HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

May 2017

RESOURCE CATALOG

Resource Catalog

Pursuant to the task identified in the Act, this document summarizes a number of the key resources available to the sector. The Task Force made every effort to be comprehensive, while identifying resources that are easily accessible and publically available.

1. Where Should I Start?

HHS Resources

HealthIT.gov Cybersecurity: HHS ONC has developed resources for health care cybersecurity and risk management. The HealthIT.gov Cybersecurity website points to these resources, including the Top Ten Tips and cybersecurity training games.

HealthIT Cybersecurity Shared Responsibility

HHS Office of the Assistant Secretary for Preparedness and Response (ASPR): ASPR's Technical Resources, Assistance Center, and Information Exchange (TRACIE) was created to meet the information and technical assistance needs of regional ASPR staff, health care coalitions, health care entities, health care providers, emergency managers, public health practitioners, and others working in disaster medicine, health care system preparedness, and public health emergency preparedness.

The resources in the Cybersecurity Topic Collection can help stakeholders better protect against, mitigate, respond to, and recover from cyber threats, to ensure patient safety and operational continuity.

ASPR TRACIE Cybersecurity

DHS Resources

Cybersecurity Overview: Strengthening the security and resilience of cyberspace is an important part of DHS's mission. This website points to the many resources and programs DHS makes available.

DHS Cybersecurity Overview

Stop. Think. Connect: DHS's "Stop. Think. Connect." Campaign is aimed at increasing the understanding of cyber threats and empowering the public to be more secure online. The toolkit provides resources for all segments of the public.

DHS StopThinkConnect

NIST Resources

NIST develops cybersecurity standards and best practices that address interoperability, usability, and privacy. The NIST Cybersecurity website provides an overview of their programs (including the National Cybersecurity Center of Excellence and the Cybersecurity Framework) and pointers to specific cybersecurity topics.

NIST Cybersecurity

2. Who Should I Turn To?

Healthcare and Public Health (HPH) Sector Critical Infrastructure Protection Partnership: HHS/ASPR's Critical Infrastructure Protection Program leads a public and private sector partnership to protect the HPH Sector from all hazards, including cyber threats. Health care industry organizations can join the partnership's HPH Sector Coordinating Council (HSCC). The HSCC is an independent, industry-led group that works closely with HHS and other governmental partners to address cybersecurity and other critical infrastructure issues through a collaborative partnership approach.

HHS ASPR Critical Infrastructure Protection

HITRUST*:* The HITRUST Alliance is a not for profit organization that collaborates with public and private sector leaders from health care technology, privacy, and information security organizations. HITRUST's focus is to promote the protection of health information and manage the risk to that information. HITRUST provides a range of frameworks, related assessment and assurance methodologies, and programs that support cyber sharing, analysis, and resilience.

HITRUST

National Health – Information Sharing and Analysis Center (NH-ISAC)

NH-ISAC: The NH-ISAC is the official ISAC for the HPH sector. It is a membership organization that enables sharing cybersecurity threat information, best practices, and mitigations across the sector.

NH ISAC

InfraGard: InfraGard is a partnership between the FBI and the private sector dedicated to sharing information and intelligence to counter threats.

InfraGard

DHS

U.S. Computer Emergency Readiness Team (US-CERT): The US-CERT develops actionable information to the public and private sectors. The National Cyber Awareness System publishes alerts about current cybersecurity issues, weekly vulnerability bulletins, advice and best practices, and in-depth technical articles.

US CERT

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): The ICS-CERT coordinates among federal, state, local, and tribal governments and the private sector about cybersecurity vulnerabilities, incidents, and mitigations related to industrial control systems, include medical devices.

ICS CERT

Information Sharing Programs: This is the landing page for DHS' various programs for sharing cybersecurity information with private industry, including Automated Indicator Sharing, Cyber Information Sharing and Collaboration Program, Enhanced Cybersecurity Services, ISAOs, and the National Cybersecurity and Communications Integration Center.

DHS NCCIC

3. Detailed Cybersecurity Guidance for HPH Stakeholders

For Health Care Providers – EHRs

HIPAA Security Rule: OCR provides a summary of the HIPAA Security Rule.

