responsibilities of ISACs and ISAOs

An ISAC or ISAO generally performs the following functions:

- Provides 24/7 secure operating capability that establishes its constituency's specific information sharing/intelligence requirements for incidents, threats, and vulnerabilities;
- Collects, analyzes, and disseminates alerts and incident reports to its membership based on its sector- or other constituency-focused subject matter analytical expertise;
- Helps the Federal Government understand impacts on its constituency;
- Provides an electronic, trusted capability for its membership to exchange and share information on cyber, physical, and all-hazards threats in order to defend critical infrastructure or other assets, resources and functions; and
- Provides analytical support to the Federal Government and other ISACs and ISAOs regarding technical constituency details, and may provide mutual information sharing and assistance during actual or potential disruptions whether caused by intentional, accidental or natural events.

ISACs and ISAOs are encouraged to further disseminate CTIs, DMs, cyber threat information and best practices received from federal entities to their membership. They also are encouraged to share with federal entities, subject to any required anonymization, the CTIs, DMs, cyber threat information and best practices received from their membership.

9.3 Notification of Cyber Threat Indicators/Defensive Measures Error (Section 103(b)(1)(C))

This section relates to 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 this title that is known or determined to be in error or in contravention of the requirements of this title or another provision of federal law or policy of such error or contravention. Details for this notification can be found in the Privacy and Civil Liberties guidance developed pursuant to Section 105(b) of CISA.

9.4 Protection of Unauthorized Access to Cyber Threat Indicators/Defensive Measures (Section 103(b)(1)(D))

The head of each federal entity sharing CTIs or defensive measures is responsible for providing information security protections 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 or defensive measures, as described in the Federal Information Security Modernization Act (FISMA) of 2014 (Pub. L. 113-283, 44 USC 3554).

9.5 Personal Information Review and Removal (Section 103(b)(1)(E))

This section relates to procedures that require a federal entity, prior to the sharing of a cyber threat indicator—

> (i) to review such cyber threat indicator to assess whether such cyber threat indicator contains 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[5] and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat 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.

Details for this process can be found in the Privacy and Civil Liberties guidance developed pursuant to Section 105(b) of CISA.

9.6 Privacy/Civil Liberties Violation Notification (Section 103(b)(1)(F))

Notification procedures associated with a federal entity that becomes aware that it has shared in violation of CISA the personal information of any United States person can be found in the Privacy and Civil Liberties guidance developed pursuant to Section 105(b) of CISA.

[5] 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 agency, so long as the definition would, at a minimum, include personal information of a specific individual, or information that identifies specific individuals.

Appendix A: Acronyms

AIS	Automated Indicator Sharing
CFR	Code of Federal Regulations
CISA	Cybersecurity Information Sharing Act of 2015
CISCP	Cyber Information Sharing and Collaboration Program (DHS)
CRADA	Cooperative Research and Development Agreement
CRISP	Cybersecurity Risk Information Sharing Program (DOE)
CSP	Commercial Service Provider
CTFs	Cyber Task Forces
CTI	Cyber Threat Indicator
DC3	DOD Cyber Crime Center (DOD)
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DM	Defensive Measure
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
ECS	Enhanced Cybersecurity Services (DHS)
EO	Executive Order
FBI	Federal Bureau of Investigation
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team (DHS)
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
JTTFs	Joint Terrorism Task Forces
NCCIC	National Cybersecurity and Communications Integration Center (DHS)
NCIJTF	National Cyber Investigative Joint Task Force (FBI)
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
ORCON	Originator Controlled
PCII	Protected Critical Infrastructure Information
SBA	Small Business Administration
US-CERT	United States Computer Emergency Readiness Team (DHS)

The Department of Homeland Security
The Department of Justice

Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015

February 16, 2016

Table of Contents

Table of Contents 2

1. Scope of Guidance 3

a. Key Concepts 4

i. Cyber Threat Indicator 4

ii. Defensive Measure 6

iii. Information Protected under Otherwise Applicable Privacy Laws that are Unlikely to be Directly Related to a Cybersecurity Threat 7

2. How to Share Cyber Threat Indicators and Defensive Measures with the Federal Government 10

a. Requirements for Non-Federal Entities Sharing Cyber Threat Indicators and Defensive Measures with Federal Entities 10

b. Non-Federal Entities Sharing Cyber Threat Indicators and Defensive Measures through the Real-Time DHS Process and Capability 11

i. Automated Indicator Sharing (AIS) 12

ii. Web Form 12

iii. Email 12

iv. Information Sharing and Analysis Organizations and Centers 13

c. Non-Federal Entities Sharing with Federal Entities through other Means 13

3. Protections Received by Sharing Entities 13

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

1. Scope of Guidance

As required by Section 105(a)(4), this guidance addresses:

1. Identification of types of information that would qualify as a cyber threat indicator under the Act that would be unlikely to include information that is not directly related to a cybersecurity threat and is personal information of a specific individual or information that identifies a specific individual; and
2. Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.[4]

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

---

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

[2] Pursuant to CISA, "non-federal entity" means any private entity, non-Federal government agency or department, or state, tribal, or local government (including a political subdivision, department, or component thereof) and includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States, but does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801). Section 102(14)(A)-(C).

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

[4] This guidance is intended as assistance, not authority. It has no regulatory effect, confers no rights or remedies, and does not have the force of law. *See United States v. Caceres*, 440 U.S. 741 (1979). Further, the sharing of a cyber threat indicator or defensive measure with a non-federal entity under the Act shall not create a right or benefit to similar information by such non-federal entity or any other non-federal entity.

