ISAO 600-1

U.S. Government Relations, Programs, and Services

Draft Document—Request for Comment

v0.4

ISAO Standards Organization

July 27, 2016

Item	Version	Description	Date
1	0.1	Initial document: Products and Services	April 5, 2016
2	0.2	Update: Role of Government and State and Local	April 19, 2016
3	0.3	Update: Regulation	April 22, 2016
4	0.4	Update: First round of comments inserted	July 26, 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
Executive Director, ISAO SO
Director, Center for Infrastructure Assurance and Security, UTSA

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

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

Working Group Six—Government Relations

Michael Echols
Director, Cyber Joint Program Management Office
Cybersecurity and Communications,
Department of Homeland Security

David Weinstein
Chief Technology Officer
State of New Jersey

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

Doug DePeppe
Cyber Resilience Institute

Stuart Gerson
Epstein Becker & Green PC

Elizabeth McGrath
The MITRE Corporation

Mark Boggis
Cybersecurity Policy Solutions

Nancy Pomerleau
Department of Homeland Security

Ricky Chitwood
Federal Aviation Administration

Table of Contents

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 regulations regarding information sharing within the United States. Developing trust between the U.S. government and ISAOs is a major consideration for all parties, particularly in the area of information sharing and privacy. This document also addresses considerations for ISAO interaction with the intelligence community, law enforcement agencies, U.S. regulatory agencies, the Department of Homeland Security, and other government departments and agencies.

The primary sections of this voluntary ISAO Standards Organization (SO) guide are organized as follows:

- Section 2 outlines the scope, strategy, and outputs concerning the role of government with respect to ISAOs.
- Section 3 provides an overview of relevant federal regulations.
- Section 4 addresses issues and considerations from the perspective of state and local governments.
- Section 5 identifies government resources available to assist ISAOs.

This is the first complete draft of this voluntary guide on scope, strategy, and outputs concerning the role of government. Additionally, this document provides a wide range of available services to new and emerging ISAOs. This draft is intended to be a starting point and will be updated continuously through public input and working group research.

2 SCOPE, STRATEGY, AND OUTPUTS CONCERNING THE ROLE OF GOVERNMENT

Presidential Directive 41, released 26 July 2016, states " 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". 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, there are many government programs that ISAOs may utilize in the performance of their operation.

2.1 PRELIMINARY MATTERS

There are six fundamental issues to resolve before exploring other issues:

- What voice should serve as the driver for issue spotting and analysis?
- What broad functional categories should serve as a framework for analysis?
- What principles should guide our analysis of the legitimacy of government participation?
- What is the best way to develop role of government issues for consideration?
- To what extent should mechanisms be created to resolve disputes at the federal, state, and local level between governmental and private-sector entities—for example, in the context of law enforcement investigations?
- What continuity mechanisms are needed to ensure a viable and meaningful feedback and issue resolution loop?

2.2 WHAT VOICE?

Information sharing, cross-sector partnering, and regional capacity building are part of the national approach to improved cybersecurity that has been promulgated at a national level (such as via executive orders and federal law). The approach that led to establishment of the ISAO SO was by Executive Order from the White House. To achieve national adoption of the ISAO approach to improved cybersecurity, other views besides those of the federal government are essential to achieving success.

This pathway is to ensure dialogue and collaboration. The voice of the federal government will help to ensure that the voluntary standards for ISAOs reflect all levels of appropriate considerations and take into account the equities of all participants in the public-private partnership.

2.3 WHAT CATEGORIES?

The scope suggested by the ISAO SO was re-framed, with a focus on the roles of government with respect to the enablement, collaboration, and support for

ISAOs. The analysis will focus on these participation functions, assessing these categories for federal, state, and local government.

2.4 WHAT PRINCIPLES?

Below is an initial list of roles that are generally accepted as government functions in society (assessed at each level). The purpose of the list is for use as a measure of the legitimacy of government involvement in functions identified for analysis. The generally accepted roles are:

- National security and defense
- International relations and diplomacy
- Public safety and preparedness
- Administration of justice
- Governance and legislation
- Economic stability
- Critical infrastructure
- Social welfare
- Education
- Law enforcement.

Online research and subject matter experts were used to produce this list. It is anticipated this list will continue to evolve and increase in specificity as use cases trigger deeper analysis. This list is helpful in terms of establishing a framework for assessing the legitimacy of a government role.

