Medical Device Cybersecurity

Regional Incident Preparedness and Response Playbook

Version 1.0

October 2018

MITRE

Sponsor: FDA

Dept. No.: T8A5

Contract No.: HHSM-500-2012-00008I

Project No.: 37177042

Medical Device Cybersecurity

Regional Incident Preparedness and Response Playbook

Table of Contents

List of Figures

List of Tables

1. Background

Cybersecurity attacks on Healthcare and Public Health (HPH) critical infrastructure, such as healthcare delivery organizations (HDOs), are occurring with greater frequency. Disruptions in clinical care operations can put patients at risk. The global ransomware event known as WannaCry demonstrated how the performance of vulnerable medical devices may be compromised by an exploit, whether it intentionally targets the healthcare system or is purely opportunistic. Similarly, other attacks such as Petya/NotPetya have highlighted key challenges in preparedness and response across the HPH critical infrastructure sector. Securing critical infrastucture is a shared responsibility across many stakeholders, and with respect to medical devices the primary stakeholders are FDA, Medical Device Manufacturers (MDMs), and HDOs.

A common preparedness and response challenge FDA heard from its stakeholders in the aftermath of the aforementioned attacks is that HDOs did not know with whom to communicate (e.g. MDM–HDO interactions); what actions they might consider taking; and what resources were available to aid in their response. Without timely, accurate information and incorporation of medical device cybersecurity into their organizational emergency response plans, it was difficult for HDOs to assess and mitigate the impact of these attacks on their medical devices. To address this unmet need, the MITRE team (with the support of FDA), engaged with a broad distribution of stakeholder groups to understand the gaps, challenges, and resources for HDOs participating in medical device cybersecurity preparedness and response activities. These stakeholders included HDOs of varying size and demographics, state departments of health, medical device manufacturers, and government agencies. Information gathered resulted in the creation of this playbook that may serve as a resource for HDOs. The playbook provides a stakeholder–derived, open source, and customizable framework that HDOs may choose to leverage as a part of their emergency response plans in order to ultimately limit disruptions in continuity of clinical care as well as the potential for direct patient harm stemming from medical device cyber security incidents.

2. Playbook Audience

HDOs, particularly staff involved in medical device cybersecurity incident preparedness and response, are the primary audience for this regional playbook (hereinafter referred to as *playbook*). Staff involved in an integrated preparedness and response team may include but are not limited to clinicians, healthcare technology management (HTM) professionals, and information technology (IT), emergency response, risk management and facilities staff. Other stakeholders may also find the playbook useful, including device manufacturers and other external entities that support HDOs' response efforts, such as maintenance contractors and health system, regional, and national response partners.

3. Scope

The playbook covers preparedness and response for medical device cybersecurity issues that impact the functionality of a device. Of particular focus are threats or vulnerabilities that have the potential for large–scale, multi–patient impact and raise patient safety concerns; the playbook is not intended to aid in the day–to–day patch management of devices.

The playbook presents target capabilities for medical device cybersecurity incident preparedness and response; many HDOs will not be able to fully execute all recommendations due to operational constraints. The playbook is also intended to be used within the context of a "region" and may be a starting point for HDOs without a medical device cybersecurity response plan that can be incorporated into existing response plans. The HDO's environment will dictate what a region means. For a large HDO/health system

with campuses spread across multiple states, those campuses may comprise its region. For HDOs that look to partner with other HDOs at state or county levels, those partnerships may comprise their region. The term *region* is not necessarily constrained by a geographical boundary, but rather is driven by the incident response (IR) organizational structure that best fits the needs of the participating HDOs.

4. Purpose and Objective

Regions are beginning to organize cybersecurity incident preparedness activities. While similarities exist with natural disaster emergency preparedness and response, cybersecurity has unique characteristics that warrant specific integration of cybersecurity incident planning within an HDO's emergency plans and across stakeholders. The purpose of the playbook is to serve as a tool for regional readiness and response activities to aid HDOs in addressing cybersecurity threats affecting medical devices that could impact continuity of clinical operations for patient care and patient safety. The objectives of the framework are to:

- Provide baseline medical device cybersecurity information that can be incorporated into an HDO's emergency preparedness and response framework;
- Outline roles and responsibilities for responders internal and external to the HDO to clarify lines of communication and concept of operations (CONOPs) across HDOs, medical device manufacturers (MDMs), state and local governments, and the federal government;
- Describe a standardized approach to response efforts that would enable a unified response within HDOs and across regions as appropriate;
- Serve as a basis for enhanced coordination activities among medical device cybersecurity stakeholders, including mutual aid across HDOs;
- Inform decision making and the need to escalate response;
- Identify resources HDOs may leverage as a part of preparedness and response activities; and
- Serve as a customizable regional preparedness and response tool for medical device cyber resiliency that could be broadly implemented.

5. Regional Medical Device Cybersecurity Incident Preparedness and Response

HDO incident preparedness and response for medical device cybersecurity can be strengthened through regional outreach and collaboration. Cybersecurity is a "team sport,"[1] and pooling limited resources and expertise across a region before, during, and after a medical device cybersecurity incident will help ensure that patient safety is maintained.

A region, which may be geographic (e.g., state, tri-state area, portion of a state) and/or organizational (e.g., HDOs in the same hospital system), should be a source of trusted partners to facilitate preparedness and response sharing. An HDO may belong to one or more regions. Examples of regional partners include the following:

- State/local Department of Health,
- State/local Department of Safety/Emergency Response,
- State/regional Cybersecurity Communications Integration Center (CCIC),

1 Chertoff, Michael, former Homeland Security secretary, https://www.csoonline.com/article/2844133/data-protection/chertoff-cybersecurity-takes-teamwork.html

- Regional Health Care Coalition,[2]
- Regional hospital trade association(s),
- Regional fusion center,
- Local InfraGard chapter,
- Regional and/or sector–specific Information Sharing and Analysis Organizations (ISAOs)/ Information Sharing and Analysis Centers (ISACs),
- Regional testing laboratories, and
- Geographically and/or organizationally aligned peer hospitals.

Additional information about these regional partners can be found in Appendix A, Stakeholders. Regional partners can be helpful in both medical device cybersecurity incident preparedness and response, as described in the sections that follow.