[5] Although section 105(a)(4) omits any reference to defensive measures, we have elected to include them in this guidance because the Act authorizes non-federal entities to share defensive measures. Section 104(c). Furthermore, providing guidance to non-federal entities on sharing defensive measures is important because improperly shared information is not eligible for the Act's protections.

In addition to covering how to identify and share cyber threat indicators and defensive measures, this guidance also explains how to share that information with federal entities through the Federal Government's capability and process that is operated by DHS (See section 2.B.) This guidance also explains how to share such information with DHS and other federal entities—including law enforcement—through other means authorized by the Act, and discusses the various legal protections the Act provides for such authorized sharing (See sections 2.C. and 3).

a. Key Concepts

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

i. Cyber Threat Indicator

The Act defines a cyber threat indicator to mean information that is necessary to describe or identify:

- Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; [6]
- A method of defeating a security control or exploitation of a security vulnerability;

[6] The definition of cyber threat indicator references a "cybersecurity threat" and "security vulnerability," which are terms defined by the Act. A cybersecurity threat is defined under section 102(5) to mean:

> An action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Many terms of service agreements prohibit activities that satisfy the definition of a "cybersecurity threat." However, activities that are "solely" violations of consumer agreements but do not otherwise meet the definition are not cybersecurity threats under CISA.

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

A security vulnerability is defined by section 102(17) to mean "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control." In contrast to a cybersecurity threat, it does not require adverse impact to an information system or information.

- A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- Malicious cyber command and control;
- The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- Any combination thereof.[7]

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

Information is not directly related to a cybersecurity threat if it is not necessary to assist others detect, prevent, or mitigate the cybersecurity threat. For example, a cyber threat indicator could be centered on a spear phishing email. For a phishing email, personal information about the sender of email ("From"/"Sender" address), a malicious URL in the e-mail, malware files attached to the e-mail, the content of the e-mail, and additional email information related to the malicious email or potential cybersecurity threat actor, such as Subject Line, Message ID, and X-Mailer, could be considered directly related to a cybersecurity threat. The name and e-mail address of the targets of the email (i.e., the "To" address), however, would be personal information not directly related to a cybersecurity threat and therefore should not typically be included as part of the cyber threat indicator.

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

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

[7] Section 102(6).

- A manufacturer could report unexecuted malware found on its network.
- A researcher could report on the domain names or IP addresses associated with botnet command and control servers.
- An engineering company that suffers a computer intrusion could describe the types of engineering files that appear to have been exfiltrated, as a way of warning other companies with similar assets.
- A newspaper suffering a distributed denial of service attack to its web site could report the IP addresses that are sending malicious traffic.

To help ensure consistency with CISA's definitions and requirements, standardized fields in structured formats can be used to establish a profile that limits the type of information in a cyber threat indicator. Much of the information within an indicator is centered on an observable fact about the cyber threat. For example, a cyber threat indicator has a variety of observable characteristics: a malicious email, internet protocol (IP) addresses, file hashes, domain names, uniform resource locators (URLs), malware files, and malware artifacts (attributes about a file). The specificity and nature of the observable facts are designed to reduce the risk that a cyber threat indicator contains personal content or information inappropriate to share. DHS's AIS initiative uses this means of controlling the type of information that may be shared using the automated system discussed in section 2.B.1.

ii. Defensive Measure

The Act defines a defensive measure to mean:

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

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

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

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

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

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

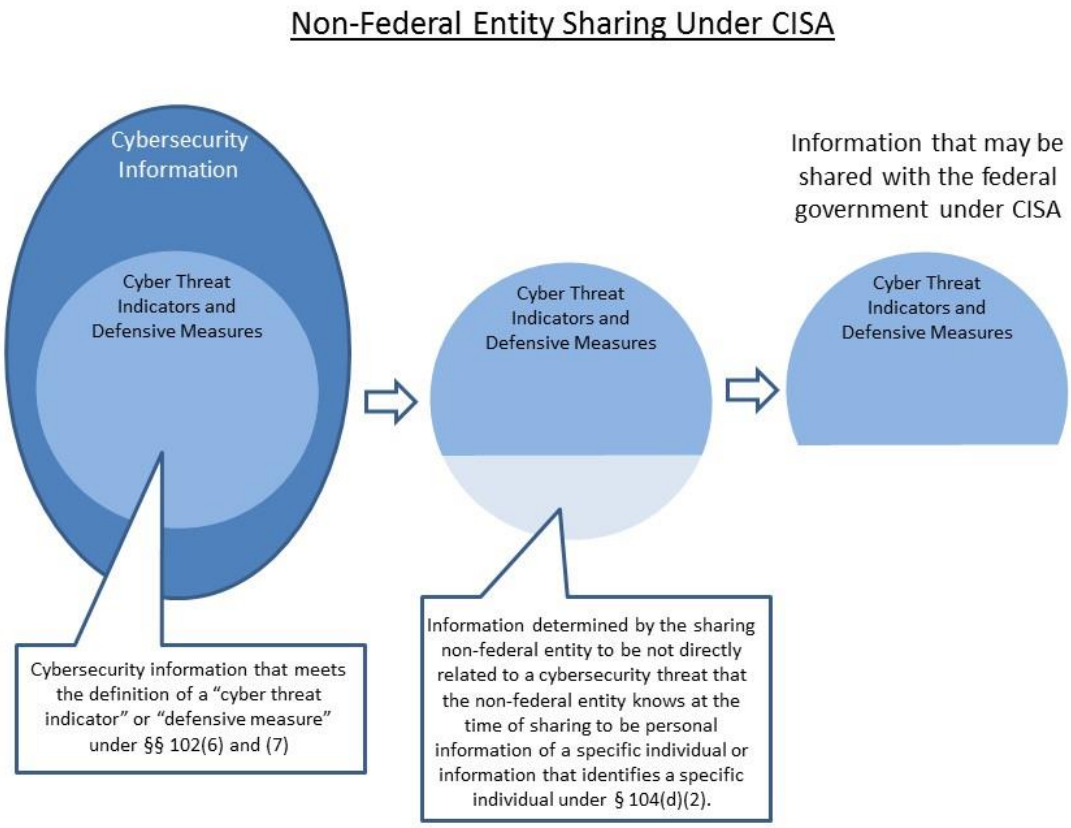
- A computer program that identifies a pattern of malicious activity in web traffic flowing into an organization.
- A signature that could be loaded into a company's intrusion detection system in order to detect a spear phishing campaign with particular characteristics.
- A firewall rule that disallows a type of malicious traffic from entering a network.
- An algorithm that can search through a cache of network traffic to discover anomalous patterns that may indicate malicious activity.
- A technique for quickly matching, in an automated manner, the content of an organization's incoming Simple Mail Transfer Protocol (SMTP, a protocol commonly used for email) traffic against a set of content known to be associated with a specific cybersecurity threat without unacceptably degrading the speed of email delivery to end users.

