ISAO
Standards Organization

ISAO 600-2: U.S. Government Relations, Programs, and Services

v1.0

September 30, 2016

ISAO 600-2

U.S. Government Relations, Programs, and Services

v1.0
ISAO Standards Organization
September 30, 2016

Acknowledgements

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from industry, government, and academia in an ongoing effort to produce a unified voluntary set of guidelines and guidance for information sharing. The ISAO SO and the Working Group leadership are listed below.

ISAO Standards Organization
Dr. Gregory B. White
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Richard Lipsey
ISAO SO—Deputy Director
Senior Strategic Cyber Lead, LMI

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

Working Group Six—Government Relations

Doug DePeppe
Acting Chair, Working Group Six
*Founder, **eos**EDGE Legal*

David Weinstein
Vice Chair, Working Group Six
CTO, State of New Jersey

The ISAO SO leadership would also like to acknowledge those individuals who contributed significantly in the development of this document:

Mark Boggis
Cybersecurity Policy Solutions

Ricky Chitwood
Federal Aviation Administration

Mike Echols
Former Chair, Working Group Six

Stuart Gerson
Epstein Becker & Green PC

Elizabeth McGrath
The MITRE Corporation

James Murphy
SRA International

Azzar Nadvi
Department of Homeland Security

Nancy Pomerleau
Department of Homeland Security

Revision Updates

Item	Version	Description	Date
1	1.0	Initial Publication	September 30, 2016

Table of Contents

1 Executive Summary 1
2 Describing the Role of Government with Respect to ISAOs 1
2.1 General Principles 1
2.2 Government Functions 2
2.3 U.S. Government Policies 2
2.3.1 Executive Order 13636, Improving Critical Infrastructure Cybersecurity 2
2.3.2 Presidental Policy Directive 21, Critical Infrastructure Security and Resilience 3
2.3.3 Presidential Policy Directive 41, United States Cyber Incident Coordination 3
2.3.4 Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing 4
3 Overview of Relevant Federal Laws and Regulations 4
3.1 Homeland Security Act of 2002 4
3.2 Cybersecurity Information Sharing Act of 2015 5
3.2.1 “Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015” 5
3.2.2 “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” 6
3.2.3 “Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government” 7
3.2.4 “Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015” 7
3.3 Critical Infrastructure Information Act of 2002 8
3.3.1 Protected Critical Infrastructure Information Programs 8
3.4 The Privacy Act 9
3.5 The Bank Secrecy Act and the USA Patriot Act 9
3.6 Postmarket Management of Cybersecurity in Medical Devices 10
4 Issues to Address from the State and Local Government Perspective 10
4.1 Trust Relationship 10
4.2 Recommendations 11
4.3 Existing Capabilities and Programs 12

4.3.1 Protected Critical Infrastructure Information Program 12
4.3.2 Fusion Centers 13
4.3.3 Memoranda of Understanding or Agreement 13

5 Resources Available for ISAOs 13
5.1 Department of Homeland Security 13
5.1.1 Cybersecurity Framework Function Areas 13
5.1.2 Critical Infrastructure Cyber Community Voluntary Program 14
5.1.3 National Cybersecurity and Communications Integration Center 15
5.1.4 Additional DHS Resources 19
5.1.5 National Infrastructure Protection Plan 23
5.2 Department of Justice 25
5.2.1 Best Practices for Victim Response and Reporting of Cyber Incidents 25
5.3 Federal Bureau of Investigation 25
5.3.1 Domestic Security Alliance Council 25
5.3.2 Fusion Centers 25
5.3.3 Infragard 26
5.3.4 Internet Crime Complaint Center 26
5.3.5 Affiliated Information Sharing Association 27
5.4 Federal Communications Commission 27
5.4.1 Communications Security, Reliability, and Interoperability Council 27
5.4.2 Cybersecurity Planning Guide 27
5.4.3 Cybersecurity Tip Sheet 28
5.4.4 Small Business Cyber Planner 2.0 28
5.5 Federal Financial Institutions Examination Council 28
5.5.1 Cybersecurity Assessment tool 28
5.6 Federal Trade Commission 28
5.6.1 CAN-SPAM Act: A Compliance Guide for Business 28
5.6.2 Careful Connections: Building Security in the Interneet of Things 29
5.6.3 Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business 29
5.6.4 Complying with the FTC's Health Breach Notification Rule 29
5.6.5 Disposing of Consumer Report Inforamtion? Rule Tells How 29
5.6.6 Fighting Identity Theft with the Red Flags Rule: A Guide for Business 29
5.6.7 Information Compromise and Risk of identity Theft: Guidance for Your Business 30

5.6.8 Mobile Health App Developers: FTC Best Practices 30
5.6.9 Mobile Health Apps Interactive Tool 30
5.6.10 Peer-to-Peer File Sharing: A Guide for Business 30
5.6.11 Protecting Personal Information: A Guide for Business 30
5.6.12 Start with Security: A Guide for Business 30
5.7 National Institute of Standards and Technology 31
5.7.1 Framework for Improving Critical Infrastructure Cybersecurity 31
5.7.2 NIST Interagency Report 7621—Small Business Information Security: The Fundamentals 31
5.7.3 NIST Special Publication 800-36: Guide to Selecting Information Technology Security Products 32
5.7.4 NIST Special Publication 800-150: Draft Guide to Cyber Threat Information Sharing 32
5.8 National Security Agency 32
5.8.1 National Security Cyber Assistance Program 32
5.9 Small Business Administration 33

1 EXECUTIVE SUMMARY

The objective of this guide is to identify preliminary matters of policy and principles, state and local government perspectives, and relevant federal laws regarding cybersecurity information sharing within the United States. Developing trust within and across an information sharing ecosystem that involves both the public and private sectors is a major consideration for all collaborating entities, particularly in the areas of information sharing and privacy, the role of government, and national security. This document also addresses considerations for Information Sharing and Analysis Organization (ISAO) interaction with the intelligence community, law enforcement agencies, U.S. regulatory agencies, the Department of Homeland Security (DHS), and other government departments and agencies. The primary sections of this voluntary ISAO Standards Organization (SO) guide are organized as follows:

- Section 2 addresses the role of government with respect to ISAOs.
- Section 3 provides an overview of relevant federal laws and regulations.
- Section 4 addresses issues and considerations from the perspectives of state and local governments.
- Section 5 identifies government resources available to assist ISAOs and their members.

This document will be updated through ongoing open dialogue between the public and private sectors facilitated by the ISAO SO.

2 DESCRIBING THE ROLE OF GOVERNMENT WITH RESPECT TO ISAOS

2.1 GENERAL PRINCIPLES

The cyber ecosystem consists of a complex environment of private and public entities that share varying degrees of interdependency. Effective information sharing requires appropriate public-private partnership to ensure that mutually beneficial information is available to government agencies and private-sector organizations that choose to share, while protecting the privacy and civil liberties of affected citizens and corporate entities. Voluntary standards and guidelines for ISAOs should reflect appropriate considerations for laws and regulations while also taking into account the perspectives of industry, academia, and all levels of government.