5.1 Regional Preparedness

Building trust relationships with regional partners is the first step in medical device cybersecurity preparedness. Larger HDOs may have existing relationships across the community through participation in different consortia; consideration should be given to fostering these relationships and exploring partnerships that offer key and/or complementary resources. Smaller, less resourced HDOs, which may benefit more from the deeper bench that regional collaborations offer, may consider building or augmenting regional relationships, such as through participation in HCC meetings.

Regional opportunities for preparedness collaboration may include the following:

- Sharing medical device cybersecurity best practices, such as policies and plans;
- Developing mutual aid agreements for medical device cybersecurity, or supplements as part of broader incident response mutual aid agreements—to include loaner devices, diverting patients to a facility with operational devices, and incident response assistance;
- Establishing and exchanging point of contact (POC) names and contact information, to include public key infrastructures (PKIs) for more sensitive communications, as applicable;
- Ensuring that all key HDO medical device cybersecurity personnel have access to alerts disseminated via the regional health emergency response communication system, such as the state Health Alert Network (HAN);
- Conducting joint exercises and participating in collaborative clinical simulations;
- Identifying a primary and backup regional incident command/coordination center for use during incidents (e.g., state CCIC, state Emergency Response command center); and
- Sharing cybersecurity advisories and alerts.

5.2 Regional Response

Regional IR draws upon the strength of regional partnerships and may include the following:

- Incident notification: aberrant device behavior, potential incident, discovered vulnerability, etc.;

2 http://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf

- Ad hoc information sharing, such as confirmation of activity ("Are you seeing this?"), feedback on manufacturer responsiveness, pointers to the Healthcare and Public Health (HPH) Sector Critical Infrastructure Protection (CIP) Program sector-wide calls held by HHS/ASPR CIP;[3]
- More formal information sharing, such as indicators of compromise and other relevant actionable incident information (e.g., incident source, mitigation strategies, lessons learned);
- Communications mechanism(s) in use if primary means are compromised;
- Activation/use of regional command center;
- Request for technical assistance;
- Tracking incidents across state/region; and
- Execution of mutual aid agreements (e.g., loaner devices, diverted patients).

HDOs may be hesitant to share information during an incident, due to concerns they will attract negative media attention and/or that doing so may violate nondisclosure agreements (NDAs) with manufacturers. NDAs with regional partners may protect sensitive incident information and facilitate information sharing, perhaps with the Health Information Sharing and Analysis Center (H-ISAC) or other medical device ISAO acting as an initial conduit.

6. HDO Medical Device Cybersecurity Incident Preparedness and Response

Preparing for and responding to incidents involving cybersecurity attacks often require many different parties to interact, both internal and external to the HDO (e.g. medical device manufacturers); various structures and processes may be in place to facilitate these interactions. Cybersecurity attacks are inherently unpredictable 'no notice' events, with insufficient or inaccurate information in the early stages. HDOs cannot predict the timing, severity, and rapid trajectory of a particular cyber attack. An incident may result in organizational confusion and delays that may adversely affect delivery of care.

This section provides tools, references, and resources to help HDOs prepare for and respond to medical device cybersecurity incidents. Its high-level structure follows the incident response life cycle outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61r2, *Computer Security Incident Handling Guide*,[4] shown in Figure 1. This process, and the suggestions provided, are intended to complement existing all-hazards incident preparedness and response activities and can be applied to specific cybersecurity incidents involving medical devices.

3 https://www.phe.gov/Preparedness/planning/cip/Pages/mailinglist.aspx

4 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Figure 1. Incident Response Life Cycle

6.1 Preparedness

During the preparation or preparedness phase, the HDO assesses and bolsters its cyber defensive measures as well as develops incident handling processes and procedures to enable smoother operations when an incident arises. Actions for medical device cybersecurity incident preparedness—consistent with and complementary to broader emergency response procedures described by the Centers for Medicare & Medicaid Services (CMS) Emergency Management Final Rule,[5] National Incident Management System (NIMS),[6] Hospital Incident Command System (HICS),[7] Medical Surge Capacity and Capability, and Assistant Secretary for Preparedness and Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE)[8] Healthcare Coalitions—are described in the subsections that follow.

6.1.1 Medical Device Procurement

Incorporating cybersecurity into medical device procurement can strengthen medical device cybersecurity incident response:

Incident Costs:

- Trying to cover unforeseen costs during an incident is a distraction that slows down incident response. Consider building into the device purchase and/or maintenance fees the cost for mitigating device vulnerabilities. This could include ensuring that spare or extra devices will be available, as needed, during an incident.

Exercise Participation:

- During the procurement process, consider securing a commitment by the manufacturer to participate in HDO cybersecurity exercises, such as the type of exercises described in section 6.1.7.2 below and Appendix B. Inclusion of manufacturers in regional medical device cybersecurity exercises affords HDOs the opportunity to build the HDO–manufacturer relationship, define roles and responsibilities of each

5 https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html

6 https://www.fema.gov/national-incident-management-system

7 http://hicscenter.org/SitePages/HomeNew.aspx

8 https://asprtracie.hhs.gov

party, and better understand the coordination efforts needed during a device incident, such as the need to share:

- Scope, magnitude and impact of the incident on device(s) functionality, clinical care and patient safety initially and as it evolves (HDO);
- Actionable and product-specific information to enable a timely response (manufacturer);
- Tangible patches/fixes to contain and eradicate the attack (manufacturer); and
- Regular status communications (HDO/manufacturer).

- Exercise participation together with HDOs can also aid manufacturers in developing and refining their own internal processes for incident management.

Third-party Component Identification:

- Requesting a Software Bill of Materials (SBoM) will enable the HDO to identify and address vulnerable device components. This information is valuable in the development of IR plans as it enables triage and prioritization across an organization's device inventory helping facilitate a swift response when an incident occurs.

Service Layer Access:

- Consider arranging for a cybersecurity preparedness user account that provides service layer access during an incident. This may enable minimal disruption of clinical operations and a more rapid response.

AAMI's *Medical Device Cybersecurity: A Guide for HTM Professionals*[9] can serve as an additional resource.

6.1.2 Medical Device Asset Inventory[10]

A foundational preparedness principle is knowing what systems are connected to the HDO's network. By maintaining a centrally managed, baseline set of information about each medical device, an HDO will be better situated to account for and manage medical devices before, during, and after a cybersecurity incident. This includes legacy devices and devices located on research or other non-standard networks. Updating this information regularly (ideally, real-time and/or when there are changes) will help ensure that the inventory is current when an incident arises so that devices can be quickly located and patched, pulled offline, and/or replaced, as needed.