2.5 WHAT PROCESS FOR ISSUE DEVELOPMENT?

Issues concerning the role of government can affect many of the voluntary standards under development by the ISAO SO. At the same time, the organizing and standards development work of these other groups is likely to generate concrete role of government issues. A liaison structure will help participants spot issues and refer them to the working group for analysis and production of consensus views, recommendations, and best practices.

2.6 WHAT POLICIES OR MECHANISMS MIGHT BE CREATED FOR RESOLVING DISPUTES?

Especially, but not only, in the area of law enforcement, disputes will arise concerning the desire for government entities at all levels to obtain information from private-sector entities whose potential cooperation might be conflicted by various privacy interests. While the safety and security components of the role of government are clear enough, can the government’s role be amplified to involve

mechanisms short of judicial proceedings that involve ongoing conventions between government and ISAOs or groups of ISAOs?

2.7 WHAT PERMANENT CONTINUITY?

The initial view is that role of government issues will continue to emerge as society adopts and implements the ISAO approach. A future recommendation is anticipated that will outline the need for permanence and offer a proposed model that enables continuity and meaningful contributions to a dynamic ISAO ecosystem.

3 OVERVIEW OF FEDERAL REGULATIONS FOR ISAO CONSIDERATIONS

3.1 FEDERAL STATUTES RELATED TO INFORMATION SHARING

ISAOs may wish to consider a number of existing federal statutes when establishing policies and procedures for sharing of information, including those discussed below.

3.1.1 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 the private sector and the federal government. CISA provides various protections to non-federal entities that share cyber threat indicators or defensive measures with the federal government. The DHS Automated Indicator Sharing (AIS) initiative is the principal mechanism for such sharing. Sharing information with DHS through AIS or other DHS mechanisms in accordance with CISA provides the submitter with certain liability protections[1].

As mandated by the Cybersecurity Act of 2015, 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 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.

[1] Click here for CISA information.

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

The procedures outlined in this document describe the current mechanisms through which the appropriate federal entities, as named in Section 102(3), share 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, 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. 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.

3.1.1.2 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

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

1. Identification of types of information that would qualify as a cyber threat indicator under the Act that would be unlikely to include information that is not directly related to a cybersecurity threat and is personal information of a specific individual or information that identifies a specific individual; and

2. Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

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

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

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

This document establishes privacy and civil liberties guidelines governing the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with the activities authorized by CISA, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats, any other applicable provisions of law, and the Fair Information Practice Principles (FIPPs) set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

Federal entities engaging in activities authorized by CISA must do so in full compliance with the Constitution and all other applicable laws of the United States, Executive Orders; other Executive Branch directives, regulations, policies, and procedures; court orders; and all other legal, policy, and oversight requirements. Nothing in these guidelines affects the conduct of authorized law enforcement or intelligence activities or modifies applicable authority of a department or agency of the federal government, including, but not limited to, the protection of classified information and sources and methods and the national security of the United States.

3.1.1.5 PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

The PCII program enhances voluntary information sharing between infrastructure owners and operators and the government by providing a level of protection to facilities submitting information authorized as PCII to DHS. This better enables DHS to work directly with infrastructure owners and operators to identify vulnerabilities, mitigation strategies, and protective measures. If the information submitted to DHS satisfies the requirements of the CII Act, it is protected from:

- FOIA
- State, tribal, and local disclosure laws
- Use in regulatory actions
- Use in civil litigation.

PCII protections mean that homeland security partners, including ISAOs, can be confident that sharing their information with the government will not expose sensitive or proprietary data[2]. In fact, the PCII final rule specifically discusses the protections afforded to information provided to DHS by ISAOs.

You may view guidance documents and learn more about AIS and sharing cyber threat indicators by visiting the US CERT page[3].

3.1.2 CRITICAL INFRASTRUCTURE INFORMATION ACT OF 2002/PROTECTED CRITICAL INFRASTRUCTURE INFORMATION PROGRAM

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 authorized 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 FOIA, 5 U.S.C. § 552, and other laws, rules, and processes. To implement the CII Act, DHS established the PCII program, 6 Code of Federal Regulations (CFR) Part 29.

3.1.3 THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act, 5 U.S.C. § 552, generally provides that any person has the right to request access to federal agency records or information except to the extent that the records are protected from disclosure. Records may be protected from disclosure under one of nine exemptions contained in the law:

- Classified information for national defense or foreign policy
- Internal personnel rules and practices
- Information that is exempt under other laws
- Trade secrets and confidential business information
- Interagency or intra-agency memoranda or letters that are protected by legal privileges
- Personnel and medical files
- Law enforcement records or information
- Information concerning bank supervision
- Geological and geophysical information.