For their part, governments at all levels share a responsibility to enable, support, and appropriately partner with ISAOs to improve the security and resilience of the nation. Additionally, an effective public-private partnership implies that ISAOs must have a voice in the formulation of relevant government policies that impact

information sharing and analysis activities, as well as regular opportunities to provide feedback on the effectiveness of government actions.

2.2 GOVERNMENT FUNCTIONS

The following is a list of generally accepted functions of federal, state, local, and tribal governments, provided to identify areas where ISAOs and government agencies may interact based on shared interests:

- National security and defense
- International relations and diplomacy
- Public safety and preparedness
- Administration of justice
- Governance and legislation
- Economic stability
- Critical infrastructure management and protection
- Social services
- Education
- Law enforcement
- Protection of individual privacy and civil liberties
- Consumer protection.

2.3 U.S. GOVERNMENT POLICIES

2.3.1 EXECUTIVE ORDER 13636, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

According to Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, “It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.” Additionally, 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.”

To implement sharing cyber threat indicators (CTIs), defensive measures (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 tear-lines to ensure the dis-

semination of cyber threat information to the maximum extent possible. 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.

Pursuant to EO 13636, 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 the Cybersecurity Information Sharing Act of 2015, 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, participating federal entities will ensure coordination and deconfliction associated with outreach to targeted entities or victims.

The Federal Government developed and maintains the capability to share CTIs and DMs in near real time consistent with the protection of classified information. To accomplish this, the government uses DHS's Automated Indicator Sharing (AIS) initiative as the primary mechanism to share unclassified CTIs and DMs with federal entities and non-federal entities.[1]

2.3.2 PRESIDENTAL POLICY DIRECTIVE 21, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Presidential Policy Directive 21 states that "critical infrastructure security and resilience … is a shared responsibility among Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure." [2]

2.3.3 PRESIDENTIAL POLICY DIRECTIVE 41, UNITED STATES CYBER INCIDENT COORDINATION

Presidential Policy Directive 41 states that "individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the nation from malicious cyber incidents and their consequences."[3]

[1] AIS access procedures can be found at https://www.us-cert.gov/ais.

[2] See https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[3] See https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

2.3.4 EXECUTIVE ORDER 13691, PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

By Executive Order 13691, the President stated that it is the policy of the United States that "to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." The U.S. government is able to provide a variety of means to effect more efficient sharing of cyber threat information as well as best practices and tips. Additionally, ISAOs may use many government programs in the performance of their operations.[4]

3 OVERVIEW OF RELEVANT FEDERAL LAWS AND REGULATIONS

ISAOs may need to consider a number of existing federal laws and regulations when establishing policies and procedures for sharing information. Information sharing is specifically addressed in the laws and regulations listed below.

3.1 HOMELAND SECURITY ACT OF 2002

The Homeland Security Act of 2002 (6 U.S.C. §131[5]) defines an ISAO as "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of

- gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;
- communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and
- voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B)."

The primary characteristic of an ISAO in the cybersecurity ecosystem is that the ISAO shares information related to cybersecurity risks and incidents between and among its membership. This holds true across a wide range of ISAOs with varying constituent membership organizations. While not all members of all ISAOs may be critical infrastructure entities, and some ISAOs will be organized

[4] See https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform.

around models other than sectors of critical infrastructure, ISAOs that share information related to cybersecurity risks and incidents meet the intent of EO 13691.

The Act, as amended by the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015, further authorizes the Department of Homeland Security to include appropriate representatives of non-federal entities, such as ISAOs, as part of the National Cybersecurity and Communications Integration Center. It also authorizes DHS to work with ISAOs and others in developing, updating, maintaining, and exercising adaptable cyber incident response plans. Finally, among other things, it provides DHS with the authority and responsibility to provide members of the public and private sectors with cyber threat, vulnerability, and other risk information, proposed mitigations, and situational awareness.

3.2 CYBERSECURITY INFORMATION SHARING ACT OF 2015

On December 18, 2015, President Obama signed into law the Cybersecurity Information Sharing Act of 2015 (CISA), which is designed to increase cybersecurity information sharing between and among private-sector entities and between the private sector and the federal government. CISA provides various protections to non-federal entities that share cyber threat indicators or defensive measures with each other or the federal government.

The DHS Automated Indicator Sharing (AIS) initiative is the principal mechanism for such sharing with DHS. Sharing information with DHS through AIS or other DHS mechanisms in accordance with CISA provides the submitter with certain liability protections.[5] As mandated by CISA, DHS certified the operability of AIS in March 2016 and released guidance to help non-federal entities share cyber threat indicators with the federal government. DHS and the Department of Justice (DOJ) also released policies and procedures relating to the receipt and use of cyber threat indicators by federal entities, guidelines relating to privacy and civil liberties in connection with the exchange of those indicators, and guidance to federal agencies on sharing information in the government's possession. Such guidance, procedures, and guidelines are described in the following four subsections.

3.2.1 "SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015"

The procedures outlined in the Office of the Director of National Intelligence/ Department of Defense/DOJ document[6] describe the current mechanisms through which the appropriate federal entities, as named in Section 102(3) of CISA, share

[5] For additional CISA information, see https://search.us-cert.gov/search?utf8=%E2%9C%93&affiliate=us-cert&query=CISA&commit=Search.

[6] See https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf.

information with non-federal entities. 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 through a series of programs and provide the foundation for appropriate federal entities' cybersecurity information sharing capability. These programs are dynamic and are expected to grow or evolve over time. That said, some programs may be discontinued and new programs may begin as updates are made to this document.

Additionally, 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.

3.2.2 "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"

This DHS/DOJ document[7] provides information sharing guidance for non-federal entities. This guidance addresses the following:

- Identification of the 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
- Identification of the types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat. That document also explains how to identify and share defensive measures. Under CISA section 106(b)(1), private entities that share a cyber threat indicator or defensive measure with an Information Sharing and Analysis Center (ISAC) or ISAO in accordance with the Act receive liability protection and other protections and exemptions for such sharing. Similarly, ISACs and ISAOs that share information in accordance with the Act also receive liability protection under section 106(b)(1), as well as other protections and exemptions. Likewise, an ISAC or ISAO that shares cyber threat indicators or defensive measures with the federal government in accordance with section 104(c) through the DHS capability and process created under section 105(c), or as otherwise consistent with section 105(c)(1)(B), is also eligible for liability protection under section 106(b)(2), in addition to CISA's other protections and exemptions.

[7] See https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

The document also notes that CISA 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.[8]

3.2.3 "FINAL PROCEDURES RELATED TO THE RECEIPT OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT"

Consistent with section 105(a)(2) and (3) of CISA, this DHS/DOJ document[9] establishes procedures relating to the receipt of cyber threat indicators and defensive measures by all federal entities. It describes the processes for receiving, handling, and disseminating information that is shared with DHS pursuant to section 104(c) of CISA, including through operation of the DHS Automated Indicator Sharing capability under section 105(c) of CISA. It also states and interprets the statutory requirements for all 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 must 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 those procedures should 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, sources, and methods and the national security of the United States.

3.2.4 "PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES: CYBERSECURITY INFORMATION SHARING ACT OF 2015"

This DHS/DOJ document[10] 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 CISA, consistent with the need to protect information systems from cybersecurity threats

[8] The 2014 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." The policy statement is available at http://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf.