Device information may include:

- Device name and description;
- Device physical location;
- Logical device location (e.g., Internet Protocol address, switch port and/or wireless access point connection(s));
- Device owner and manager;
- Device maintenance parameters (e.g., no longer supported by the manufacturer; internally maintained by X organization [with current contact information]; maintenance outsourced and provided by Y entity with these Service Level Agreement [SLA] parameters);
- Device operational status (in use, broken, etc.), to include current Operating System and patch status;
- Embedded components (e.g., SBoM), to include component version, release, patch status, etc.;
- Interaction with and/or dependencies on other devices/IT resources, and

9 http://my.aami.org/store/detail.aspx?id=MDC-PDF

10 This is considered a goal capability; many HDOs currently do not have the capability to catalog all their medical devices to this degree.

- Log files that capture device operating and/or diagnostic information (e.g., to diagnose malfunctions as cyber-related or not), ideally with a capability to interpret error codes, as applicable.

The NIST Cybersecurity Framework (CSF)[11] provides additional detail regarding asset inventory (e.g., hardware, software) within the CSF "Identify" function's asset management category. Each subcategory within asset management maps to an appropriate security control(s) to provide additional implementation best practices.

HDO medical device procurement practices might consider requiring the manufacturer to provide both an SBoM and a query capability to maintain the device asset inventory. Additional medical device asset inventory materials can be found in AAMI's *Medical Device Cybersecurity: A Guide for HTM Professionals.*

6.1.3 **Hazard Vulnerability Analysis**

Cybersecurity incidents and their potential impact on medical devices are important to include in a broader Hazard Vulnerability Analysis (HVA)[12]. An HVA is used to "assess and identify potential gaps in emergency planning."[13] Anticipated cybersecurity threats and existing mitigations should be reviewed to identify and manage residual cybersecurity risks (e.g., accept, avoid, transfer).

Resources to support a cybersecurity hazard analysis include:

- AAMI's *Medical Device Cybersecurity: A Guide for HTM Professionals,*[14]
- Manufacturer Disclosure Statement for Medical Device Security(MDS^2),[15]
- Veteran's Affairs (VA) 6550, Pre-Procurement Assessment For Medical Device/Systems,[16]
- NIST SP 800-30 revision 1, Guide for Conducting Risk Assessments,[17]
- ASPR TRACIE,[18]
- Kaiser Permanente's HVA planning tool,[19]and
- The American Health Care Association and the National Center for Assisted Living's overview of the HVA process.[20]

Potential cybersecurity risks include:

- The inability to conduct a complete medical device asset inventory,
- The inability to collect and correlate system audit logs across the enterprise,
- Limited sensor coverage (e.g., security monitoring tools) to detect adversary activity on HDO devices, other systems, and networks,
- Device procurement process that does not address cybersecurity, and

11 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

12 Such as to support the CMS Emergency Management Final Rule

13 https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Downloads/FAQ-Round-Four-Definitions.pdf

14 http://my.aami.org/store/detail.aspx?id=MDC-PDF

15 https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

16 https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=790&FType=2

17 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

18 https://asprtracie.hhs.gov/technical-resources/3/Hazard-Vulnerability-Risk-Assessment/0

19 https://www.calhospitalprepare.org/post/revised-hva-tool-kaiser-permanente

20 https://www.ahcancal.org/facility_operations/disaster_planning/Documents/Hazard%20Vunerability%20Assessment%20for%20Healthcare%20Facilities.pdf

- Lack of staff able to detect and respond to a cybersecurity incident.

Potential mitigations include:

- Assessing the HDO's infrastructure and tiering/prioritizing functions and assets to protect and maintain during an incident in order of importance;[21]
- Reviewing and prioritizing remote connections, as IR may require temporarily blocking or severing these connections;
- Putting medical devices—especially legacy devices that cannot be easily secured—on their own dedicated and protected network segment, separate from general IT assets;[22]
- Improving device procurement practices;[23]
- User awareness and training; and
- Intrusion detection and/or security information and event management capability.

The risk assessment results can be used to identify the need for additional mitigating measures (e.g., the need to hire skilled cybersecurity incident responders or allocate resources to training of designated staff) and inform the medical device cybersecurity portions of the HDO's Emergency Operations Plan (EOP).

6.1.4 Medical Device Cybersecurity Support to the HIMT

HDOs typically have an Incident Command System (ICS) that defines a Hospital Incident Management Team (HIMT) to lead response to all-hazards incidents. If the incident includes medical device cybersecurity concerns, include Medical-Technical Specialists with cybersecurity and medical device expertise as part of the activated HIMT.

During the preparedness phase, a senior leadership champion, such as the Chief Information Officer (CIO), may officially sanction (e.g., through policy) the cybersecurity decisions and actions the HIMT takes during an incident (e.g., curtailing device usage). During a cyber attack, there is not always time to make calls through a chain of command; accordingly, to facilitate timely decision making during an incident, clarify, in advance, who has what authority.

In addition, determine if any IR roles require external support, such as from the manufacturer(s), maintenance contractor(s), peer HDOs, regional partners, trade associations, the H-ISAC, etc. For instance, will they partner during exercises only, or are they also needed to fulfill Service Level Agreements (SLAs) during an incident? Foster relationships with manufacturers during the preparedness phase—such as establishing POCs for each manufacturer. Create a chart that identifies all medical device cybersecurity roles, people filling the roles, and two methods of contact for each person. A starting place is to determine whether the manufacturer has an outward-facing product security and privacy webpage, which includes contact information for reporting incidents and incident-specific alerts.