HIPAA Security Rule

ONC Security and Privacy Guide: ONC, in coordination with OCR, created a guide to privacy and security of electronic health information, along with a Security Risk Assessment Tool.

ONC Security and Privacy Guide

OCR Security Rule: OCR created a collection of resources on the HIPAA Security Rule, including guidance for implementing the security standards, risk analysis, pointers to key NIST documents, and OCR Awareness Newsletters on vulnerabilities and threats.

OCR Security Rule

National Cybersecurity Center of Excellence (NCCoE): One of the NCCoE health IT projects is related to EHRs on mobile devices.

NCCoE EHRs on Mobile Devices

For Health Care Providers – Devices

NCCoE: One of the NCCoE health IT projects is related to wireless infusion pumps.

NIST NCCoE Wireless Infusion Pumps

Veterans Affairs: Veterans Affairs Directive 6550 establishes the technical assessment requirements for pre-procurement of medical devices/systems, including those that are connected to Veterans Affairs systems or contain patient sensitive information. The appendix is a questionnaire that health care providers can use to evaluate the configuration and security profile of medical devices during acquisition planning to identify potential risks and integrate devices into hospital operations. The 6550 questionnaire extends the Manufacturer Disclosure Statement for Medical Device Security, which was developed by HIMSS and the American College of Clinical Engineering, and then standardized through a joint effort between HIMSS and the National Electrical Manufacturers Association.

VA Directive 6550

For Medical Device Manufacturers

FDA Cybersecurity: FDA's Cybersecurity web page summarizes FDA's activities related to medical device cybersecurity, including issuing premarket and postmarket guidance, issuing Safety Communications for vulnerabilities discovered in devices, convening public workshops, and entering into a Memorandum of Understanding with the NH-ISAC and the Medical Device Innovation, Safety and Security Consortium.

FDA Cybersecurity

FDA Consensus Standards: FDA recognizes several consensus standards related to medical device security. Quick search for "security" in the database.

FDA Consensus Standards

Coordinated Vulnerability Disclosure: An important element of FDA's postmarket guidance is developing coordinated disclosure policies for medical device vulnerabilities. ISO/IEC 29147 - Information technology - Security techniques - Vulnerabilities provides guidelines for vendors to include in their business processes when receiving information about potential vulnerabilities and distributing vulnerability resolution information.

ISO Coordinated Vulnerability Disclosure Standards

For all stakeholders – Configurations and Best Practices

IAD Guidance: Information assurance at the National Security Agency provides security solution guidance based upon their unique and deep understanding of risks, vulnerabilities, mitigations, and threats. This information can be utilized to harden and defend network and system infrastructure, while providing for a sustained presence. This guidance covers a broad range of topics including secure architectures, configuration guidance for networks and industrial control systems, and security tips.

IAD Guidance

NIST NCCoE: The NIST NCCoE accelerates the private sector's adoption of advanced, standards-based security technologies by developing use cases, working with vendors to develop solutions in NCCoE's labs, and publish practice guides (in NIST Special Publication 1800 series).

NIST NCCoE

NIST Special Publications: The NIST Special Publications 800 series provides computer/cyber/information security guidelines, recommendations, and reference materials. Special Publication 800-53 provides a catalog of security and privacy controls for use in federal information systems, which many private enterprises find useful for establishing their security controls. There are a wide range of guides to help securely implement various technologies (e.g., servers, mobile devices, cloud computing, encryption, and wireless protocols).

The NIST Special Publication 1800 series consists of practical guides that provide standards based approaches to cybersecurity challenges in the public and private sectors.

NIST Special Publications

NIST National Checklist Program: The National Checklist Program is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low-level guidance on setting the security configuration of operating systems and applications.

NIST National Checklist Program

Defense Information Systems Agency (DISA) publishes the Security Technical Implementation Guides (STIGs): DISA publishes the STIGs, which provide configuration guidance for information assurance enabled Department of Defense systems. Even though these STIGS provide configurations for Department of Defense systems, manufacturers and health care providers can adopt configurations for their systems (medical devices and health IT systems) and networks.