[9] See https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf.

[10] See https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_.See) and 6 U.S.C. § 133(a)(1).e attached to headings.Civil_Liberties_Guidelines_%28Sec%20105%28b%29%29.pdf.

and mitigate cybersecurity threats, any other applicable provisions of law, and the Fair Information Practice Principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

Federal entities engaging in activities authorized by CISA must 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 those guidelines should 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, sources, and methods and the national security of the United States.

3.3 CRITICAL INFRASTRUCTURE INFORMATION ACT OF 2002

The Critical Infrastructure Information (CII) Act of 2002 was established to facilitate DHS's ability to collaborate effectively to protect America's critical infrastructure. It authorizes DHS to accept information relating to critical infrastructure from the public, owners and operators of critical infrastructure, and state, local, and tribal governmental entities, while limiting public disclosure of that sensitive information under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and other laws, rules, and processes. To implement the CII Act, DHS established the Protected Critical Infrastructure Information (PCII) Program, 6 Code of Federal Regulations (CFR) Part 29.

3.3.1 PROTECTED CRITICAL INFRASTRUCTURE INFORMATION PROGRAMS

The Department of Homeland Security created the PCII Program in accordance with the Critical Infrastructure Information Act of 2002. The PCII Program protects from public disclosure critical infrastructure information voluntarily shared with government entities for homeland security purposes. This better enables DHS to work directly with infrastructure owners and operators to identify vulnerabilities, mitigation strategies, and protective measures. Once information is voluntarily submitted to DHS and the PCII Program has validated it as PCII consistent with the requirements of the CII Act, it is protected from the following:

- Disclosure under FOIA consistent with 5 U.S.C. § 522(b)(3) and 6 U.S.C. § 133(a)(1)
- State, tribal, and local disclosure laws
- Use in regulatory actions
- Use in civil litigation.

PCII protections mean that homeland security partners, including ISAOs, can more freely share sensitive and proprietary CII with government partners with the

confidence that it will be protected from public release. Federal, State, and local government entities can use the information to protect the Nation's critical infrastructure. PCII is accessed only by authorized users who have a need-to-know specified PCII. In fact, the PCII final rule specifically discusses the protections afforded to information provided to DHS by ISAOs.[11]

3.4 THE PRIVACY ACT

The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A "system of records" is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of 12 statutory exceptions. The Privacy Act also provides individuals with a way to seek access to and amend their records, and it sets forth various agency record-keeping requirements.[12]

3.5 THE BANK SECRECY ACT AND THE USA PATRIOT ACT

Safe-harbor provisions (Bank Secrecy Act Interagency Examination Manual, p. 61) and federal law (31 U.S.C. 5318§[g][3]) provide protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the Suspicious Activity Report (SAR) instructions. Specifically, the law provides that a bank and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.

[11] See https://www.dhs.gov/submit-cii-pcii-protection.

[12] See https://www.justice.gov/opcl/privacy-act-1974.

3.6 POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES

Recognizing the growing importance of cybersecurity for medical devices and the potential public health risks that could result from inadequate post-market cybersecurity management, the U.S. Food and Drug Administration (FDA) on January 22, 2016, issued "Postmarket Management of Cybersecurity in Medical Devices (Draft Guidance)."[13] The guidance states that FDA views voluntary participation in an ISAO to be a "critical component of a medical device manufacturer's proactive post-market cybersecurity plan," and it strongly recommends that device manufacturers participate in a cybersecurity ISAO (Draft Guidance, pp. 7, 12).

The guidance also includes recommendations with regard to reporting actions taken by device manufacturers to address identified cybersecurity vulnerabilities. Generally, actions to address controlled risks will not require reporting under FDA's regulations, and FDA does not intend to enforce reporting requirements under 21 CFR Part 806 if several conditions are met, one of them being that the manufacturer is a participating member of an ISAO.

4 ISSUES TO ADDRESS FROM THE STATE AND LOCAL GOVERNMENT PERSPECTIVE

4.1 TRUST RELATIONSHIP

Effective information sharing requires a trust relationship among those who share and receive information. Specific concerns related to government entities include the following:

- Governmental entities should feel safe to share and receive sensitive cyber threat and vulnerability information without fear of public disclosure via state sunshine or freedom of information laws.
- Governmental entities must balance citizen privacy and civil liberties concerns with effective information sharing policies and practices.
- Private entities may not want to share sensitive threat and vulnerability information with governmental entities if there is a fear of regulatory enforcement actions based on the information received.
- It should be assumed that the relevance of cyber threat and vulnerability information may extend outside of a formal information sharing environment—that is, entities external to the ISAO might benefit from certain information being shared. ISAOs should consider whether and how they will respond to requests for sensitive cyber threat and vulnerability information from external entities.

[13] See http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/ GuidanceDocuments/UCM482022.pdf.

- Governmental entities should be assured that the receipt of cyber threat and vulnerability information does not create affirmative duties for which they could be held liable.
- Care and consideration should be given to the quality, timeliness, and relevance of information that states and localities share with ISAOs.

4.2 RECOMMENDATIONS

State disclosure laws have historically created a substantial barrier to effective sharing of cyber threat and vulnerability information. Fortunately, the Cybersecurity Information Sharing Act of 2015 addressed this issue:

Section 104(d)(4), Use of Cyber Threat Indicators by State, Tribal, or Local Government—

(A) **Law Enforcement Use.** A State, tribal, or local government that receives a cyber threat indicator or defensive measure under this title may use such cyber threat indicator or defensive measure for the purposes described in Section 105(d)(5)(A).

(B) **Exemption from Disclosure.** A cyber threat indicator or defensive measure shared by or with a State, tribal, or local government, including a component of a State, tribal, or local government that is a private entity, under this section shall be—

> deemed voluntarily shared information, and exempt from disclosure under any provision of State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

Furthermore, Section 106(b)(1) of CISA affords a private-sector entity liability protection for sharing with an SLTT government entity in accordance with the Act:

- No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under Section 104(c).

Several states have also addressed this issue via state legislation, explicitly creating such exemptions for critical infrastructure and cybersecurity information. It is recommended that states consider whether they should undertake the development of such exemptions to enable more effective collaboration and ultimately build trust between states and private-sector entities.

Some key themes, principals, and language found in successful state legislation effectively address these exemptions:

- A definition for critical infrastructure information and exclusion from disclosure under state freedom of information or sunshine laws. Critical infrastructure information may be defined using the following:
  - The federal definition of critical infrastructure information found within 6 U.S.C. § 131
  - Language defining public utility systems such as oil, electric, gas, sewer, water, or wastewater sectors
  - More specific language pertaining to a specific sector such as critical energy infrastructure.
- A definition of security information, which may include physical or cyber- related data. Examples of types of security information include the following:
  - Cybersecurity plans, assessments, and operational manuals
  - Technical or diagnostic records that, if disclosed, could reveal the location or operational details of sensitive systems
  - Information not lawfully available to the public regarding specific cybersecurity threats or vulnerabilities
  - Information that identifies, or provides means of identifying, a person who could, as a result of the disclosure, become a victim of a cybersecurity incident, or that would disclose a person's cybersecurity plans or practices, procedures, methods, results, or organizational structure, hardware, or software.

