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

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)