Congress also provided special protection in the FOIA for three narrow categories of law enforcement and national security records. The provisions

[2] Link to PCII Program Information.
[3] Link to US CERT Cyber threat and AIS information.

protecting those records are known as “exclusions.” The first exclusion protects the existence of an ongoing criminal law enforcement investigation when the subject of the investigation is unaware that it is pending and disclosure could reasonably be expected to interfere with enforcement proceedings. The second exclusion is limited to criminal law enforcement agencies and protects the existence of informant records when the informant’s status has not been officially confirmed. The third exclusion is limited to the FBI and protects the existence of foreign intelligence or counterintelligence, or international terrorism records when the existence of such records is classified. Records falling within an exclusion are not subject to the requirements of the FOIA[4].

.

3.1.4 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 sets forth various agency record-keeping requirements[5].

3.2 FEDERAL CYBERSECURITY REGULATIONS WITH AN INFORMATION SHARING NEXUS

A small number of existing or proposed federal regulations concerning cybersecurity touch on cybersecurity information sharing that ISAOs may wish to consider when establishing policies and procedures. They include those discussed below.

3.2.1 CHEMICAL FACILITY ANTI-TERRORISM STANDARD

Under the Chemical Facility Anti-Terrorism Standards[6] (CFATS), 6 CFR Part 27, high-risk chemical facilities must develop and submit to DHS for approval site security plans that, among other things, include the facility’s cybersecurity measures. While CFATS-covered facilities have flexibility in establishing a

[4] Link to FOIA information
[5] Link to Privacy Act information
[6] Link to CFATS information

security posture that is tailored to their unique characteristics, DHS expects such facilities to include in their security plans a description of their approach to addressing cybersecurity incidents, including the reporting of such incidents to US-CERT (www.us-cert.gov).

3.2.2 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 "Post-market Management of Cybersecurity in Medical Devices (Draft Guidance)."[7] 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 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 governmental regulation based on the information received.

[7] Management of Cybersecurity Medical Devices.

- It should be assumed that the relevance of cyber threat and vulnerability information extends outside of a formal information sharing environment—that is, entities external to the ISAO could benefit from the information being shared. There should to be a mechanism to ensure that such an entity is able to receive sensitive cyber threat and vulnerability information upon request.
- 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

The greatest barrier to sharing cyber threat and vulnerability information with state governments is state disclosure laws. Critical infrastructure and cyber disclosure exemption laws would streamline the sharing of information between private entities and government to set a pathway so that cybersecurity information sharing is more proactive rather than reactive. This could facilitate and encourage the private sector to participate and collaborate with states more regularly. Several states have begun to address this issue via state legislation, creating such exemptions for critical infrastructure and cyber security information. It is recommended that states 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 defined using:
  - The federal definition of critical infrastructure information found within 6 United States Code (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:
  - 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 between local, state, federal, and private-sector stakeholders. These capabilities include but are not limited to those discussed below.

4.3.1 PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

Formed as a result of the passage of the Critical Infrastructure Act in 2002, the Protected Critical Infrastructure Information (PCII) program affords protections to information provided by the private sector to the federal government. These protections include exemption from the federal Freedom of Information Act (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 MEMORANDUMS OF UNDERSTANDING OR AGREEMENT

States and localities should also consider the use of Memorandums 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 a PCII like 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 broader distribution of information under certain conditions.

5 RESOURCES AVAILABLE FOR ISAOs

Listed below are the resources available for ISAOs. The descriptive summaries below are in part based on the information publicly available from their respective agencies' web sites. These agency web sites 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 www.ISAO.org.

5.1 DEPARTMENT OF HOMELAND SECURITY (DHS)

The DHS resources below are available to assist ISAOs today and are aligned to the five cybersecurity framework function areas:

- Identify
- Protect
- Detect
- Respond
- Recover.

5.1.1 RESOURCES TO IDENTIFY THREATS

Activities to identify threats 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. Categories, which will be subdivisions of each of the five function areas listed above may include asset management, business environment, governance, risk assessment, and risk management strategy, among others. The outcomes of these activities will be tied to programmatic needs and relevant actions.

5.1.1.1 CYBER RESILIENCE REVIEW (CRR)

The Cyber Resilience Review (CRR) is a no-cost, voluntary, non-technical 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, 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. For additional information, see http://us-cert.gov/ccubedvp/self-service-crr.