4.3 EXISTING CAPABILITIES AND PROGRAMS

States may also look to existing capabilities and programs that support broader information sharing among local, state, federal, and private-sector stakeholders. Some of these capabilities are identified in the following subsections.

4.3.1 PROTECTED CRITICAL INFRASTRUCTURE INFORMATION PROGRAM

Formed as a result of the passage of the Critical Infrastructure Act in 2002, the PCII Program affords protections to information provided by the private sector to the federal government. These protections include exemption from the federal FOIA, state and local disclosure laws, regulatory action, and civil litigation. Although DHS manages the PCII program at the federal level, states are encouraged to maintain their own programs in order to provide access to PCII protected information for state and local authorities with a need to know. States can implement PCII programs to more effectively share information with the private sector and build trust by protecting the information from regulators and the public.

4.3.2 FUSION CENTERS

Fusion centers were formed as a result of the terrorist attacks on September 11, 2001, and serve as a means of collecting, analyzing, and disseminating information that pertains to terrorism and organized crime activities. They exist in most states and are already integrated into local, state, and regional homeland security initiatives. Though fusion centers have varying levels of maturity with respect to cyber analytical capability, they have already established themselves within the critical infrastructure community as a means of sharing information on physical threats and are poised as an effective mechanism to share cyber threat information across sectors and disciplines. As states look to interface with and/or develop ISAOs, fusion centers may serve as a key capability in this effort.

4.3.3 MEMORANDA OF UNDERSTANDING OR AGREEMENT

States and localities should also consider the use of Memoranda of Understanding or Agreement (MOUs or MOAs) as a formal means of forging partnerships with public and private stakeholders and to foster information sharing. Although the PCII Program assists in protecting information that the private sector shares with government, it also precludes other private-sector entities from accessing that information. States and localities that seek to form or support ISAOs might wish to use an MOU or MOA to allow for a broader distribution of information under certain conditions.

5 RESOURCES AVAILABLE FOR ISAOS

The following subsections list the resources available for ISAOs. The descriptive summaries below are in part based on the information publicly available from their respective agencies' websites. These agency websites are the primary source for the information found in this document. For the most current and authoritative information, refer to the respective agency website and point of contact, accessible through the ISAO Standards Organization Resource Library at the ISAO.org web page.[14]

5.1 DEPARTMENT OF HOMELAND SECURITY

Many of DHS's programs, resources, and training platforms were created or otherwise modified to help organizations use the Cybersecurity Framework to improve their cyber resilience. The programs connect organizations with public and private-sector resources that align to the framework's five function areas: Identify, Protect, Detect, Respond, and Recover.

5.1.1 CYBERSECURITY FRAMEWORK FUNCTION AREAS

Identify—develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

[14] See https://www.ISAO.org/.

The activities in the Identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome categories within this function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Protect—develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services.

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Detect—develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

The Detect function enables the timely discovery of cybersecurity events. Examples of outcome categories within this function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Respond—develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

The Respond function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include Response Planning, Communications, Analysis, Mitigation, and Improvements.

Recover—develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome categories within this function include Recovery Planning, Improvements, and Communications.

5.1.2 CRITICAL INFRASTRUCTURE CYBER COMMUNITY VOLUNTARY PROGRAM

As part of Executive Order 13636, the Department of Homeland Security launched the Critical Infrastructure Cyber Community or C³ (pronounced “C cubed”) Voluntary Program to assist in enhancing critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology’s (NIST’s) Cybersecurity 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.

To contact C³, e-mail the program at ccubedvp@hq.dhs.gov. To stay informed of upcoming events, new resources, publications, and other announcements, subscribe to C³ Voluntary Program alerts.[15]

5.1.3 NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

The National Cybersecurity and Communications Integration Center (NCCIC) serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation, and recovery efforts.

5.1.3.1 AUTOMATED INDICATOR SHARING

Function Category: Protect, Detect

The Department of Homeland Security's Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information such as malicious IP addresses or the sender address of a phishing e-mail (although they can also be much more complicated).

AIS is a part of the Department's effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of its partners, protecting them from that particular threat. That means that adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS won't eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

More information is available from the United States Computer Emergency Readiness Team (US CERT).[16]

5.1.3.2 CYBER INCIDENT RESPONSE AND ANALYSIS

Function Category: Respond

The NCCIC offers incident response services to owners of critical infrastructure assets that are experiencing impacts from cyber-attacks. Services include digital media and malware analysis, identification of the source of an incident, analyzing

[15] See https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

[16] See https://www.us-cert.gov/ais.

the extent of the compromise, and developing strategies for recovery and improving defenses. Incident response teams also provide concepts for improving intrusion detection capabilities and ways to eliminate vulnerabilities and minimize losses from a cyber-attack. For more information or to request response services, e-mail ics-cert@hq.dhs.gov.

5.1.3.3 CYBER INFORMATION SHARING AND COLLABORATION PROGRAM

Function Category: Protect, Detect, Respond

The Cyber Information Sharing and Collaboration Program (CISCP) is a no-cost information sharing partnership between enterprises and DHS. It creates shared situational awareness across critical infrastructure communities, enhances cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverages government and industry subject matter expertise to collaboratively respond to cybersecurity incidents. To contact CISCP, e-mail ciscp_coordination@hq.dhs.gov.[17]

5.1.3.4 CYBERSECURITY EVALUATION TOOL AND ON-SITE CYBERSECURITY CONSULTING

Function Category: Identify, Protect

The Cybersecurity Evaluation Tool (CSET), a self-assessment tool, offers assessments of the security posture of industrial control systems. Features include mapping to control systems standards based on the sector, as well as a network architecture mapping tool. The tool can be downloaded for self-use, or organizations can request a facilitated site visit, which could include basic security assessments, network architectural review and verification, network scanning using custom tools to identify malicious activity and indicators of compromise, and penetration testing.[18]

5.1.3.5 ENHANCED CYBERSECURITY SERVICES

Function Category: Protect, Detect, Respond

Enhanced Cybersecurity Services (ECS) is an intrusion prevention and analysis capability that helps U.S.-based companies protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs). These CSPs in turn use that information to block certain types of malicious traffic from entering customer networks. All U.S.-based public and private entities are eligible to enroll in ECS. Program participation is voluntary and is designed to protect government intelligence, corporate information security, and the privacy of participants.[19]

[17] See https://www.dhs.gov/ciscp.

[18] See http://ics-cert.us-cert.gov/assessments.

[19] See https://www.dhs.gov/enhanced-cybersecurity-services.