Additional medical device cybersecurity HIMT roles and responsibilities may include the following:

---

21 https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

22 The VA isolation architecture provides one such approach: http://www.himss.org/department-veterans-affairs-medical-device-isolation-architecture-guide-v20

23 The VA's Medical Device Cybersecurity design patterns document provides guidance on device procurement and other medical device cybersecurity topics: https://www.oit.va.gov/library/programs/ts/edp/privacy/MedicalDeviceSecurity_V1.pdf

- **Information Security Officer (ISO)** – Designated by the Incident Commander to lead the cybersecurity portion of the HIMT and deal with the logistics of managing IR. The ISO is the liaison to the Incident Commander and the cybersecurity support staff.
- **Chief Medical Information Officer (CMIO)** – The CMIO is involved with IT-related decisions having a potential impact on patient care (e.g., taking a portion of the network offline, shutting off devices).
- **Specialized Technical Experts** – Specialized medical device and/or cybersecurity expertise may be needed to augment the Medical-Technical Specialists. Example expertise may include HTM, intrusion detection, malware analysis, and digital forensics. Not all HDOs will have staff with these skills; collaborating with regional peers and/or outsourcing may be needed.
- **Medical Device Cybersecurity Liaison** – To facilitate IR coordination with external entities, such as regional partners and/or the device manufacturer, a medical device cybersecurity liaison should be identified. Ideally, this person will be familiar with the affected device(s) (e.g., an HTM professional) and may be part of the HIMT Liaison Officer's team as a Medical-Technical Specialist.
- **Other HDO Support Staff** – While the technical team is responsible for incident detection, analysis, and eradication, the HIMT may require support from other HDO departments, such as HMT, legal, risk management, finance, human resources and public affairs/media relations, to ensure that the right information is conveyed to the right people at the right time. Additional information about these roles is in Appendix A.

6.1.5 Emergency Operations Plan Medical Device Cybersecurity Supplement

The CMS Emergency Management Final Rule, NIMS, HICS, and other emergency preparedness systems call for the creation of an EOP to describe how an HDO will "respond to and recover from a threat, hazard, or other incident."

- Authorization from a senior leadership champion, such as the CIO or CMIO, to sanction the medical device cybersecurity-related plan development, HIMT member activation, and HIMT member actions during an incident;
- Identification of HIMT members handling incident actions, including roles, responsibilities, and names, with at least two distinct methods of communication; and
- Definition of a medical device cybersecurity incident. Clarifying questions include the following:
  - When is a medical device cybersecurity issue considered an incident?
  - What are the trigger scenarios that will cause the IR activity to occur?
  - Are vulnerabilities with available patches considered incidents, for instance?
  - Do alerts from external entities (e.g., regional HCC, ASPR, HCCIC, H-ISAC) help establish incident status? Under what circumstances?

Additional considerations include:

- Cyber insurance: HDOs with cyber insurance might want to be aware of the policy terms and have access to the policy;
- When and how to activate and transition to/from the medical device cybersecurity elements of a Business Continuity Plan;
- Medical device cybersecurity incident notification sources;
- Triggers for medical device cybersecurity HIMT member activation;
- Internal and external communication requirements, to include regional and federal partners, as applicable;
- How situational awareness is maintained; and

- Creation of mutual aid agreements within the region to enable incident-related access to additional medical devices (e.g., through device loans or agreements to divert patients).

6.1.6 Incident Response Communications Plan

Include medical device cybersecurity incident-specific communications in an overall HDO IR Communications Plan. Communications regarding medical device cybersecurity incidents often involve different external stakeholders, as shown in Figure 2. Additional information about these and other stakeholder roles can be found in Appendix A.

Within the IR Communications Plan, call out medical device cybersecurity-specific communication needs, which may include the following:

- Identification of key internal and external stakeholders and their communication roles (e.g., state Department of Health liaison, public affairs), with primary and secondary means of communication (e.g., email, landline), including who is authorized to speak publicly about the incident;
- Planned frequency of communications between internal stakeholders (e.g., IT, HTM, C-suite);
- Planned frequency of communications with external stakeholders, to include device manufacturers as noted in their Incident Management Policies, as applicable; and
- Incident sharing parameters.

6.1.6.1 Incident Sharing

Given potential incident sensitivities, specify incident sharing expectations for all participants in the IR communications plan. This may include the following:

- What incident information can (and cannot) be shared.
- With whom incident information can (and cannot) be shared and under what circumstances.
- By what mechanism the information can be shared.
- When incident information can be shared. Are there circumstances that would prevent sharing during an incident? Is there an incident reporting timetable requirement?
- Is there a designated regional command center to facilitate sharing, and if so, how will the HDO participate?

6.1.6.2 Incident Identification

If a cybersecurity incident involving a medical device is identified, initiate outreach, first to the manufacturer and then to the broader healthcare community. Informal outreach to regional peers may confirm similar symptoms and provide validation. In addition, as applicable, share the medical device cybersecurity incident information with the H-ISAC or another healthcare-oriented ISAO, with regional incident response partners, and with the state Department of Health.

6.1.6.3 Incident Notification

HDOs need to receive notifications of externally discovered medical device cybersecurity issues to initiate the appropriate response activities. These notifications may come from many sources, such as the manufacturer, the H-ISAC (or other ISAO), the FDA, Department of Homeland Security National Cyber Command Information Center (NCCIC), Department of Health and Human Services Healthcare Cybersecurity and Communications Integration Center (HCCIC), regional partners, and state Department(s) of Health. For example, as part of the WannaCry response, several forward-leaning manufacturers posted alerts on their product security and privacy webpages, with a list of the products impacted and associated mitigations available. Additionally, they coordinated with US-CERT/NCCIC to consolidate their alerts under one NCCIC