5.1.1.2 CYBERSECURITY EVALUATION TOOL (CSET) AND ON-SITE CYBERSECURITY CONSULTING

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. More information is available at: http://ics-cert.us-cert.gov/assessments.

5.1.1.3 INDUSTRIAL CONTROL SYSTEMS COMPUTER EMERGENCY READINESS TEAM (ICS-CERT) RECOMMENDED PRACTICES

The Industrial Control Systems Computer Emergency Readiness Team (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. Access to recommended practices is available at: http://ics-cert.us-cert.gov/introduction-recommended-practices.

5.1.1.4 NATIONAL CYBER AWARENESS SYSTEM (NCAS)

The National Cybersecurity and Communications Integration Center (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 year in review to alert partners of emerging cyber threats, vulnerabilities, and current activities. Certain products such as alerts, current activity updates, bulletins, and

tips are released through the U.S. Computer Emergency Readiness Team (US-CERT) NCAS. More information on obtaining NCAS products is available at:

- http://us-cert.gov/ncas
- http://us-cert.gov/mailing-lists-and-feeds
- http://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new

5.1.1.5 U.S. COMPUTER EMERGENCY READINESS TEAM (US-CERT) AND ICS-CERT ALERTS, BULLETINS, TIPS, AND TECHNICAL DOCUMENTS

Alerts, bulletins, tips, and technical documents are published by ICS-CERT and US-CERT. 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. More information is available at: http://ics-cert.us-cert.gov and http://us-cert.gov.

5.1.1.6 CYBER SECURITY ADVISORS (CSAS)

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 more information about CSAs, email cyberadvisor@hq.dhs.gov (link sends e-mail).

5.1.1.7 PROTECTIVE SECURITY ADVISORS (PSAS)

Protective Security Advisors (PSAs) are trained subject matter experts in critical infrastructure protection and vulnerability mitigation. Regional directors are supervisory PSAs, responsible for the activities of eight or more PSAs and geospatial analysts, who ensure that all Office of Infrastructure Protection critical infrastructure protection programs and services are delivered to federal and SLTT stakeholders and private-sector owners and operators. The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing. For more information about PSAs, see: http://dhs.gov/protective-security-advisors.

5.1.1.8 FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA) EMERGENCY PLANNING EXERCISES

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 man-made disaster, and evaluate their ability to cooperate and work together, as well as test their readiness to respond. To access the exercises, see: http://www.fema.gov/emergency-planning-exercises.

5.1.2 RESOURCES TO PROTECT AGAINST THREATS

Protecting against threats involves 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.

5.1.2.1 ICS-CERT TRAINING

ICS-CERT offers training in industrial control systems security at the overview, intermediate, and advanced levels, including web-based and instructor-led formats. More information on ICS-CERT training opportunities is available at: http://ics-cert.us-cert.gov/training-available-through-ics-cert.

5.1.2.2 ICS-CERT RECOMMENDED PRACTICES

ICS-CERT maintains 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 the end user community 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. Access to recommended practices is provided through: http://ics-cert.us-cert.gov/introduction-recommended-practices.

5.1.2.3 NATIONAL CYBER AWARENESS SYSTEM (NCAS)

The National Cybersecurity and Communications Integration Center (NCCIC) produces advisories, alert & situation reports, analysis report, current activity updates, daily summaries, indicator bulletins, periodic newsletters, recommended practices, Weekly Analytic Synopsis Product (WASP), weekly digests, and year in review to alert partners of emerging cyber threats, vulnerabilities, and current activities. Certain products such as alerts, current activity, bulletins, and tips are released through US-CERT's NCAS. More information on obtaining NCAS products is available at:

- http://us-cert.gov/ncas
- http://us-cert.gov/mailing-lists-and-feeds/
- http://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new

5.1.2.4 US-CERT AND ICS-CERT ALERTS, BULLETINS, TIPS, AND TECHNICAL DOCUMENTS

Access to alerts, bulletins, tips, and technical documents published by ICS-CERT and US-CERT. ICS-CERT also offers an extensive bibliography of relevant standards and references. Both sets of documents and references provide a better understanding of relevant control systems vulnerabilities and suggest measures critical infrastructure owners and operators can take to address them. More information on ICS-CERT and US-CERT alerts, bulletins, tips, and technical documents is available at: http://ics-cert.us-cert.gov and http://us-cert.gov.