5.1.3.6 INDUSTRIAL CONTROL SYSTEMS TRAINING

Function Category: Protect

The NCCIC's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers training in industrial control systems security at the overview, intermediate, and advanced levels, including web-based and instructor-led formats.[20]

5.1.3.7 INDUSTRIAL CONTROL SYSTEMS RECOMMENDED PRACTICES

Function Category: Protect

ICS-CERT offers a list of recommended practices aimed at helping industry understand and prepare for ongoing and emerging control systems cybersecurity issues, vulnerabilities, and mitigation strategies. ICS-CERT works with control systems manufacturers, service providers, researchers, and end users to ensure that the recommended practices are vetted by industry subject matter experts prior to publication. Recommended practices cover topics such as defense-in-depth strategies, cyber forensics, and incident response and are updated on a routine basis to account for emerging issues and practices.[21]

5.1.3.8 MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER

Function Category: Identify, Protect, Detect, Respond, Recover

Grant-funded by DHS, the Multi-State Information Sharing and Analysis Center (MS-ISAC) exists to improve the overall cybersecurity posture of state, local, tribal, and territorial governments and is designated as the key resource for cyber threat prevention, protection, response, and recovery. Through its 24/7 Security Operations Center, the MS-ISAC serves as a focal point for situational awareness and incident response for SLTT governments, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

The MS-ISAC is a collaborative cybersecurity organization that bolsters SLTT capacity and network defense capabilities against cyber threats. It provides a centralized forum for information sharing on cyber threats between the Federal Government and SLTT governing bodies through a number of crucial services, while providing opportunities to analyze and correlate information among SLTT membership. Collaboration and information sharing among members, private-sector partners, and DHS are the keys to success. Membership is free.[22]

5.1.3.9 NCCIC ALERTS, BULLETINS, TIPS, AND TECHNICAL DOCUMENTS

Function Category: Protect, Detect

[20] See http://ics-cert.us-cert.gov/training-available-through-ics-cert.

[21] See http://ics-cert.us-cert.gov/introduction-recommended-practices.

[22] See https://msisac.cisecurity.org/resources.

ICS-CERT and US-CERT publish alerts, bulletins, tips, and technical documents. ICS-CERT also offers an extensive bibliography of relevant standards and references. Both sets of documents and references help explain relevant control system vulnerabilities and the measures critical infrastructure owners and operators can take to mitigate them.[23]

5.1.3.10 NATIONAL CYBER AWARENESS SYSTEM

Function Category: Identify, Protect

The NCCIC produces advisories, alert and situation reports, analysis reports, current activity updates, daily summaries, indicator bulletins, periodic newsletters, recommended practices, a Weekly Analytic Synopsis Product (WASP), weekly digests, and a year in review to alert partners of emerging cyber threats, vulnerabilities, and current tips, released through the US-CERT National Cyber Awareness System (NCAS).[24]

5.1.3.11 NATIONAL CYBER EXERCISE AND PLANNING PROGRAM EXERCISE TEAM

Function Category: Protect, Respond

The NCCIC's National Cyber Exercise and Planning Program (NCEPP) provides cyber exercise and cyber incident response planning support to all DHS stakeholders. NCEPP delivers a full spectrum of cyber exercise planning workshops and seminars, and conducts tabletop, full-scale, and functional exercises, as well as the biennial National Cyber Exercise: Cyber Storm and annual Cyber Guard Prelude exercise. These events are designed to assist organizations at all levels in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities. For additional information, e-mail CEP@hq.dhs.gov.

5.1.3.12 NATIONAL CYBERSECURITY ASSESSMENT AND TECHNICAL SERVICES

Function Category: Identify, Protect, Recover

The NCCIC's National Cybersecurity Assessment and Technical Services (NCATS) offers cybersecurity scanning and testing services that identify vulnerabilities within stakeholder networks and provide risk analysis reports with actionable remediation recommendations. These critical services enable proactive mitigation to exploitable risks and include network (wired and wireless) mapping and system characterization; vulnerability scanning and validation; threat identification and evaluation; social engineering, application, database, and operating system configuration review; and incident response testing. For additional information, e-mail NCATS_Info@DHS.gov.

[23] See http://ics-cert.us-cert.gov.

[24] See http://us.cert.gov/ncas and https://www.us-cert.gov/mailing-lists-and-feeds.

5.1.4 ADDITIONAL DHS RESOURCES

Beyond the resources offered by the NCCIC, DHS provides a variety of assessments, education, workforce development, and awareness resources. These are generally available for the private sector; state, local, tribal, and territorial governments; and federal agencies.

5.1.4.1 CYBER INFRASTRUCTURE SURVEY TOOL

Function Category: Identify, Protect

The Cyber Infrastructure Survey Tool (C-IST) is an assessment of essential cybersecurity practices in place for critical services within critical infrastructure organizations. C-IST is a structured, interview-based assessment focusing on more than 80 cybersecurity controls grouped under five key surveyed topics. Following the assessment, DHS provides participants with the ability to review and interact with the surveyed findings through a user-friendly, data-rich dashboard.[25]

5.1.4.2 CYBER RESILIENCE REVIEW

Function Category: Identify, Protect

The Cyber Resilience Review (CRR) is a no-cost, voluntary, nontechnical assessment to evaluate an organization's operational 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 practices and procedures across a range of 10 activity areas, including risk management, incident management, and service continuity. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.[26]

5.1.4.3 CYBER SECURITY ADVISORS

Function Category: Identify, Protect, Respond

Cyber Security Advisors (CSAs) are regionally located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of U.S. critical infrastructure and state, local, territorial, and tribal (SLTT) governments. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. They bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer coordination with the federal government. CSAs represent a front-line approach and promote resilience of key cyber infrastructures throughout the United States and its territories. For additional information, e-mail cyberadvisor@hq.dhs.gov.

[25] See http://www.lba.org/userfiles/files/CIST_Fact_Sheet_2014.pdf.

[26] See http://us-ert.gov/ccubedvp/self-service-crr.

5.1.4.4 CYBERSECURITY SERVICE OFFERING REFERENCE AIDS

Function Category: Protect, Respond

DHS's National Protection and Programs Directorate (NPPD) has developed a list of freely available reports and resources pertinent to managing the acquisition of cybersecurity services. It is not intended to be exhaustive but covers a wide range of cybersecurity services, including cloud service providers, cyber incident response, cloud computing, software assurance, and industrial control systems. While most of its recommendations and reports are vendor-agnostic, some identify specific service providers that have met certification criteria related to their service offerings. DHS does not endorse any particular service provider or offering.[27]

5.1.4.5 CYBERSECURITY WORKFORCE DEVELOPMENT TOOLKIT

Function Category: Identify, Protect, Detect, Respond, Recover

Organizations need to have the right staff in place to protect their information, customers, and networks. They need to find and keep top cybersecurity staff. DHS has a new resource to help organizations get—and keep—the right cybersecurity staff and use the Workforce Framework.

The Cybersecurity Workforce Development Toolkit will help organizations understand their cybersecurity workforce and staffing needs; it includes such things as templates to create cybersecurity career paths, and resources to recruit and retain top cybersecurity talent.

Use the toolkit to talk with managers about building their cybersecurity teams, lead employees to professional development opportunities, and guide strategic planning efforts for future staffing needs.[28]

5.1.4.6 FEDERAL EMERGENCY MANAGEMENT AGENCY, EMERGENCY PLANNING EXERCISES

Function Category: Identify, Protect, Detect, Respond, Recover

The Federal Emergency Management Agency (FEMA), Private Sector Division, Office of External Affairs, introduced a series of tabletop exercises in 2010 as a tool to help private-sector organizations advance their continuity, preparedness, and resiliency. Tabletop exercises are designed to help organizations test a hypothetical situation, such as a natural or manmade disaster, and evaluate their ability to cooperate and work together, as well as test their readiness to respond.[29]

---

[27] See https://www.us-cert.gov/sites/default/files/c3vp/cybersecurity_service_offerings_reference_aids.pdf.