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

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

---

and authorization to use a defensive measure (sections 102(7) and 104(b), respectively) do not permit unauthorized access to or execution of computer code on another entity's information systems or other actions that would substantially harm another entity's information systems. Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015, p. 2, available at http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/JES%20for%20Cybersecurity%20Act%20of%202015.pdf. Cognizant of the fact that defensive measures deployed on one entity's network could have effects on other networks, Congress defined a defensive measure to only include measures on an entity's information systems that do not cause substantial harm to another entity's information systems or data.



To assist in this task, section 105(a)(4)(B)(ii) requires this guidance to help entities identify certain types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat. As explained above, cyber threat indicators and defensive measures will typically consist of technical information that describes attributes of a cybersecurity threat which typically need not include various categories of information that are considered sensitive and, therefore, protected by privacy laws. Information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat falling into this category of protected information may include:[9]

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

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

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

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

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

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

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

- Financial Information constitutes a vast category of information, which is highly sensitive and highly regulated. Financial information includes anything from bank statements, to loan information, to credit reports. Certain laws, such as the Gramm-Leach-Bliley Act require financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

- Identifying Information about Property Ownership. Although some information about property ownership may be publicly available, such as property purchase records, other information such as Vehicle Identification Numbers are inherently more sensitive and typically governed by state laws.

- Identifying Information of children under the age of 13. The Children's Online Privacy Protection Act (COPPA) imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

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

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

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

The Act only authorizes information sharing for a cybersecurity purpose.[10] It does not limit or modify any existing information sharing relationship, prohibit an existing or require a new information sharing relationship, or mandate the use of the capability and process within DHS developed under section 105(c). Section 108(f).

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

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

Under the Act, a non-federal entity must review cyber threat indicators prior to sharing them to assess whether they contain any information not directly related to a cybersecurity threat that the non-federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information. Section 104(d)(2)(A). While not explicitly required by the Act, non-federal entities are encouraged to conduct a similar review prior to sharing defensive measures under the Act. A defensive measure may contain a cyber threat indicator. Consequently, even though CISA may

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

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

If a non-federal entity does not "know at the time of sharing" that a cyber threat indicator contains personal information of a specific individual or information that identifies a specific individual, the non-federal entity is not required to alter the shared information. A non-federal entity may conduct its review for such information using either a manual or technical process; either is permissible under CISA. Section 104(d)(2)(A) and (B).[11]

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

Section 105(c) of the Act directs the Secretary of DHS to develop a capability and process within DHS that will accept cyber threat indicators and defensive measures in real time from any non-federal entity, including private entities. Non-federal entities may share such information with DHS through this capability, and DHS will in turn relay that information to federal entities in an automated manner,[12] as required by the Act and consistent with the operational and privacy and civil liberties policies instituted under sections 105(a) and (b).[13] Upon certification by the Secretary of Homeland Security in accordance with section 105(c), the DHS capability and process shall be the process by which the Federal Government receives cyber threat indicators and defensive measures under the Act that are shared by a non-federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems, with only specific exceptions.[14]

Provided that sharing is conducted in accordance with the Act, sharing conducted using this DHS capability will receive liability protection under section 106. It will also receive the other protections provided by the Act discussed more fully below in section III. The implementation of this capability does not, however, limit or prohibit otherwise lawful disclosures of communications, records, or other information, including the reporting of known or suspected criminal activity. Section 105(c)(1)(e). It also does not limit or prohibit voluntary or legally compelled participation a federal law enforcement investigation or affect the provision of cyber

---

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

[12] Section 105(a)(3)(A) requires DHS to disseminate cyber threat indicators and defensive measures shared with DHS pursuant to section 105(c) to the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence in an automated fashion. Section 105(a)(3)(A)(i).

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

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

> (i) consistent with section 104 of the Act, communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and
> (ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat.