5.1.2.5 CYBER SECURITY ADVISORS (CSAS)

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 the Nation's critical infrastructure and SLTT governments. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. CSAs 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 U.S. and its territories. For more information about CSAs, please email: cyberadvisor@hq.dhs.gov.

5.1.2.6 PROTECTIVE SECURITY ADVISORS (PSAS)

PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts. Regional Directors are Supervisory PSAs, responsible for the activities of eight or more PSAs and geospatial analysts, who ensure all Office of Infrastructure Protection critical infrastructure protection programs and services are delivered to Federal and SLTT stakeholders and private sector owners and operators. The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing. For more information about PSAs, visit: http://dhs.gov/protective-security-advisors.

5.1.2.7 CYBER INFORMATION SHARING AND COLLABORATION PROGRAM (CISCP)

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. For more information about CISCP, email ciscp_coordination@hq.dhs.gov (link sends e-mail) and download an overview of CISCP.

5.1.2.8 ENHANCED CYBERSECURITY SERVICES (ECS)

Enhanced Cybersecurity Services (ECS) is a voluntary information sharing program that assists U.S.-based public and private entities as they improve the protection of their 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. It develops cyber threat indicators based on this information and shares them with qualified commercial service providers, thus enabling them to better protect their customers. ECS augments, but does not replace, entities' existing cybersecurity capabilities. More information is available at: http://dhs.gov/enhanced-cybersecurity-services.

5.1.2.9 STOP.THINK.CONNECT. CAMPAIGN

Launched in 2010, the Stop.Think.Connect. 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 coalition of private companies, non-profits, and government organizations, including DHS, through the Anti-Phishing Working Group Messaging Convention and the National Cyber Security Alliance (NCSA).

For more information on how to get involved, see: http://dhs.gov/stopthinkconnect or email stopthinkconnect@dhs.gov (link sends e-mail).

5.1.2.10 NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

Various cybersecurity education and awareness initiatives fall under the umbrella of the National Initiative for Cybersecurity Education (NICE). It includes the National Initiative for Cybersecurity Careers and Studies (NICCS) portal, which provides a variety of resources for awareness, training, education, and career development for cybersecurity professionals and the general public. More information is available at: http://niccs.us-cert.gov/education/education-home.

5.1.2.11 NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (NICCS) PORTAL

The 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. More information is available at: http://niccs.us-cert.gov.

5.1.2.12 CYBERSECURITY WORKFORCE PLANNING DIAGNOSTIC TOOL

The Cybersecurity Workforce Planning Diagnostic tool, which was developed by NICE, introduces a qualitative management aid to help organizations identify the data they need to gather for effective cybersecurity workforce planning. By considering implications of specific organizational characteristics around two factors—risk exposure (as a function of mission cybersecurity dependence aligned to compliance standards) and risk tolerance—organizations will gain

insight into what types of data they need to better plan for and manage their cybersecurity workforce. To learn more, see: http://niccs.us-cert.gov/careers/cybersecurity-workforce-planning-diagnostic.

5.1.2.13 NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

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. To learn more about the framework, see: http://niccs.us-cert.gov/training/tc/framework/overview.

5.1.2.14 CYBERSECURITY SERVICE OFFERING REFERENCE AIDS

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. Access the reference aids at: Cybersecurity Service Offering Reference Aids.

5.1.2.15 FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA) EMERGENCY PLANNING EXERCISES

The 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 an organization test a hypothetical situation, such as a natural or man-made disaster, and evaluate the groups' ability to cooperate and work together, as well as test their readiness to respond. To access the exercises, visit: http://www.fema.gov/emergency-planning-exercises.

5.1.3 RESOURCES TO DETECT THREATS

Detecting threats involves timely discovery of cybersecurity events. Examples of outcome categories within this function include anomalies and events, security continuous monitoring, and detection processes.

5.1.3.1 CYBER INFORMATION SHARING AND COLLABORATION PROGRAM (CISCP)

A no-cost information sharing partnership between enterprises and DHS, CISCP 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. For more information about CISCP, please email ciscp_coordination@hq.dhs.gov (link sends e-mail) and download an overview of CISCP.

5.1.3.2 ENHANCED CYBERSECURITY SERVICES (ECS)

ECS is a voluntary information sharing program that assists U.S.-based public and private entities as they improve the protection of their 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 cyber threat indicators 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. More information is available at: http://dhs.gov/enhanced-cybersecurity-services.