[28] See https://niccs.us-cert.gov/home/cybersecurity-workforce-development-toolkit.

[29] See http://www.fema.gov/emergency-planning-exercises.

5.1.4.7 FEDERAL VIRTUAL TRAINING ENVIRONMENT

Function Category: Identify, Protect, Detect, Respond, Recover

The Federal Virtual Training Environment (FedVTE) content library contains pre-recorded classroom cybersecurity training for Federal Government personnel and contractors, as well as State, local, tribal, and territorial government personnel. FedVTE provides government-wide, online, and on-demand access to cybersecurity training to help the workforce maintain expertise and foster operational readiness. With courses ranging from beginner to advanced levels, the system is available at no cost to users and is accessible from any Internet-enabled computer.[30]

5.1.4.8 HOMELAND SECURITY INFORMATION NETWORK

Function Category: Identify, Protect, Detect, Respond, Recover

The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive but Unclassified information. Federal, state, local, territorial, tribal, international, and private-sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and share the information they need to do their jobs. HSIN's features and capabilities include the following:

- Alerts and notifications
- Basic Learning Management System
- Comprehensive HSIN training
- Document repository
- GIS mapping
- Instant messaging (HSIN Chat)
- Managed workflow capabilities
- Secure messaging (HSINBox)
- Web conferencing (HSIN Connect).

For more information about HSIN, contact HSIN.Outreach@hq.dhs.gov.

5.1.4.9 NATIONAL CYBER SECURITY AWARENESS MONTH

Function Category: Identify, Protect, Detect, Respond, Recover

Recognizing the importance of cybersecurity awareness, the Department of Homeland Security leads National Cyber Security Awareness Month (NCSAM) annually in October. The Department is committed to raising cybersecurity awareness across the nation and to working across all levels of government, in

[30] See https://www.fedvte.usalearning.gov.

the private sector, and internationally to protect against and respond to cyber incidents.

Since President Obama's proclamation in 2004, NCSAM has been formally recognized by Congress, federal, state, and local governments, as well as leaders from industry and academia. This united effort is necessary to maintain a cyberspace that is safer, more resilient, and remains a source of tremendous opportunity and growth for years to come. NCSAM is designed to engage and educate public and private-sector partners through events and initiatives with the goal of raising awareness about cybersecurity and increasing the resiliency of the nation in the event of a cyber incident.[31]

5.1.4.10 NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

Function Category: Identify, Protect, Detect, Respond, Recover

The National Cybersecurity Workforce Framework is an online resource that classifies the typical duties and skill requirements of cybersecurity workers. It is meant to define professional requirements in cybersecurity, much as in other professions such as medicine and law. The framework organizes cybersecurity into seven high-level categories, each comprising several specialty areas. Clicking on a specialty area reveals the details about that area. Each specialty area detail displays the standard tasks and the knowledge, skills, and abilities needed to successfully complete those tasks.[32]

5.1.4.11 NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Function Category: Identify, Protect, Detect, Respond, Recover

The National Initiative for Cybersecurity Careers and Studies (NICCS) portal is a one-stop shop for cybersecurity careers and studies. It connects the public with information on cybersecurity awareness, degree programs, training, careers, and talent management. The portal includes a searchable catalog of more than 2,000 cybersecurity courses offered nationwide. Many courses are offered for free to government employees and veterans through the DHS Federal Virtual Training Environment.[33]

5.1.4.12 NATIONAL TRAINING AND EDUCATION DIVISION

Function Category: Identify, Protect

The National Training and Education Division (NTED) provides tailored training to enhance the capacity of state and local jurisdictions to prepare for, prevent, deter, respond to, and recover safely and effectively from potential manmade and natural catastrophic events, including terrorism.

---

[31] See https://niccs.us-cert.gov/awareness/national-cyber-security-awareness-month.

[32] See https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework.

[33] See http://niccs.us-cert.gov.

NTED training conforms to nationally recognized standards and adheres to the principles of both adult learning theory, including problem-based learning, and instructional system design. In addition, training developed under the auspices of NTED undergoes a rigorous validation process before delivery and is continuously assessed while being delivered to the public. NTED training is increasingly being tested and evaluated through state and local exercises to enhance further development of training courses. [34]

5.1.4.13 PROTECTIVE SECURITY ADVISORS

Function Category: Identify, Protect, Respond

Protective Security Advisors (PSAs) are security subject matter experts who engage with SLTT government mission partners and members of the private-sector stakeholder community to protect the Nation's critical infrastructure. Regional directors oversee and manage the Department's PSA program in their respective region, while PSAs facilitate local field activities in coordination with other DHS offices. The PSAs support the protection of critical infrastructure through planning, coordinating, and conducting voluntary security surveys and assessments; planning and conducting outreach activities; supporting National Special Security Events and Special Event Activity Rating events; responding to incidents; and coordinating and supporting improvised explosive device awareness and risk mitigation training.[35]

5.1.4.14 STOP.THINK.CONNECT.CAMPAIGN

Function Category: Identify, Protect, Detect, Respond, Recover

Launched in 2010, the Stop.Think.Connect. (STC) campaign was created to empower Americans to reduce cyber risk online by incorporating safe habits into their online routines. The campaign was conceived by a private coalition, the National Cyber 602 Security Alliance (NCSA). The STC campaign provides free, downloadable resources on online safety for citizens and professionals to use and share.[36]

5.1.5 NATIONAL INFRASTRUCTURE PROTECTION PLAN

The National Infrastructure Protection Plan (NIPP) provides a framework for collaboration between DHS and the private sector and implements Federal Government policy for improving the Nation's resilience. It lays out the structural model through which DHS executes collaboration and coordination functions with the private sector. This model functions through 16 critical infrastructure sectors and involves organizations and mechanisms designed to achieve collaboration and coordination within the specified sectors. Many established ISACs operate within the NIPP's sector-based approach. ISAOs, having emerged after issuance of

[34] See http://www.firstrespondertraining.gov.

[35] See http://dhs.gov/protective-security-advisors.

[36] See http://dhs.gov/stopthinkconnect.

NIPP 2013, are not countenanced within the sector model. However, the NIPP broadly calls for collaboration and partnership between the public and private sectors. Moreover, the following organizations specified in the NIPP can afford ISAOs a collaboration and cooperation framework that may operate in parallel and in partnership with the NIPP sector model.[37]

5.1.5.1 COORDINATING COUNCILS

The NIPP established four cross-sector councils that participate in planning efforts regarding the development of national priorities and policy related to the resilience and capacity-building objectives of the NIPP: the Critical Infrastructure Cross-Sector Council; the Federal Senior Leadership Council; the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); and the Regional Consortium Coordinating Council (RC3). The SLTTGCC and RC3 responsibilities under the NIPP for coordination among its non-federal and geographically dispersed members, while tied to the federal resilience framework through the NIPP, render them suitable for ISAO supporting functions.