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

Non-federal entities may share cyber threat indicators and defensive measures through the DHS capability and process created under section 105(c) via the AIS initiative, web form, email, or other information sharing programs that use these means of receiving cyber threat indicators or defensive measures. Instructions on utilizing each method can be found below.

i. Automated Indicator Sharing (AIS)

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

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

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

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

ii. Web Form

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

iii. Email

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

iv. Information Sharing and Analysis Organizations and Centers

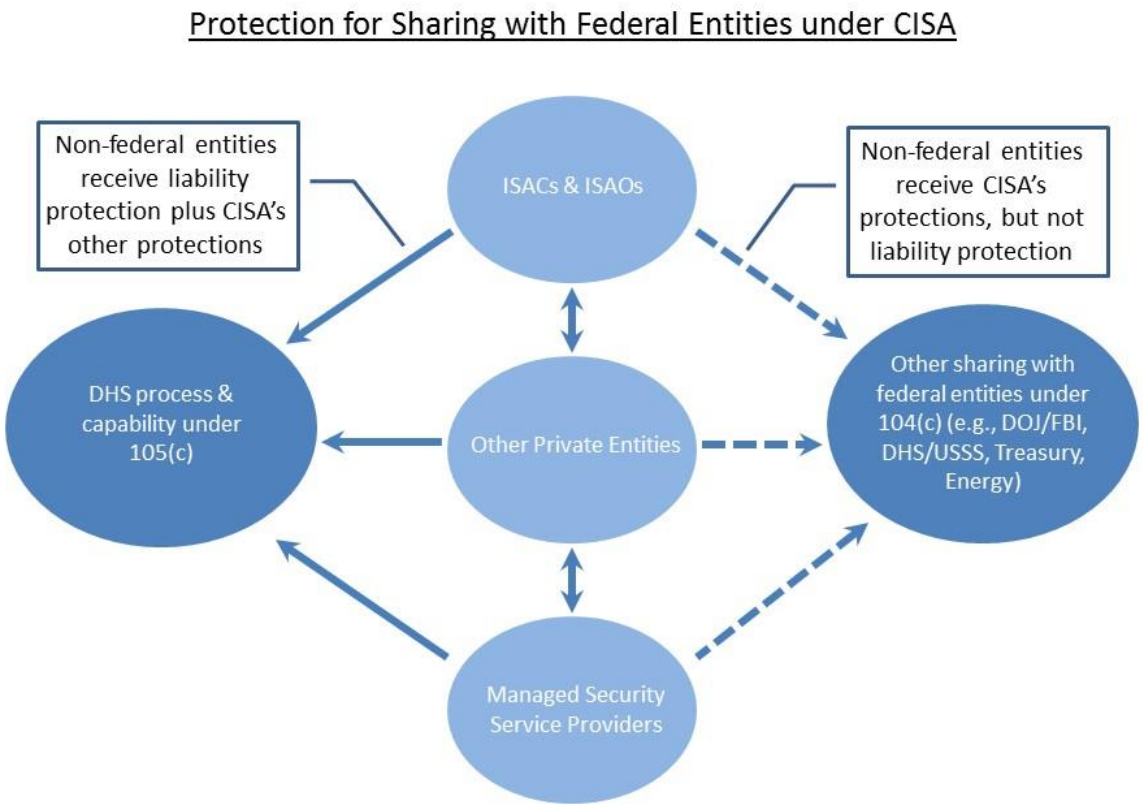
Non-federal entities may also share cyber threat indicators and defensive measures with federal entities through Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations, which will share them with federal entities through DHS on their behalf. Non-federal entities that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

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

Consistent with CISA, non-federal entities may also share cyber threat indicators and defensive measures with federal entities through means other than the Federal government's capability and process operated by DHS described in sections B.1 through 4 above. Section 104(c) authorizes a non-federal entity to share cyber threat indicators with a federal entity—or any non-federal entity—so long as sharing is conducted for a cybersecurity purpose. However, as noted below, the protection from liability of Section 106(b)(1) does not attach.

3. Protections Received by Sharing Entities

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



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

- Antitrust Exemption: The Act provides a statutory exemption to federal antitrust laws that supplements the policy statement issued by the Department of Justice's Antitrust Division and the Federal Trade Commission in May 2014 stating that sharing of cyber threat information would in the normal course be unlikely to violate federal antitrust laws.[15] Section 104(e). However, the Act also expressly prohibits conduct that would otherwise constitute an antitrust violation, notwithstanding the exception provided by section 104(e)(1) to prevent this exception from being used as the basis for committing antitrust violations under the guise of cybersecurity information sharing. Section 108(e).

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

[15] The DOJ/FTC policy statement revisited a business review letter prepared by the Antitrust Division in 2000 in which it examined a proposed cybersecurity information sharing program. The policy statement reaffirmed the conclusions of the 2000 business review letter. It stated, "While this guidance is now over a decade old, it remains the Agencies' current analysis that properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns." Policy Statement at 1, *available at* http://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf .

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

- Exemption from certain state and federal regulatory uses: Cyber threat indicators and defensive measures shared under the Act shall not be used by any state, tribal, or local government to regulate, including an enforcement action, the lawful activity of any non-federal entity or any activity taken by a non-federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator. However, a cyber threat indicator or defensive measure may, consistent with a federal, state, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems. CISA's legislative history states that congressional drafters viewed this as a narrow exception to ensure that government agencies with regulatory authority understand the current landscape of cyber threats and those facing the particular regulatory sector over which they have cognizance. Section 104(d)(4)(C); section 105(d)(5)(D).

- No waiver of privilege for shared material: Under the Act, sharing cyber threat indicators and defensive measures with the Federal government does not constitute the waiver of any applicable privilege or protection provided by law; in particular, shared information does not surrender trade secret protection. Section 105(d)(1).