Some relevant STIGS are Application Security and Development STIG, Multifunction Device and Network Printers STIG, and Network Device Management STIG.

DISA Security Technical Implementation Guides

For all stakeholders – Cybersecurity Risk Management

NIST Risk Management Framework: The NIST Risk Management Framework provides an effective framework for selecting the appropriate security controls for a system—the security controls necessary to protect individuals and the operations and assets of the organization—by managing organizational risk. The Risk Management Framework provides a process that integrates security and risk management activities into the system development lifecycle. The risk management concepts are intentionally broad-based with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by the supporting NIST security standards and guidelines.

NIST Cybersecurity Risk Management Framework

NIST Cybersecurity Framework: The NIST Cybersecurity Framework website contains the latest version of the Framework, a reference tool (a database implementing the framework core), and industry resources.

NIST Cybersecurity Framework

Baldrige Cybersecurity Excellence Builder: NIST's Baldrige Cybersecurity Excellence Builder is a voluntary self-assessment tool that enables organizations to better understand the effectiveness of their cybersecurity risk management efforts. It blends the systems perspective and business practices of the Baldrige Excellence Framework with the concepts of the NIST Cybersecurity Framework.

Baldrige Cybersecurity Excellence Builder

DHS Critical Infrastructure Cyber Community C^3 Voluntary Program (C3VP): The C3VP aims to support industry efforts to increase cyber resilience, awareness and use of the NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity and encourage organizations to manage cybersecurity as part of an all-hazard approach to enterprise risk management.

The C3VP website contains information about the Cybersecurity Framework, including sector-specific guidance, and resources for business organized by the framework. In addition, the Assessments section of the C3VP website contains information on the Cyber Resiliency Review program, a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices, which can be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.

DHS C3VP

For all stakeholders – Small Business

DHS C3VP: DHS C3VP has resources to help small and medium businesses address their cybersecurity risks, given the scope and complexity of the issue in the face of a small staff and limited resources.

DHS C3VP Small Business

NIST Small Business Corner: NIST's Small Business Corner website has cybersecurity resources for small businesses. NIST, the FBI, and the Small Business Administration conduct workshops on cybersecurity threats and solutions. The Small Business Corner Library contains workshop materials and a link to NIST Internal/Interagency Report 7621 r1: *Small Business Information Security: The Fundamentals*.

NIST Small Business Corner

4. Education, Training, Workforce Development

DHS National Initiative for Cybersecurity Careers and Studies (NICCS): DHS's NICCS provides a collection of resources on cybersecurity education, including a catalogue of courses, information about the National Centers of Academic Excellence program managed by National Security Agency, K-12 resources, and industry resources.

DHS NICCS

NIST National Initiative for Cybersecurity Education (NICE): NIST's NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The website contains resources for workforce development (including the NICE Cybersecurity Workforce Framework documented in NIST draft Special Publication 800-181, which provides a taxonomy for classifying cybersecurity roles), educational activities and programs, and other materials and resources that support cybersecurity training.

NIST NICE

CAE-CD: The CAE-CD program is jointly sponsored by NSA and DHS. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation. All regionally accredited two-year, four-year, and graduate level institutions in the U.S. are eligible to apply to be designated as a two-year, four-year, or research CAE-CD. Prospective schools are designated after meeting stringent CAE criteria and mapping curricula to a core set of cyber defense knowledge units or specialized focus areas. The CAE-CD website has a list of the current academic centers of excellence, as well as the curriculum requirements and additional resources to help map curricula.

NSA and DHS CAE-CD

DHS Cyber Storm Exercises: DHS conducts the Cyber Storm exercises every two-years to strengthen cyber preparedness in the public and private sectors. The exercises follow the training theory of “train like you fight, fight like you train”, allowing participants to exercise decision-making, coordination, collection, response and recovery to validate actual readiness. Cyber Storm V, in part, focused on the HPH Sector.

DHS Cyber Storm Cyber Storm: Securing Cyber Space