5.1.5.2 STATE, LOCAL, TERRITORIAL, AND TRIBAL GOVERNMENT COORDINATING COUNCIL

SLTTGCC serves as a forum to promote the engagement of SLTT partners as active participants in national critical infrastructure security and resilience efforts, including cybersecurity and information sharing functions, and to provide an organizational structure to coordinate across jurisdictions on SLTT government-level guidance, strategies, and programs, including cybersecurity and information sharing.[38]

5.1.5.3 REGIONAL CONSORTIUM COORDIATING COUNCIL

RC3 is a consortium composed of regional groups engaged in partnering functions in support of resilience, all-hazards planning and coordination, training, cybersecurity, and other resilience projects and initiatives. RC3 supports its member organizations with awareness, education, and mentorship on a wide variety of subjects, projects, and initiatives. RC3 provides a framework that supports existing regional groups in their efforts to promote resilience activities in the public and private sectors.[39]

[37] See https://www.dhs.gov/national-infrastructure-protection-plan.

[38] See https://www.dhs.gov/sltt-gcc.

[39] See https://rtriplec.wordpress.com/.

5.2 DEPARTMENT OF JUSTICE

5.2.1 BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber-attack. A quick, effective response can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is before an incident occurs.

The Department of Justice's Cybersecurity Unit has prepared a list of best practices to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private-sector companies that have managed cyber incidents. Although the document was drafted with smaller, less well-resourced organizations in mind, even larger organizations with more experience in handling cyber incidents may benefit from it.[40]

5.3 FEDERAL BUREAU OF INVESTIGATION

5.3.1 DOMESTIC SECURITY ALLIANCE COUNCIL

Modeled on the U.S. Department of State's Overseas Security Advisory Council, the Domestic Security Alliance Council (DSAC) was created in October 2005 to strengthen information sharing with the private sector to help prevent, detect, and investigate threats impacting American businesses. Today, DSAC enables an effective two-way flow of vetted information between the Federal Bureau of Investigation (FBI) and participating members, including some of America's most respected companies. It also gives the Bureau valuable contacts when it needs assistance with its investigations.[41]

5.3.2 FUSION CENTERS

Fusion centers are usually set up by states or major urban areas and run by state or local authorities, often with the support of the FBI. They "fuse" intelligence from participating agencies to create a more comprehensive threat picture, locally and nationally.[42] They integrate new data into existing information, evaluate it to determine its worth, analyze it for links and trends, and disseminate their findings to the appropriate agency for action.

[40] See https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

[41] See https://www.fbi.gov/about/partnerships/domestic-security-alliance-council.

[42] See https://archives.fbi.gov/archives/news/stories/2009/march/fusion_031209.

5.3.3 INFRAGARD

InfraGard is a partnership between the FBI and the private sector. It is an association of people who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. Each InfraGard Members Alliance (IMA) is geographically linked with an FBI field office, providing all stakeholders immediate access to experts from law enforcement, industry, academic institutions, and other federal, state, and local government agencies. By leveraging the talents and expertise of the InfraGard network, information is shared to mitigate threats to critical infrastructure and key resources. Collaboration and communication are the keys to protection. Providing timely and accurate information to those responsible for safeguarding our critical infrastructures, even at a local level, is paramount in the fight to protect the United States and its resources.[43]

Today, 85 InfraGard chapters with a total of more than 35,000 members work through the field offices to ward off attacks against critical infrastructure that can come in the form of computer intrusions, physical security breaches, or other methods. These members represent state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry.

At the chapter level, members meet to discuss threats and other matters that impact their companies. The meetings, led by a local governing board and an FBI agent who serves as InfraGard coordinator, give everyone an opportunity to share experiences and best practices.

InfraGard members have access to a secure FBI communications network featuring an encrypted website, web mail, listservs, and message boards. The website plays an integral part in information-sharing efforts: It also is used. In recent years the agency has opened hundreds of cases as a result of information provided by InfraGard members and has received assistance on more than 1,000 others.

5.3.4 INTERNET CRIME COMPLAINT CENTER

The Internet Crime Complaint Center (IC3) provides the public with a mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity. It also develops effective alliances with law enforcement and industry partners.[44] Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness. ISAOs can identify IC3 as a resource to help their members report Internet crime, and they may also elect to submit reports to IC3 on their members' behalf. ISAOs may also make use of public alerts published by IC3.

[43] See https://www.infragard.org/.

[44] See http://www.ic3.gov.

Since 2000, IC3 has received complaints crossing the spectrum of cyber crime matters, including online fraud in its many forms, such as intellectual property rights matters, computer intrusions (hacking), economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of Internet-facilitated crimes. Regardless of the label placed on cyber crimes, the potential for them to overlap with other criminal matters is substantial. Therefore, the former Internet Fraud Complaint Center was renamed "IC3" in October 2003 to better reflect the broad character of such matters having an Internet, or cyber, nexus, and to minimize the need to distinguish "Internet fraud" from other potentially overlapping cyber crimes.

5.3.5 AFFILIATED INFORMATION SHARING ASSOCIATION

The National Cyber Forensics & Training Alliance, located in Pittsburgh, consists of experts from industry, academia, and the FBI who work side by side to share and analyze information on the latest and most significant cyber threats.[45]

5.4 FEDERAL COMMUNICATIONS COMMISSION

5.4.1 COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL

The mission of the Communications Security, Reliability and Interoperability Council (CSRIC) is to provide recommendations to the Federal Communications Commission (FCC) to ensure optimal security and reliability of communications systems, including telecommunications, media, and public safety.[46] The CSIRC has identified best practices and developed recommendations to identify, protect, detect, respond to, and recover from cyber events.[47] The CSIRC has formed a number of working groups that have developed useful information on cybersecurity information sharing, secure hardware and software, and consensus cybersecurity controls, among other topics.

5.4.2 CYBERSECURITY PLANNING GUIDE

The Cybersecurity Planning Guide is designed to meet the specific needs of a company using the FCC's customizable Small Biz Cyber Planner tool. The tool is designed for businesses that lack the resources to hire dedicated staff to protect their business, information, and customers from cyber threats. Even a business with one computer or one credit card terminal can benefit from this important tool.

[45] See https://www.ncfta.net/.

[46] For more information on CSRIC, see https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-10.

[47] To access CSRIC best practices, see https://www.fcc.gov/nors/outage/ bestpractice/BestPractice.cfm.

Businesses using more sophisticated networks with dozens of computers should consult a cybersecurity expert in addition to using the cyber planner.[48]

5.4.3 CYBERSECURITY TIP SHEET

The FCC has released a Cybersecurity Tip Sheet, which outlines the top 10 ways for entrepreneurs to protect their companies—and customers—from cyber attack. This streamlined resource features tips on creating a mobile device action plan and on payment and credit card security.[49]

5.4.4 SMALL BUSINESS CYBER PLANNER 2.0

Information technology and high-speed Internet service are great enablers of small business success, but with the benefits comes the need to guard against growing cyber threats. In October 2012, the FCC relaunched the Small Biz Cyber Planner 2.0,[50] an online resource to help small businesses create customized cybersecurity plans. Companies can use this tool to create and save a custom cybersecurity plan, choosing from a menu of expert advice to address their specific business needs and concerns.