- Treatment of commercial, financial, and proprietary information: When so designated by the sharing entity, shared information shall be treated as commercial, financial, and proprietary information. The legislative history indicates that Congress expected the Federal government to further share and use such information for cybersecurity purposes consistent with the privileges, protections, and any claims of propriety on such information. Section 105(d)(2).

- Ex parte communications waiver: Under the Act, the sharing of cyber threat indicators and defensive measures under the Act shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official. This provision addresses concerns about ex parte communications related to the Administrative Procedure Act (APA), 5 U.S.C. § 553. Section 105(d)(4).

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

The Department of Homeland Security
The Department of Justice

Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government

February 16, 2016

Table of Contents

1. Terms of Reference 3
2. Receipt, processing, and dissemination of cyber threat indicators submitted through real-time means [Sec. 105 (a)(3)(A)] 3
   2.1. Connecting to the TAXII server 4
   2.2. Receipt of indicators and defensive measures 4
   2.3. Filtering and analysis of indicators and defensive measures 6
      2.3.1. Automated actions that do not modify or delay transmission of cyber threat indicators or defensive measures. 6
      2.3.2. Actions that may modify or delay transmission of a portion of a cyber threat indicator or defensive measure. 7
   2.4. Dissemination of indicators and defensive measures 8
3. Receipt, processing, and dissemination of cyber threat indicators submitted through non-automated means [Sec. 105 (a)(3)(B)] 9
   3.1. General Guidance 9
      3.1.1. Timeliness 9
      3.1.2. Permitted Modifications and Delays 9
   3.2. DHS Procedures 9
      3.2.1. Web form submissions 9
      3.2.2. Email submissions 10
4. Audit capabilities and unsanctioned use [Sec. 105 (a)(3)(C)] 10
   4.1. Auditing capabilities 10
   4.2. Sanctions 11
Appendix A: Glossary 12

This document establishes procedures relating to the receipt of certain cyber threat indicators and defensive measures by all federal entities under the Cybersecurity Information Sharing Act of 2015 (CISA). It describes the processes for receiving, handling, and disseminating information that is shared pursuant to CISA, including through operation of the DHS Automated Indicator Sharing capability undersection 105(c) of CISA. It also states and interprets the statutory requirements for federal entities that receive cyber threat indicators and defensive measures under CISA to share them with other appropriate federal entities.

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 procedures shall affect the conduct of authorized law enforcement or intelligence activities or modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

1. Terms of Reference

Section 105(c) of CISA establishes within the Department of Homeland Security the Federal Government's capability and process for the receipt of cyber threat indicators and defensive measures from non-federal entities through an automated real-time exchange, electronic mail or media, or a website interface. The following operational procedures reference several key terms. These terms have been defined by the CISA and are set forth in Appendix A.

2. Receipt, processing, and dissemination of cyber threat indicators submitted through real-time means [Sec. 105 (a)(3)(A)]

This section describes the sharing of cyber threat indicators and defensive measures with the Federal Government through the DHS Automated Indicator Sharing (AIS) capability provided for by section 105(c) of CISA.[1] The DHS capability to receive, filter, analyze, and disseminate such information in real-time leverages Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) specifications, along with the procedures and standards developed by the national cybersecurity centers. Any entity participating in this AIS capability must be able to communicate using these machine-to-machine specifications, as further described below. Entities wishing to share cyber threat indicators through non-real-time means should see below for other options.

[1] Upon making a certification as provided in section 105(c)(2)(B) of the CISA, the President may designate one or more other federal entities to develop and implement a capability and process pursuant to 105(c)(2)(B)(III) of CISA. If that were to occur, the procedures in this section 2 and section 105(a)(3)(A) of CISA would apply to that capability and process as well.

2.1. Connecting to the TAXII server

In order to participate in the AIS capability, federal entities, as well as non-federal entities participating in the program must coordinate with DHS to ensure proper implementation, including access to the necessary technical infrastructure, establishment of network connectivity and exchange of authentication and other technical specifications, required for access to the sharing capability. For details on certifications and connectivity specifics, see the Frequently Asked Questions (FAQ) located at https://www.us-cert.gov/ais.

2.2. Receipt of indicators and defensive measures

To make a submission via the DHS automated capability, participating Federal and non-federal entities must follow submission guidance specifications made available by DHS. Federal entities should use a profile to standardize the indicator information and adhere to all relevant requirements contained in the Privacy and Civil Liberties Guidelines, which can be found at https://www.us-cert.gov/ais. Non-Federal entity submissions should conform to the AIS Profile, which can also be found at https://www.us-cert.gov/ais. The AIS Profile is intended to ensure that submissions include input fields most directly related to cyber threat indicators and defensive measures, as assessed by DHS in consultation with other federal entities. This assessment included a review of STIX fields for privacy, civil liberties, and other compliance concerns and risks. The STIX format includes several thousand fields, whereas the AIS Profile is a subset of those fields that are determined to directly relate to a cybersecurity threat and that otherwise protects privacy and civil liberties as required by CISA. Different indicator types may require the submission of a specific subsection of the fields in the AIS Profile.

Through continued collaboration and experience, the appropriate federal entities and other information sharing participants will identify STIX fields to be added and removed from the AIS Profile. DHS will chair the AIS Profile Change Control Board, the membership of which will comprise an authorized representative of the head of each appropriate Federal agency listed in section 102(3). Requests to modify the STIX schema used within the AIS Profile will be submitted in writing by any member of the AIS Profile Change Control Board. In addition, the AIS Profile Change Control Board will provide other federal entities and information sharing participants with opportunities to submit change requests. The following specific process will be followed by the AIS Profile Change Control Board:

- Each member can submit a written proposal to add or delete a field.