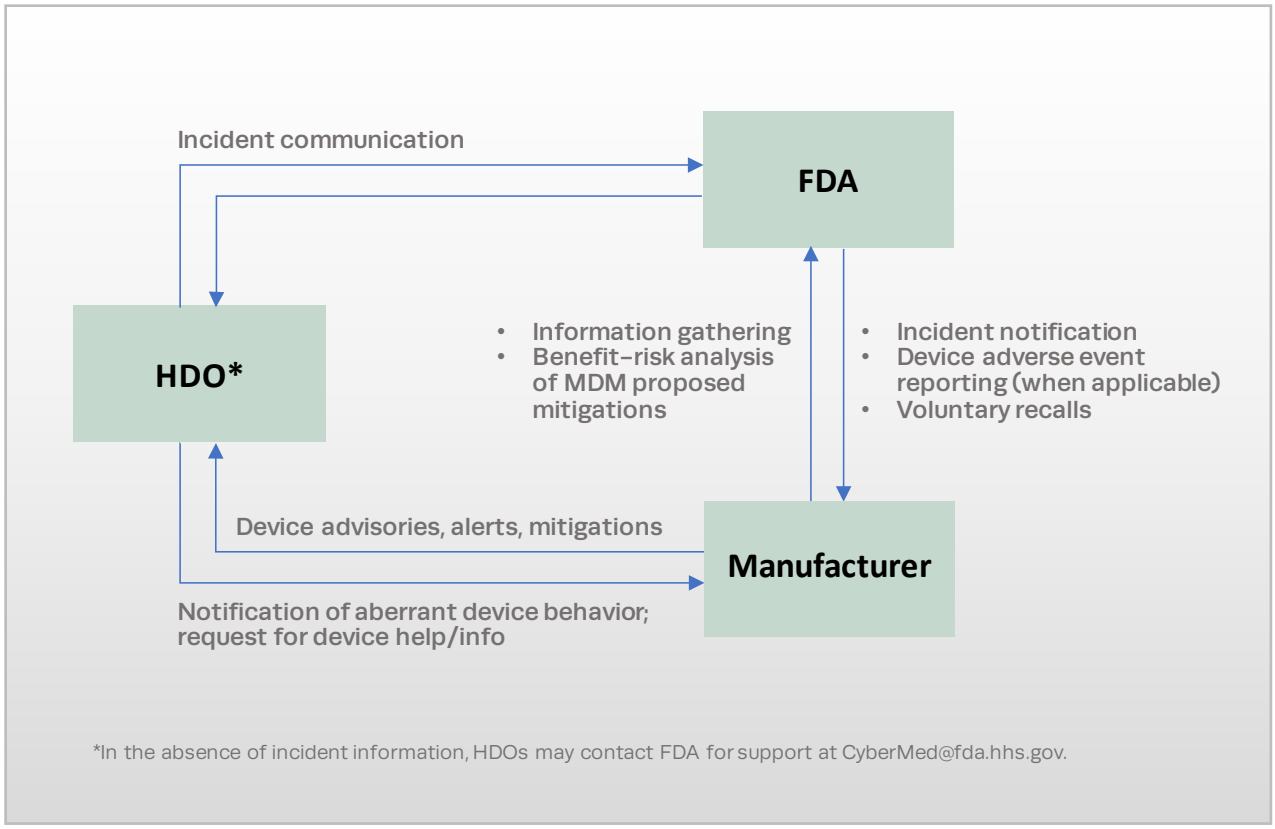


Figure 2. Medical Device Cybersecurity Key Stakeholders Incident Response Interactions

alert[24] to facilitate the accessibility of information to the user community. H–ISAC receives and disseminates all healthcare–related threat and vulnerability information through its sector–wide Outreach Program,[25]which provides a "one–stop shopping" alerting mechanism for non–members. Public vulnerability databases, such as the National Vulnerability Database,[26] disseminate notifications of broader cybersecurity issues.

6.1.6.4 Incident Situational Awareness

To stay abreast of incident status, such as new intrusion details and/or mitigation recommendations, engage with contacts at the manufacturer(s), as well as at the regional and federal levels.

For widespread healthcare–related incidents—including but not limited to medical device cybersecurity—HHS ASPR CIP provides regular, if not daily, regular situational awareness calls to the HPH Sector.

H–ISAC also provides sector–wide calls that are generally more technical in nature.

6.1.6.5 Communication Templates

Draft communication templates should be developed to prepare for different IR messaging needs, to include the following:

24 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01I

25 https://nhisac.org/outreach/outreach-program/

26 https://nvd.nist.gov/

- Incident notification,
- Internal communications to, for instance, activate the HIMT, contact impacted staff (e.g., system users/owners/managers), inform the C-suite of incident parameters, and notify all users of the incident and its impacts,
- External communications to business associates or others whose assets and/or communication channels could be impacted by the original incident (e.g., severing remote connections due to compromise),
- Internet service provider notification,
- Outreach to trusted partners to share incident parameters,
- Public affairs messaging to make the public aware of the incident and its impacts,
- Compliance and/or regulatory notification communications, and
- Notification to law enforcement.

Prepare boilerplate emails, press releases, and other communications templates to facilitate timely IR communications.

Identify primary and secondary methods for communicating with key stakeholders. In particular, request that HIMT members designate a primary and secondary mechanism of contact (e.g., landline, email, cell phone, pager).

Explore and exercise alternative communications mechanisms that may be needed during an incident to ensure, in advance, that they are accessible. For incidents with compromised communications, the HHS/HCCIC, the Department of Homeland Security/Homeland Security Information Network (DHS/HSIN)[27], the state's health emergency communication network (e.g., Massachusetts' Health and Homeland Alert Network, Nevada's Health Alert Network)[28], and the FDA's safety notification dissemination channel[29] may provide an alternate means for cross-region communication. H-ISAC offers "WEE Secrets" [30] for its members. Regional organizations, such as the state Department of Health or the Regional Fusion Centers, may also offer an out-of-band communication capability during emergencies.

6.1.7 Training

Two types of training will help prepare HDOs for medical device cybersecurity incidents, as described in the sections that follow.

61.7.1 User Awareness Training

Medical device users, from clinicians to IT helpdesk staff and HTM professionals, should be aware of potential device cybersecurity incidents, their impacts, and appropriate responses. User awareness is particularly important in incident discovery, as many device cybersecurity issues are found by users. Cybersecurity issues often initially manifest as unusual device behavior; regular training for device users will help to ensure that cybersecurity is considered as a potential cause for any device peculiarity. In addition, identify medical device cybersecurity POCs and familiarize users with the device cybersecurity incident classification and

27 https://www.dhs.gov/homeland-security-information-network-hsin

28 Massachusetts' and Nevada's statewide health alerting systems: https://www.researchgate.net/publication/23463585_The_Massachusetts_Health_and_Homeland_Alert_Network_a_scalable_and_secure_public_health_knowledge_management_and_notification_system
http://dpbh.nv.gov/Programs/NVHAN/NVHAN_-_Home/

29 https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/default.htm

30 http://www.nhisac.org

prioritization system (see section 6.2.2). Incorporate awareness training into broader emergency preparedness or medical device user training.

Device users would also benefit from participation in exercises, building their understanding and enhancing their situational awareness of the types of medical device cybersecurity scenarios that may arise.