5.5 FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

5.5.1 CYBERSECURITY ASSESSMENT TOOL

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool to help institutions identify their risks and determine their cybersecurity preparedness. The assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.[51]

5.6 FEDERAL TRADE COMMISSION

5.6.1 CAN-SPAM ACT: A COMPLIANCE GUIDE FOR BUSINESS

The CAN-SPAM Act establishes requirements for commercial messages, gives recipients the right to have companies stop e-mailing them, and spells out tough penalties for violations.[52]

[48] See https://transition.fcc.gov/cyber/cyberplanner.pdf.

[49] See https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf.

[50] See https://www.fcc.gov/cyberplanner.

[51] See https://www.ffiec.gov/cyberassessmenttool.htm.

[52] See https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

5.6.2 CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNEET OF THINGS

The Careful Connections guidance provides advice for businesses about building security into products connected to the Internet of Things, including proper authentication, reasonable security measures, and carefully considered default settings.[53]

5.6.3 CHILDREN'S ONLINE PRIVACY PROTECTION RULE: A SIX-STEP COMPLIANCE PLAN FOR YOUR BUSINESS

This compliance guidance is a step-by-step plan for determining whether a company is covered by the Children's Online Privacy Protection Act, and it guides companies on how to comply with the rule.[54]

5.6.4 COMPLYING WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE

This guidance helps businesses complying with the Federal Trade Commission's (FTC's) Health Breach Notification Rule specifically determine whether they are covered by the rule and what they must do if they experience a breach of personal health records.[55]

5.6.5 DISPOSING OF CONSUMER REPORT INFORAMTION? RULE TELLS HOW

This guidance provides information on how companies can comply with the Disposal Rule, which requires companies to take steps to securely dispose of sensitive information derived from consumer reports once they are finished with it.[56]

5.6.6 FIGHTING IDENTITY THEFT WITH THE RED FLAGS RULE: A GUIDE FOR BUSINESS

This guide provides businesses with tips to determine whether they need to design an identity theft prevention program.[57]

---

[53] See https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things.

[54] See https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[55] See https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[56] See https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how.

[57] See https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business.

5.6.7 INFORMATION COMPROMISE AND RISK OF IDENTITY THEFT: GUIDANCE FOR YOUR BUSINESS

These days, it is almost impossible to be in business and not have personally identifying information about customers or employees. If this information falls into the wrong hands, it could put them at risk for identity theft. This guidance provides businesses with the steps to take and whom to contact if sensitive data are compromised.[58]

5.6.8 MOBILE HEALTH APP DEVELOPERS: FTC BEST PRACTICES

When developing a health app, sound privacy and security practices are key to consumer confidence. These FTC best practices should help businesses build privacy and security into their apps. These practices also can help companies comply with the FTC Act.[59]

5.6.9 MOBILE HEALTH APPS INTERACTIVE TOOL

This interactive tool can help businesses determine which federal rules may apply when they are developing a health app for mobile devices.[60]

5.6.10 PEER-TO-PEER FILE SHARING: A GUIDE FOR BUSINESS

Most businesses collect and store sensitive information about their employees and customers. This guide provides businesses using Peer-to-Peer (P2P) file-sharing software with the security implications of using such software and ways to minimize the risks associated with it.[61]

5.6.11 PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS

This guide provides practical tips for businesses on creating and implementing a plan for safeguarding personal information.[62]

5.6.12 START WITH SECURITY: A GUIDE FOR BUSINESS

This guide offers 10 practical lessons that businesses can learn from the FTC's 50-plus data security settlements. Lessons include suggestions like "Start with

[58] See https://www.ftc.gov/tips-advice/business-center/guidance/information-compromise-risk-identity-theft-guidance-your.

[59] See https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

[60] See https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[61] See https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business.

[62] See https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

security," "Control access to data sensibly," and "Require secure passwords," each complete with detailed tips and explanations. The guide also links to online tutorials to help train employees, as well as publications to address particular data security challenges.[63]

5.7 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

5.7.1 FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the president issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," in February 2013.[64] It directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure.

Created through collaboration between industry and government, the Framework for Improving Critical Infrastructure Cybersecurity[65] consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

A companion roadmap discusses future steps and identifies key areas of cybersecurity development, alignment, and collaboration.

NIST welcomes informal feedback about the framework and roadmap. Organizations and individuals may contribute observations, suggestions, examples of use, and lessons learned to cyberframework@nist.gov.

5.7.2 NIST INTERAGENCY REPORT 7621—SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS

Small businesses are a very important part of the economy and a significant part of the critical U.S. economic and cyber infrastructure. Because larger businesses have been strengthening information security with significant resources, technology, people, and budgets for some years, they have become more difficult targets. As a result, hackers and cyber criminals are now focusing more attention on

[63] See https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[64] See https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[65] See https://www.nist.gov/cyberframework.

less secure small businesses. This Interagency Report helps small business managers understand how to provide basic security for their information, systems, and networks.[66]

5.7.3 NIST SPECIAL PUBLICATION 800-36: GUIDE TO SELECTING INFORMATION TECHNOLOGY SECURITY PRODUCTS

The selection of information technology security products is an integral part of the design, development, and maintenance of an infrastructure that ensures confidentiality, integrity, and availability of mission-critical information. NIST Special Publication 800-36, "Guide to Selecting Information Technology Security Products," defines broad security product categories and specifies product types within those categories. It provides a list of characteristics and pertinent questions an organization should ask when selecting such products.[67]

5.7.4 NIST SPECIAL PUBLICATION 800-150: DRAFT GUIDE TO CYBER THREAT INFORMATION SHARING

This draft guide provides guidelines for establishing, participating in, and maintaining cyber threat information sharing relationships. The publication describes the benefits and challenges of sharing, the importance of building trust, the handling of sensitive information, and the automated exchange of cyber threat information. The goal of the publication is to provide guidelines that help improve cybersecurity operations and risk management activities through safe and effective information sharing practices. The guide is intended for computer security incident response teams (CSIRTs), system and network administrators, security staff, privacy officers, technical support staff, chief information security officers (CISOs), chief information officers (CIOs), computer security program

5.8 NATIONAL SECURITY AGENCY

5.8.1 NATIONAL SECURITY CYBER ASSISTANCE PROGRAM

The National Security Agency (NSA)/Information Assurance Directorate (IAD) has established a National Security Cyber Assistance Program[68] allowing commercial organizations to receive accreditation for cyber incident response services. This accreditation validates that an organization has established processes, effective tools, and knowledgeable people with the proper skills and expertise to perform cyber incident response for national security systems. The

[66] See http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.
[67] See http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf.
[68] See https://www.nsa.gov/ia/programs/cyber_assistance_program/index.shtml.

accreditation is issued only to organizations that meet the criteria set forth in the NSA/IAD Accreditation Instruction Manual.

5.9 SMALL BUSINESS ADMINISTRATION

The Small Business Administration (SBA) provides information to small business and small business network partners through SBA's landing page covering government-wide cybersecurity best practices.[69] Additionally, each SBA District Office can disseminate information to SBA resource partners through a combination of webinars, in-person trainings, and roundtables.

[69] See https://www.sba.gov/cybersecurity.