- DHS will forward such proposals to the AIS Profile Change Control Board.
- Upon receipt of a proposal, the AIS Profile Change Control Board members will have two weeks to consider the proposal.
- The proposal will be accepted only if no member objects.
    - If a member does not affirmatively object to a proposal within two weeks, then that member's concurrence will be presumed by the AIS Profile Change Control Board and the proposal will be accepted.
    - The AIS Profile Change Control Board will meet to discuss proposals for which an objection is provided or for which further discussion is requested.
    - The AIS Profile Change Control Board will attempt to resolve an objection or request for further discussion.
    - If the AIS Profile Change Control Board cannot resolve an objection, DHS will escalate the proposal up to and including, if necessary, each appropriate Federal agency's head for resolution with unanimous approval required.
- When considering a proposal, each member of the AIS Profile Change Control Board will ensure that fields are added or deleted:
    - in compliance with CISA's definitions of cyber threat indicators and defensive measures;
    - in compliance with CISA's provisions designed to limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals; and
    - commensurate with the overarching set of STIX fields available in the latest STIX schema available within the STIX community of users.

Note: Notwithstanding these procedures, DHS preserves its ability (1) to develop and implement emergency break fixes to the profile without having to seek approval from the AIS Profile Change Control Board and (2) to make modifications to the AIS Profile if a change to the information technology infrastructure calls for it.

Upon receipt of cyber threat indicators or defensive measures, federal entities should still follow all other applicable procedures, guidelines, and requirements, to the extent consistent with and in addition to the Privacy and Civil Liberties Guidelines produced under section 105(b) of CISA, to ensure appropriate handling of cyber threat indicators and defensive measures. In addition, federal entities should use the AIS Profile to standardize the indicator information and adhere to all relevant requirements contained in the Privacy and Civil Liberties Guidelines. As discussed in the Privacy and Civil Liberties Guidelines, using the

AIS Profile in this manner further minimizes privacy, civil liberties, and other compliance risks and discourages the submission of personal information of specific individuals or information that identifies specific individuals. In addition, the AIS Profile also reduces the risk of submission of content of communications that is not necessary to describe or identify a cybersecurity threat.

The full submission guidance document and AIS Profile can be found at https://www.us-cert.gov/ais. Non-federal entities are encouraged to review the full submission guidance and 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" for details on how to share with federal entities under CISA.

2.3. Filtering and analysis of indicators and defensive measures

Upon receipt by DHS, a series of automated actions occur. Where an automated process identifies an error or a particular field that cannot be processed by automated means, the system will flag the field for human review. When human review of a field is required, processing and dissemination of that field will necessarily be delayed, but the rest of the cyber threat indicator or defensive measure will be transmitted, with a second version following the human review. Automated processing is designed to maximize the speed, quantity, and value of information that can be shared with the Federal Government. The following subsections identify automated actions that do not incur modifications or delays and actions that may cause modifications and delays.

2.3.1. Automated actions that do not modify or delay transmission of cyber threat indicators or defensive measures.

This subsection identifies automated actions that do not modify or delay transmission of cyber threat indicators or defensive measures.

2.3.1.1. Automated validation against the AIS STIX schema. This confirms the submission is a valid STIX document and that it contains the minimum set of required AIS Profile STIX fields. If the submission is not a valid STIX document or does not contain the minimum AIS Profile fields, DHS will notify the submitter that the STIX document was invalid or rejected and delete the record.

2.3.1.2. If the submission contains fields that are not in the AIS Profile (i.e., AIS-prohibited fields, which are not part of a cyber threat indicator or defensive measure), then DHS will remove those fields from further automated processing and delete those fields. In addition, if the

submission contains values that do not match the AIS Profile controlled values, then DHS will remove those fields from further automated processing and delete those fields.

2.3.1.3. In cases where the submitter has not consented to transmission of its identity to other federal entities, automated preprocessing will remove information identifying the submitter of the information. Submitters are required to indicate whether they consent to transmission of their identity to other federal entities. If submitters consent to transmission of their identity to other federal entities, DHS will transmit their identity. If submitters do not initially consent to transmission of their identity to other federal entities, but another federal entity wishes to contact the submitter, DHS will transmit that request and ask whether the submitter consents to sharing its identity with that Federal entity. Regardless of whether the submitter consents to transmit its identity to other entities, submitters are required to identify the sector to which they belong as well as their approximate geolocation (e.g. city and state). These data fields, as provided by the submitter, will be transmitted to other federal entities in all instances.

2.3.2. Actions that may modify or delay transmission of a portion of a cyber threat indicator or defensive measure.

This subsection identifies the controls pursuant to which DHS will, in limited instances, make modifications that could delay the real-time sharing of one or more fields within a cyber threat indicator or defensive measure submitted by a non-Federal entity pursuant to section 104 of CISA. Consistent with section 105(a)(3)(A) of CISA, these controls will be carried out before any of the appropriate federal entities retains or uses the cyber threat indicators or defensive measures and will be uniformly applied such that each of the appropriate federal entities is subject to the same delay, modification, or other action. As required by section 105(a)(3)(A)(ii)(I) of CISA, the heads of the appropriate federal entities unanimously agree to these controls.[2]

2.3.2.1. Automated processing for mitigation of remaining personal information risks through schema restrictions, controlled vocabulary, regular expressions (i.e., pattern matching), known good values, and auto-generated text. Any fields that do not meet certain predetermined criteria defined through the AIS Profile and in the submission guidance will be

[2] DHS will continuously assess the controls described below, based on the volume and content of cyber threat indicators (CTIs) received, to achieve further automation and generally to avoid the unnecessary delay of the distribution of CTIs while protecting privacy.

referred for human review to ensure the field does not contain personal information of specific individuals or information that identifies specific individuals[3] not directly related to the cybersecurity threat. When a field within a cyber threat indicator or defensive measure is referred for human review, DHS will still transmit the fields that do not require human review to the appropriate federal entities without delay.