5.1.3.3 FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA) EMERGENCY PLANNING EXERCISES

The 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 an organization test a hypothetical situation, such as a natural or man-made disaster, and evaluate the groups' ability to cooperate and work together, as well as test their readiness to respond. To access the exercises, visit: http://www.fema.gov/emergency-planning-exercises.

5.1.4 RESOURCES TO RESPOND TO THREATS

Responding to threats involves containing the impact of a potential cybersecurity event. Examples of outcome categories within this function include response planning, communications, analysis, mitigation, and improvements.

5.1.4.1 CYBER INFORMATION SHARING AND COLLABORATION PROGRAM (CISCP)

A no-cost information sharing partnership between enterprises and DHS, CISCP 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. For more

information about CISCP, please email ciscp_coordination@hq.dhs.gov (link sends e-mail) and download an overview of CISCP.

5.1.4.2 CYBER SECURITY ADVISORS (CSAS)

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 the Nation's critical infrastructure and SLTT governments. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. CSAs 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 U.S. and its territories. For more information about CSAs, please email cyberadvisor@hq.dhs.gov (link sends e-mail).

5.1.4.3 PROTECTIVE SECURITY ADVISORS (PSAS)

PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts. Regional Directors are Supervisory PSAs, responsible for the activities of eight or more PSAs and geospatial analysts, who ensure all Office of Infrastructure Protection critical infrastructure protection programs and services are delivered to Federal and SLTT stakeholders and private sector owners and operators. The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing. For more information about PSAs, visit: http://dhs.gov/protective-security-advisors.

5.1.4.4 ENHANCED CYBERSECURITY SERVICES (ECS)

ECS is a voluntary information sharing program that assists U.S.-based public and private entities as they improve the protection of their 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 cyber threat indicators 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. More information is available at: http://dhs.gov/enhanced-cybersecurity-services.

5.1.4.5 CYBER INCIDENT RESPONSE AND ANALYSIS

ICS-CERT 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 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, email: ics-cert@hq.dhs.gov.

5.1.4.6 FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA) EMERGENCY PLANNING EXERCISES

The 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 an organization test a hypothetical situation, such as a natural or man-made disaster, and evaluate the groups' ability to cooperate and work together, as well as test their readiness to respond. To access the exercises, visit: http://www.fema.gov/emergency-planning-exercises.

5.1.5 RESOURCES TO RECOVER FROM THREATS

Recovering from threats involves timely return to normal operations to reduce the impact from a cybersecurity event. Examples of outcome categories within this function include recovery planning, improvements, and communications.

5.1.5.1 FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA) EMERGENCY PLANNING EXERCISES

The 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 an organization test a hypothetical situation, such as a natural or man-made disaster, and evaluate the groups' ability to cooperate and work together, as well as test their readiness to respond. To access the exercises, visit: http://www.fema.gov/emergency-planning-exercises.

5.1.6 CONTACT INFORMATION

To contact the Critical Infrastructure Cyber Community (C³) Voluntary Program, email ccubedvp@hq.dhs.gov. To stay informed of upcoming events, new resources, publications, and other announcements, subscribe to program alerts at https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new and see https://www.us-cert.gov/ccubedvp.

5.2 FEDERAL BUREAU OF INVESTIGATION (FBI)

5.2.1 INFRAGARD

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and the private sector. It is an association of persons 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 utilizing 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.

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 our 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.

For more information see InfraGard's public website or contact your local FBI field office.

5.2.1.1 INTERNET CRIME COMPLAINT CENTER (IC3)

The Internet Crime Complaint Center 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. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

Since 2000, the 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

as the 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.

For more information, see:

- http://www.ic3.gov
- http://www.fbi.gov
- http://www.ic3.gov/media/IC3-Brochure.pdf

5.2.1.2 THE DOMESTIC SECURITY ALLIANCE COUNCIL (DSAC)

Modeled on the U.S. Department of State's Overseas Security Advisory Council—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 FBI and participating members, which include some of America's most respected companies. It also gives the Bureau valuable contacts when we need assistance with our investigations. Learn more

5.2.1.3 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—"fuse" intelligence from participating agencies to create a more comprehensive threat picture, locally and nationally. 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. Learn more

5.2.1.4 AFFILIATED INFORMATION SHARING ASSOCIATIONS

- ACTRA—Arizona Cyber
- VCSP—Virginia Cyber Security Partnership

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. Click here to learn more.

