Government Programs and Services Available to Assist ISAOs

Draft Document—Request for Comment

SWG G 6—2016 v0.2

ISAO Standards Organization
Standards Working Group 6: Government Relations
Mike Echols, Chair
David Weinstein, Vice-Chair

May 2, 2016

Table of Contents

Revision Updates

Item	Version	Description	Date
1	0.1	Initial document: Products and Services	April 5, 2016
2	0.2	Update: FBI program additions	April 28, 2016

EXECUTIVE SUMMARY

The objective of Standards Working Group 6, Government Relations, is to identify and propose considerations and government resources to ensure that Information Sharing and Analysis Organization (ISAO) voluntary standards align with existing laws, regulations, and guidance. This working group 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 purpose of this voluntary ISAO Standards Organization (SO) guide is to assist ISAOs, both new and existing, in identifying existing resources and services, primarily those provided by the government, that may be of use to their organization. Much of this guide is aligned to the five cybersecurity framework function areas. As such, it outlines resources and services available to help ISAOs identify, protect from, detect, respond to, and recover from cyber threats and incidents.

This is the first complete draft of this voluntary guide. This draft is intended to be a starting point and will be updated continuously through public input and working group research.

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. [NOTE: The Resource Library functionality is in development.]

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.

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.

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.

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.

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.

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

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.

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).

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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.

FEDERAL BUREAU OF INVESTIGATION (FBI)

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.

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

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

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

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. Learn more

NIST National Institute of Standards and Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

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.

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.

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.

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.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

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.

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.

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.

NATIONAL SECURITY AGENCY (NSA)

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.

DEPARTMENT OF JUSTICE

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

OTHER SOURCES

The resources below are available from other sources.

RESOURCES TO IDENTIFY THREATS

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.

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).

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).

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/.

RESOURCES TO PROTECT AGAINST THREATS

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.

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.

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.

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/.

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.

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/.

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).

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.

RESOURCES TO DETECT THREATS

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.

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.