2.3.2.2. Human review of a small number of fields where the risk of personal information of specific individuals or information that identifies specific individuals that cannot be mitigated via automated means. If after human review: the field is determined to not contain personal information of specific individuals or information that identifies specific individuals; the field is determined to contain such information, but it is determined to be directly related to the cybersecurity threat; or the field is determined to contain personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat, however the personal information is able to be removed while still preserving other information within the field that is directly related to the cyber threat; then an updated cyber threat indicator or defensive measure will be issued using the versioning feature within STIX. If after human review, the field is determined only to contain personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat, the field will be deleted.

2.3.2.3. Indicator validation to remove nuisance indicators and enrichment of indicators using other information available to DHS.

Further details on the automated processing can be found in the System Description Document, located at https://www.us-cert.gov/ais.

2.4. Dissemination of indicators and defensive measures

Once automated processing has been performed on a submission made to DHS by a non-Federal entity, a sanitized cyber threat indicator or defensive measure will be made available to the appropriate federal entities. If human review of one or more fields is required, then the cyber threat indicator or defensive measure will be sent to the appropriate federal entities without those fields. Once human review is completed, updated indicators or defensive measures will be made available to the appropriate federal entities using the versioning feature within STIX.

[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 agency, so long as the definition would, at a minimum, include personal information of a specific individual, or information that identifies specific individuals.

3. Receipt, processing, and dissemination of cyber threat indicators submitted through non-automated means [Sec. 105 (a)(3)(B)]

This section outlines the overall process by which cyber threat indicators and defensive measures that are shared with the Federal Government by any non-Federal entity pursuant to section 104 of CISA through non-real-time mechanisms are shared with all of the appropriate federal entities.

3.1. General Guidance

3.1.1. Timeliness

Upon receipt of a cyber threat indicator or defensive measure from a non-Federal entity in a manner other than the real-time process described in section 105(c) of CISA, a recipient Federal entity shall share such cyber threat indicator or defensive measure with each appropriate Federal entity as quickly as operationally practicable, consistent with applicable law and the mission of those entities. This may be accomplished by sharing the cyber threat indicator or defensive measure through the DHS automated capability. In no event should a recipient Federal entity introduce an unnecessary delay, interference, or any other action that could impede receipt by all appropriate federal entities. However, certain modifications and delays are permitted as set forth below in section 3.1.2.

3.1.2. Permitted Modifications and Delays

A Federal entity may subject a cyber threat indicator or defensive measure, received from a non-Federal entity pursuant to section 104 of CISA in a manner other than the real-time process described in section 105(c) of CISA, to minimal delay, modification, or other action when such delay, modification, or other action is due to controls designed to remove personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat.

3.2. DHS Procedures

3.2.1. Web form submissions

DHS can receive web submissions of cyber threat indicator and defensive measure information from Federal and non-federal entities, although the automated exchange using STIX and TAXII specifications, and described in greater detail in Section 2, is strongly preferred since it encompasses a real time, machine-to-machine exchange that supports a higher volume of cyber threat indicators and defensive measures. The web submission includes validation that all required fields are present. Upon submission, the web form submission will be forwarded to DHS cyber threat analysts

to determine if there is valid cyber threat indicator or defensive measure information, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat), may be entered into the main DHS cyber threat repository. Once there, it will be delivered to the DHS TAXII server for dissemination to the appropriate federal entities. DHS will make available a publicly accessible web form for submission of cyber threat indicators and defensive measures to DHS.

3.2.2. Email submissions

DHS can receive email submissions of cyber threat indicators and defensive measure information from Federal and non-federal entities. The email ingestion includes validation that all required fields are present. Due to the additional review and separate processing workflow, email submissions are not the preferred method of submission and may result in processing delays due to the unstructured nature of email. Email submissions will be forwarded to DHS cyber threat analysts to determine if there is valid cyber threat indicator or defensive measure information, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat), may be entered into the main DHS cyber threat repository. Once there, it will be delivered to the DHS TAXII server for dissemination to the appropriate federal entities.

4. Audit capabilities and unsanctioned use [Sec. 105 (a)(3)(C)]

This section outlines the provisions and requirements for auditing and accountability to usage requirements.

4.1. Auditing capabilities

The appropriate federal entities shall maintain data, at the appropriate level of classification, regarding:

- The number of cyber threat indicators or defensive measures for which personal information of specific individuals or information that identifies specific individuals, that is not directly related to a cybersecurity threat, was removed;
- The number of notices issued with respect to a failure to remove personal information of specific individuals or information that identifies specific individuals, that is not directly related to a cybersecurity threat ;

- The extent to which cyber threat indicators or defensive measures were properly classified;
- The number of cyber threat indicators or defensive measures received through the DHS AIS capability and process established pursuant to section 105(c) of CISA; and
- A list of the federal entities with which cyber threat indicators or defensive measures have been shared pursuant to CISA.