NIST National Institute of Standards and Technology

5.3 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

5.3.1 EXECUTIVE ORDER 13636: CYBERSECURITY FRAMEWORK

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. 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.

5.3.2 FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Created through collaboration between industry and government, the Framework for Improving Critical Infrastructure Cybersecurity 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.

The framework core and informative requirements are available as separate downloads in three formats:

- Spreadsheet (Excel)
- Alternate view (PDF)
- Database (FileMaker Pro).

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.

5.3.3 NIST INTERAGENCY REPORT (IR) 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 less secure small businesses. This Interagency Report (IR) helps small business managers understand how to provide basic security for their information, systems, and networks.

The report is available at: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.

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

The selection of IT 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 (IT) 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.

The guide is available at: http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf.

5.4 FEDERAL COMMUNICATIONS COMMISSION (FCC)

5.4.1 SMALL BUSINESS CYBERPLANNER 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 re-launched the Small Biz Cyber Planner 2.0, an online resource to help small businesses create customized cybersecurity plans. Use this tool to create and save a custom cyber security plan for your company, choosing from a menu of expert advice to address your specific business needs and concerns.

In addition to the Small Biz Cyber Planner 2.0 (above), the FCC publishes the Cybersecurity Tip Sheet, a quick resource featuring tips on creating a mobile device action plan and on payment and credit card security. For more information and to access this resource, see: http://www.fcc.gov/cyberforsmallbiz.

5.4.2 CYBERSECURITY PLANNING GUIDE

The Cybersecurity Planning Guide is designed to meet the specific needs of your 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. Businesses using more sophisticated networks with dozens of computers should consult a cyber security expert in addition to using the cyber planner. For more information and to access this resource, see: https://transition.fcc.gov/cyber/cyberplanner.pdf.

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 cyberattack.

5.5 NATIONAL SECURITY AGENCY (NSA)

5.5.1 NATIONAL SECURITY CYBER ASSISTANCE PROGRAM

The National Security Agency (NSA)/Information Assurance Directorate (IAD) has established a National Security Cyber Assistance Program 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 accreditation is issued only to organizations that meet the criteria set forth in the NSA/IAD Accreditation Instruction Manual.

For more information, see the program webpage at:
https://www.nsa.gov/ia/programs/cyber_assistance_program/index.shtml.

Download best practices for keeping a home network secure at:
http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf.

5.6 DEPARTMENT OF JUSTICE

5.6.1 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.

The document is available at: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

5.7 OTHER SOURCES

The resources below are available from other sources.

5.7.1 RESOURCES TO IDENTIFY THREATS

5.7.1.1 NATIONAL ASSOCIATION OF CORPORATE DIRECTORS (NACD) CYBER-RISK OVERSIGHT HANDBOOK

Assessing cyber threats in terms of a risk-reward tradeoff is especially challenging for two reasons: the complexity of cyber threats has grown dramatically, and competitive pressures to deploy increasingly cost-effective business technologies often affect resource investment calculations. These two competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the board level is essential.

The National Association of Corporate Directors (NACD), in conjunction with the financial services and insurance provider American International Group (AIG) and the Internet Security Alliance, has identified five steps all corporate boards should consider as they seek to enhance their oversight of cyber risks. The NACD Cyber-Risk Oversight Handbook can be found at: http://www.nacdonline.org/cyber.

5.7.1.2 AN INTEL USE CASE FOR THE CYBERSECURITY FRAMEWORK IN ACTION

Intel completed a pilot project to test the use of the NIST Cybersecurity Framework. The results of the test include reusable tools and best practices; harmonized risk management methods, technologies, and language across the corporation and its supply chain; informed discussions about risk tolerance; more focused risk reduction activities; and improved visibility of the risk landscape. The use case can be found at: http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html (link is external).

5.7.1.3 CYBERCHAIN PORTAL-BASED ASSESSMENT TOOL

The CyberChain portal, managed by the University of Maryland Robert H. Smith School of Business Supply Chain Management Center, provides risk assessment tools, scenario-based mapping tools, anonymous information sharing, and

assessments to calculate factors such vulnerability and risk maturity capability. Tools also enable diagnosis of IT supply chain trouble spots and areas for improvement based on NIST guidelines. Learn more at: https://cyberchain.rhsmith.umd.edu/(link is external).

5.7.1.4 CLOUD CONTROLS MATRIX

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The matrix offers a controls framework that explains security concepts and principles aligned to tools such as the NIST Cybersecurity Framework. It strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud. Learn more at: https://cloudsecurityalliance.org/research/ccm/.