61.7.2 **Exercises**

HDOs conduct preparedness and response exercises for all-hazards. Cybersecurity can be integrated into these exercises; alternatively, separate cybersecurity exercises can be conducted. Incorporate participation from across the HDO and include not just the emergency response organization, but also the HTM and IT departments, as well as manufacturers and maintenance contractors.

To improve preparedness, create or participate in exercises designed to simulate realistic incidents. After the exercise, update the EOP and other IR plans to incorporate lessons learned, create or improve communication channels between different business units, define internal policy and processes, create new groups if necessary, obtain buy-in from senior leadership and affected business units, and identify the individuals who will participate in IR.

More information about medical device cybersecurity exercises can be found in Appendix B.

6.2 **Detection and Analysis**

The following sections describe medical device cybersecurity incident detection and analysis.

6.2.1 **Incident Detection and Validation**

The first part of incident detection and analysis is *identifying* or otherwise establishing that an incident has occurred. With natural disasters and terrorist attacks, there is no ambiguity. Cybersecurity incidents, however, are often difficult to identify and characterize correctly, as they may masquerade as malfunctions or go unnoticed. Many device cybersecurity issues are identified by the manufacturer and issued with concomitant mitigations (e.g., patches); patch management, in and of itself, would not be considered incidents if the vulnerability has not been exploited, the device is functioning properly and/or exposure is not severe.

Once the HDO has learned of a potential cybersecurity incident (as noted in Sections 6.1.5.2 and 6.1.5.3), incident validation commences. Questions to ask include:

- Is it real? How do you know?
- How did the potential incident arise? How was notification given?
  - External or internal source?
  - Security tools and sensors?
  - Device acting erratically?
- Have regional partners experienced anything similar?

Once an incident has been established, it should be categorized to determine the next steps.

6.2.2 **Incident Categorization and Prioritization**

Define classes of medical device cybersecurity incidents to help prioritize incidents and determine the appropriate level of response. Consider how the business impacts resulting from different incident types and severity levels can be tied to a priority level (e.g., high, medium, low) that ties to a concomitant resolution level of effort (e.g., from "stop everything and fix this," to "resolve during the next maintenance cycle").

Patient care is always the top priority. A Common Vulnerability Scoring System (CVSS) [31] supplemental rubric for medical devices[32] is under development by MITRE with input from the stakeholder community, and once validated[33] may be used to assess the severity of a vulnerability and help determine incident classification. This rubric can put the potential device impacts into a clinical context and help with decision making. A table that aligns the severity levels, the types of incident, the business impact, and the levels of response will provide a common communication mechanism for IR and non-IR personnel (e.g., device users). Table 1 is an example.

Table 1. Example Incident Classification and Prioritization Table[34]

Category	Severity	Priority Guideline	Score[35]	Initial Action	Containment Goal
Category 0	Emergency	Severe impact on enterprise	13–15	Immediately	ASAP
Category 1	Critical	Loss of a major service	11–12	Immediately	<24 Hours
Category 2	Important	Some impact some portion of enterprise	8–10	Within 4 hours	<72 Hours
Category 3	Routine	Minor impact on a small portion of enterprise	5–7	Within 24 hours	<7 Days

If possible, the HDO should also establish an escalation list that ties medical device cybersecurity IR decision making responsibilities to specific roles in the HIMT hierarchy, in keeping with higher incident severity levels. External entities that may play a key role (e.g., manufacturer, maintenance contractor, state/local government) should be included, as appropriate.

6.2.3 Incident Reporting

Formal and informal reporting obligations often accompany discovery of a medical device cybersecurity incident. A manufacturer is required to conduct a formal notification of the incident to its customers and user community.[36, 37, 38] Formal notification may be a condition of ISAC or ISAO membership. Depending on the nature of the incident, law enforcement may need to be contacted by the affected entity. Though outside the scope of this playbook, HDOs also need to consider those circumstances that warrant incident reporting for breaches of Protected Health Information (PHI)[39] and/or Personally Identifiable Information (PII)[40].

Depending on the HDO's incident sharing approach, informal incident sharing with others, such as regional partners, may also occur. Reporting and sharing should be carried out by someone with an official incident liaison role.

---

31 https://www.first.org/cvss/

32 Link for supplemental rubric is forthcoming.

33 Link for supplemental rubric is forthcoming.

34 Adapted from the *State of Connecticut Sample Incident Response Plan Template*, found at https://portal.ct.gov/Connecticut-Cybersecurity-Resource-Page

35 CVSS base score

36 https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=806&showFR=1

37 https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

38 https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=803.10

39 https://www.hhs.gov/hipaa/for-professionals/security/index.html

40 https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Internal reporting, such providing incident status to senior leadership or issuing an advisory to device users, may also take place.

6.2.4 Incident Analysis

Once the initial incident parameters have been established, the incident investigation begins. The assigned HIMT members need to gather data to determine the full incident impact, which will inform the containment strategy. Information sources may include:

- External sources, which provide additional insights on the vulnerability, malware, and/or potential exploits, such as:
  - Manufacturer,
  - DHS NCCIC,
  - HHS ASPR,
  - Cybersecurity–knowledgeable organizations, such as SANS, Symantec, and the CERT Coordination Center,
  - Regional partners,
  - Internet service provider, and
  - Business partners.
- Internal sources, which provide insights on the incident's impact within the HDO, such as:
  - Log files (e.g., device logs, server logs, domain name server logs, firewall logs, router logs),
  - System and network tools and sensors,
  - Device users, and
  - System and network administrators.

6.2.5 Incident Documentation

Record all activities undertaken during cybersecurity IR, from incident discovery to containment and post-activity. Capturing how the incident was discovered, the steps taken, the decisions made, etc., will aid incident investigation and can also be reviewed in the Post Activity phase to improve future IR.

If the nature of the attack may involve potential criminal activity, then preserving evidence and chain of custody is important, and the HDO may need to bring in external forensics experts.

The Detection and Analysis steps are usually iterative. When additional incident insight is acquired, the response and containment procedures may need to be adjusted, and the communications, reporting, and/or sharing may also need to be updated.

6.3 Containment, Eradication, and Recovery

Once an incident has been confirmed, the response activity begins. Many HDOs use a "contain, clean, and deny" strategy to halt a cybersecurity incident, fix the damage, and restore services as quickly as possible. When cybersecurity criminal activity is suspected, a "monitor and record" strategy that watches and captures adversary actions may be used.