The appropriate federal entities may choose to individually maintain additional data for auditing purposes based on those entities' individual requirements. Furthermore, the appropriate federal entities may evolve their audit data based on experience sharing under CISA.

4.2. Sanctions

Failure by an individual to abide by the usage requirements set forth in these guidelines will result in sanctions applied to that individual in accordance with their department or agency's relevant policy on Inappropriate Use of Government Computers and Systems. Penalties 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.

Appendix A: Glossary

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

ANTITRUST LAWS—The term ‘‘antitrust laws’’—(A) has the meaning given the term in the first section of the Clayton Act (15 U.S.C. 12); (B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and (C) includes any State antitrust law, but only to the extent that such law is consistent with the law referred to in subparagraph (A) of this definition or the law referred to in subparagraph (B) of this definition.

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) of this definition, 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) of this definition, 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 definition, 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.

STRUCTURED THREAT INFORMATION EXPRESSION (STIX)—“STIX” is a language for describing cyber threat information in a standard manner for the reading convenience of machines, not humans. STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness. In addition, STIX provides a unifying architecture tying together a diverse set of cyber threat information including:

- Cyber observables
- Indicators
- Incidents
- Adversary tactics, techniques, and procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, etc.)
- Exploit targets (e.g., vulnerabilities, weaknesses or configurations)
- Courses of action (e.g., incident response or vulnerability/weakness remedies or mitigations)
- Cyber attack campaigns
- Cyber threat actors

TRUSTED AUTOMATED EXCHANGE OF INDICATOR INFORMATION (TAXII)—“TAXII” is a standard for exchanging structured cyber threat information in a trusted manner. TAXII defines services, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information-sharing initiative or application and does not attempt to define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose all while using a single,

common set of tools. For more information on STIX and TAXII, see https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

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).

The Department of Homeland Security
The Department of Justice

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

February 16, 2016

Table of Contents

1 Purpose 3
2 Applicability 3
3 Background 3
4 Guiding Principles 4
5 Federal Entity Activity 6
5.1 Defensive Measures 6
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 10
5.7 Retention 11
5.8 Dissemination 11
6 Sanctions 12
7 Protection of classified/national security information 13
8 Audit 13
9 Periodic Review 14
Appendix A: Glossary 15

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 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 the authority of a department or agency of the Federal Government to protect 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 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 and with such entities' privacy and civil liberties officers, 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[1]. This document fulfills that requirement.

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

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

[1] In accordance with Section 105(b)(2), the Attorney General and the Secretary of Homeland Security will jointly develop, submit to Congress, and make available to the public final guidelines not later than 180 days after the date of the enactment of CISA.

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 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[2] 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 Fair Information Practice Principles (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.

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), procedures will be developed for notifying, in a timely manner, any United States person[3] 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

[2] 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 agency, so long as the definition would, at a minimum, include personal information of a specific individual, or information that identifies specific individuals.

[3] 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
	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 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 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 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.

Principle	Privacy and Civil Liberties Guidelines Implementation
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 the heads of 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 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) 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 that apply to defensive measures as well as cyber threat indicators.[4] 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

[4] *E.g.*, Section 103(b)(1)(C) (requiring specific notification requirements for cyber threat indicator or defensive measure known or determined to be received in error or in contravention of the requirements of CISA or another provision of federal law or policy); 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); 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).

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.[5]

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

1. Information that must be destroyed

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.

2. Review to ensure information is destroyed

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.[6] 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] 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.
[6] For more information on AIS, please see the Automated Indicator Sharing Privacy Impact Assessment, found at www.dhs.gov/privacy. The original AIS PIA was initially published in October 2015 and will be updated as appropriate.

5.3 Notification Procedures

Section 103(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 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) 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), including any information that does not constitute a cyber threat indicator in accordance with Section 105(b)(3)(E); 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 may 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 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. 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) 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 Section 103(b)(1)(C) and Section 105(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, the federal entity should notify the person in accordance with the federal entity's own breach/incident response plan.[7] 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.

[7] The Office of Management and Budget Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007), requires the head of each Federal agency 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 Section 103(b)(1)(F). 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.

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), 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;
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 may include:

- Internal User access controls
- Physical and/or logical segregation of data
- Required training
- Other 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 as described in

the Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554)

5.7 Retention

Federal agencies may only retain cyber threat indicators and defensive measure provided to the Federal Government under CISA for the purposes authorized in Section 105(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 105(b)(3)(B)(ii) for specific limitations on retention. In accordance with 105(b)(3)(B)(i), federal entities will also establish a process for the timely destruction of a 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.

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

2. Whether the federal entity knows at the time of sharing that the information to be 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 would 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 apply two markings for access and dissemination: TLP and AIS Consent marking. TLP was designed for ease of use and permits some degree of human judgment in the application of the rule sets. The AIS Consent marking allows non-federal entities to consent (or not) to sharing their identity with the appropriate federal entities or with the entire AIS community.

The technical procedures and requirements for these markings are defined in the ESSA/ISA Access Control Specification v2.1[8].

6 Sanctions

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

[8] For more information on the ESSA/ISA ACS v2.1, federal users may visit: https://community.max.gov/download/attachments/700842337/ISA%20Access%20Control%20Specification%202.1.draft2.clean.pdf?version=1&modificationDate=1447692497836&api=v2

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) 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 Reforms 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, 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) and the Government Accountability Office's independent report on removal of personal information107(c).

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).