5.7.2 RESOURCES TO PROTECT AGAINST THREATS

5.7.2.1 NATIONAL ASSOCIATION OF CORPORATE DIRECTORS (NACD) CYBER-RISK OVERSIGHT HANDBOOK

Assessing cyber threats from a risk-reward tradeoff perspective is especially challenging in the cyber arena for two reasons: (1) the complexity of cyber threats has grown dramatically, and (2) competitive pressures to deploy increasingly cost-effective business technologies often affect resource investment calculations. These two competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the board level is essential. NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps all corporate boards should consider as they seek to enhance their oversight of cyber risks; the NACD Cyber-Risk Oversight Handbook can be found here: http://www.nacdonline.org/cyber.

5.7.2.2 IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK AND SUPPLEMENTARY TOOLKIT

ISACA (formerly known as the Information Systems Audit and Control Association) participated in the development of the NIST Cybersecurity Framework and helped embed key principles from the Control Objectives for Information and Related Technology (COBIT) framework into the industry-led effort. As part of the knowledge, tools and guidance provided by Cybersecurity Nexus (CSX), ISACA has developed a guide for implementing the framework. Download the guide at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx.

5.7.2.3 PROCESS CONTROL SYSTEM SECURITY GUIDANCE FOR THE WATER SECTOR

The American Water Works Association (AWWA) has developed guidance to provide water utility owners and operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber attacks as recommended in ANSI/AWWA G430: Security Practices for Operations and Management and Executive Order 13636. The AWWA guidance and tool represent a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council. Download the guide at: http://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf.

5.7.2.4 INFORMATION SECURITY FORUM'S IMPLEMENTING NIST FRAMEWORK CYBERSECURITY FRAMEWORK

Members of the Information Security Forum can access a guide to help them use the NIST Cybersecurity Framework. Find out more at: https://www.securityforum.org/research/publicdownloadnistcybersecurity/.

5.7.2.5 CYBERSECURITY 101: A RESOURCE GUIDE FOR BANK EXECUTIVES

The Conference of State Bank Supervisors has published Cybersecurity 101: A Resource Guide for Bank Executives, a non-technical resource on cybersecurity that community bank chief executive officers, senior executives, and board members can use to help mitigate cybersecurity threats at their banks. The guide puts into one place industry-recognized standards and best practices for cybersecurity currently used within the financial services industry. Learn more and download the guide at: http://www.csbs.org/news/press-releases/pr2014/Pages/pr-121714.aspx.

5.7.2.6 SMALL FIRMS CYBERSECURITY GUIDANCE: HOW SMALL FIRMS CAN BETTER PROTECT THEIR BUSINESS

The Securities Industry and Financial Markets Association has developed a Small Firms Cybersecurity Guidance to help small firms to increase their security and ensure the protection of their customers. The guide builds upon the NIST Cybersecurity Framework. Firms can apply the best practices in this guide in a risk-based, threat-informed approach based on the resources available and in support of their firm's overall business model. Learn more and download the guide at: http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/.

5.7.2.7 NIST CYBERSECURITY FRAMEWORK EXPLAINED

IT security provider Rapid7 has developed a video that discusses and gives a brief overview of the NIST Cybersecurity Framework. Watch the video at: http://www.rapid7.com/resources/videos/nist-cybersecurity-framework-explained.jsp (link is external).

5.7.2.8 START WITH SECURITY: A GUIDE FOR BUSINESS

Start with Security: A Guide for Business, from the Federal Trade Commission (FTC), offers 10 practical lessons businesses can learn from the FTC's 50+ data security settlements. Lessons include suggestions like "Start with 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. To download the guide or order free copies, see: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

5.7.3 RESOURCES TO DETECT THREATS

5.7.3.1 NATIONAL ASSOCIATION OF CORPORATE DIRECTORS (NACD) CYBER-RISK OVERSIGHT HANDBOOK

Assessing cyber threats from a risk-reward tradeoff perspective is especially challenging in the cyber arena for two reasons: (1) the complexity of cyber threats has grown dramatically, and (2) competitive pressures to deploy increasingly cost-effective business technologies often affect resource investment calculations. These two competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the board level is essential. NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps all corporate boards should consider as they seek to enhance their oversight of cyber risks; the NACD Cyber-Risk Oversight Handbook can be found here: http://www.nacdonline.org/cyber.

5.7.4 RESOURCES TO RESPOND

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.