Containment begins with HIMT activation and execution of the EOP. Minimizing impact to healthcare delivery, halting the active cybersecurity disruption, assessing the damage, and restoring normal business operations are the overarching goals driving the overall response phase. Questions to consider include the following (ideally, these have been enumerated at least broadly in the EOP):

- Is the device safe to use? Has confidence in the device's effective use and operation been undermined due to cause or uncertainty? Has the device been compromised resulting in evidence of patient harm? Is there a reliable way to test the device and confirm its safety? Who can perform this testing? When?
- If confidence in the device has been compromised, what is the backup plan? Can the device(s) be safely used in a reduced or limited capacity, such as operating with fewer than the normal number of devices? Do spare or backup, uncompromised devices exist, or does the incident impact all similar devices? What is needed to make backup devices available?
- When do mutual aid agreement(s) need to be activated? Can regional peers provide loaner devices and/or do patients need to be diverted?
- Can the manufacturer or a third-party leasing service provide loaner devices? What is needed to make this happen?
- How quickly can this problem be fixed? Who can fix it? Can the HDO make device adjustments (e.g., install patches), or do maintenance contracts preclude this? Is there a mitigation (e.g., isolating the device from the network) that can enable safe continued use?
- Are there manual procedures that can be used in the absence of a reliable device? Can the affected device be used safely if removed from the HDO network?
- Have the affected devices caused collateral damage to the broader healthcare system?
- How/can region resources be leveraged to help? How/can federal resources help?
- How/is the outage communicated internally? Externally? When?

Internal and external response communications should follow the medical device cybersecurity portion of the Communications Plan.

The remediation needed to return operations to normal may take much longer than anticipated. Comprehending the extent of an incident may not be straightforward, mitigations may not be readily available, outsourced assistance may be needed, and more. Thus, HDOs should plan for a potentially lengthy recovery period.

6.4 Post Activity

When exercising an IR plan, whether as part of a practice activity or in the event of an intrusion, the response activity does not end with system recovery. One of the most important aspects of post IR is identifying what went well and what did not. This information can be leveraged to improve the existing plan and the HDO's response to another incident.

Post Activity follows the conclusion of the formal IR activities.

6.4.1 Lessons Learned

Incident insights should be obtained from key IR participants to improve future incident response. Often, a "hot wash" session is conducted to elicit this feedback. Questions to pose include the following, taken from NIST SP 800-61r2:

- Exactly what happened, and at what times?
- How well did staff and management deal with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?

- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for to detect similar incidents in the future?

6.4.2 Forensics Investigation

Consider retaining a trained digital forensics expert to determine the full extent of any damage to the affected entity associated with a cybersecurity incident.

6.4.3 Plan Updates

Document post-incident insights—what worked, what didn't, ideas for the future, etc. As appropriate, update the EOP, Communications Plan, and other pertinent plans in light of the experience gained. In addition, review all plans annually, whether an incident occurred or not, to ensure that all processes, procedures, contacts, etc., are current.

7. Summary

Through planning and practice, as well as support from and collaboration with manufacturers and regional and national partners, HDOs can be well positioned to manage medical device cybersecurity incidents. Conducting a thorough device inventory and developing a baseline of medical device cybersecurity information are the first steps in developing a cybersecurity preparedness and response framework. Within the framework, an understanding of roles and responsibilities of responders internal and external to the HDO will help to clarify lines of communication and CONOPs across HDOs, medical device manufacturers, state and local governments, and the federal government. The framework can also help to enable a unified response within HDOs and across regions, as well as serve as a basis for enhanced coordination activities among medical device cybersecurity stakeholders, including mutual aid across HDOs. With healthcare-related cyber incidents growing in size and scope, preparedness before a cyber event takes place with a strong, well-exercised, support infrastructure in place is foundational to executing a rapid, comprehensive and robust response.

8. Acknowledgements & Stakeholder Feedback

MITRE would like to thank the HDOs, state departments of health, medical device manufacturers, and government agencies that provided insights into their medical device incident response gaps and challenges. The framework and resources provided in this document are a direct result of lessons learned from these engagements. Stakeholder feedback and comments on this tool are greatly appreciated via securemed@mitre.org

Appendix A. Stakeholders

To prepare for and respond to medical device cybersecurity incidents, HDOs benefit from expertise in several areas and a willingness to interact with a number of external entities. Below are descriptions of how these key roles and responsibilities might be conceptualized and/or defined. Figure 3 shows example regional IR interactions.

A.1 Internal to the HDO

Within the HDO, several roles can enable effective IR planning and execution. Below is a non-exhaustive list of roles that might be involved in the event of a cybersecurity incident involving a medical device.

A.1.1 Information Security Officer

The ISO leads the overall cybersecurity preparedness and response activities. This role (1) oversees the internal Cybersecurity Incident Response Team[41] that is actively investigating, mitigating, and otherwise responding to an incident, and (2) manages the cross-disciplinary team that develops and executes the IR plan when incidents arise. The ISO keeps senior leadership (e.g., C-suite) informed of incidents and response activities.

A.1.2 Risk Management Officer

The Healthcare Risk Manager is an integral part of delivering safe and trusted health care[42], continually assessing and minimizing various risks to staff, patients and the public. This function plays a vital role in event and incident management.

A.1.3 Chief Medical Information Officer

The CMIO, an intermediary between the medical and IT departments, is a key decision maker during incident preparedness and response. Typically a physician with medical informatics training, the CMIO generally makes the IT decisions with potential impacts on patient care (e.g., taking a portion of the network offline, shutting off devices).

A.1.4 Privacy Officer

The Privacy Officer provides privacy expertise to incident preparedness and response activities, such as addressing potential privacy breaches, assessing potential business associates' privacy policies, guiding privacy-related policy decisions, and authoring communications to PII-breached account holders.

A.1.5 Legal

Legal involvement ensures that the organization's legal obligations, if any, are considered (e.g., intellectual property; data privacy; other).

41 Computer Security Incident Response Team (CSIRT) or equivalent, which may be an outsourced Managed Security Services Provider.

42 http://www.ashrm.org/about/HRM_overview.dhtml

A.1.6 Compliance

The compliance representative provides expertise regarding the HDO's regulatory, policy, and other compliance obligations.

A.1.7 Human Resources

Human Resources provides guidance on personnel matters.

A.1.8 Finance

A decision-making member of the finance organization may be involved in IR activities, as additional funding may be needed to cover unanticipated labor, software, or equipment costs of incident response and mitigation. In the case of a Personally Identifiable Information (PII)/Protected Health Information (PHI) breach, a fine may be levied.

A.1.9 Public Relations/Communications

Communications play a key role in effective incident response. Clear messaging of roles, responsibilities, events, actions, expectations, and timelines ensures a common understanding of incident execution to both internal and external audiences. Incident response communication templates (e.g., boilerplate emails and press releases) should be developed and exercised during preparedness to enable smooth communications during an incident.

A.1.10 Physical Security

Physical security's role includes providing physical protection to the organization's critical assets, particularly if cybersecurity protection was breached during an incident. Physical security may also facilitate communications with local law enforcement, as needed.

A.1.11 Clinical

Clinicians' roles include patient safety and continued care concerns as they relate to potential/actual incident impacts. Likewise, clinicians need to be engaged if patient care procedures must change to accommodate incident response activities.

A.1.12 Healthcare Technology Management

Representation from the HTM professionals who manage HDO medical devices is also important. Generally, HTM professionals are best suited to identify temporary device work-arounds during an incident. In addition, HTM professionals often have relationships with the device manufacturers, who may need to help devise and execute a longer term resolution.

A.1.13 Information Technology

A member of the HDO IT infrastructure team with knowledge of the HDO's key IT assets, applications, and infrastructure works in partnership with the CSIRT to help validate vulnerabilities, enable work-arounds, and establish essential minimum functionality. The IT POC establishes clear escalation and communication channels to enable rapid decision making and action during an incident. Beyond the core HDO network, the IT representative is also able to notify POCs of related network infrastructures (e.g., research networks/laboratories, direct point-to-point connectivity) that might be impacted by incident activities. The IT role may be carried out by an IT contractor.

A.2 External to the HDO (Non-federal)

Given the nature and sophistication of today's cyber adversaries, external collaboration is essential for effective cybersecurity. This section describes the key non-governmental stakeholders to be engaged by HDOs during preparedness and response activities.

A.2.1 Medical Device Manufacturers

MDMs are a key partner during medical device incident response. MDM knowledge of device components and composition, as well as ability to validate vulnerabilities, assess for device intrusion and/or compromise, and develop mitigations, are critical in returning the HDO to a fully functional capability. In some cases, device maintenance contracts may limit HDO intervention and make them completely dependent on the MDM (or other maintenance contractor) to make any needed device alterations. In other cases, a third-party supplier may need to be consulted if embedded device components contain or contribute to vulnerabilities.

A.2.2 Peer HDOs

Peer HDOs are a potentially valuable preparedness and response collaborator. By establishing trust relationships with peers, HDOs can further their collective cybersecurity preparedness through sharing cybersecurity best practices and coordinating exercises. During incidents, peer HDOs can also help each other by confirming and validating details of device intrusion and/or compromise, impacts, and mitigations. These relationships may be cultivated through membership in local, regional, and/or trade associations, or ISACs/ISAOs.

A.2.3 ISACs/ISAOs

Through presidential executive orders and policy directives, the federal government has encouraged the creation and use of ISACs and ISAOs to improve cybersecurity preparedness and response. H-ISAC is the ISAC for the Healthcare and Public Health (HPH) sector. ISAOs provide a flexible approach to self-organized information sharing activities among communities of interest.

"The Health Information Sharing and Analysis Center (H-ISAC) is a global, non-profit, member-driven organization offering health sector stakeholders a trusted community and forum for coordinating, collaborating and sharing vital Physical and Cyber Threat Intelligence and best practices with each other. Members use this information to extend their security operations team and to create situational awareness, inform risk-based decision-making and mitigate against threats."[43]

A.2.4 Trade Associations

Trade associations may play a role in cybersecurity incident preparedness, particularly in helping to educate their constituency. HDO-oriented trade associations, such as the College of Healthcare Information Management Executives Association of Executives in Healthcare Information Security (CHIME/AEHIS), the American Hospital Association, regional hospital associations, HTM societies, the Association for the Advancement of Medical Instrumentation, and Healthcare Information Management and Systems Society (HIMSS), can facilitate inter-organization trust relationships, stand up working groups to develop generic IR plans, generate standards, and produce IR communication templates. MDM-oriented trade associations, such as AdvaMed, Medical Device Manufacturers Association (MDMA) and Medical Imaging and Technical Alliance (MITA), can provide a centralized communication vehicle for HDOs and others regarding medical device cybersecurity incidents and mitigation information.

43 https://nhisac.org/

A.2.5 Public–Private Partnerships

As the bulk of the HPH sector is comprised of private entities, public–private partnerships are essential in fostering cross–sector collaboration. Some public–private partnerships that may aid incident preparedness and response include those described in the sections that follow.

A.2.5.1 Healthcare and Public Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council[44] is "a cross–sector coordinating body representing one of 16 critical infrastructure sectors identified in Presidential Executive Order (PPD–21)" and "a trust–community partnership convening companies, non–profits and industry associations across six sub–sectors with HHS, DHS, law enforcement, and intelligence community." Its mission is "to identify cyber and physical risks to the security and resiliency of the sector, and develop guidance in a 3–year Sector Specific Plan and implementing task groups for mitigation those risks."[44]

A.2.5.2 Cyber Unified Coordination Group (Cyber UCG)

Introduced in Presidential Policy Directive–41, the Cyber UCG convenes during cyber threats and incidents of national significance. The Cyber UCG "shall serve as the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts, as appropriate."[45]

A.2.5.3 Cross–Sector Cyber Security Working Group (CSCSWG)

The CSCSWG facilitates cross–sector collaboration on cyber issues. Cybersecurity concerns in other sectors may impact healthcare and public health. Participation in cross–sector efforts enhances situational awareness as well as preparedness.

A.2.5.4 Regional Testing Laboratories

Regional HDO–centric testing laboratories may provide valuable venues for regional, face–to–face preparedness and response collaboration, as well as local, cross–sector validation of device vulnerabilities and concomitant remediations.

A.3 External to the HDO (Federal)

The federal government provides a number of resources to help the HPH sector and the broader government and industry ecosystem address cybersecurity preparedness and response. Those relevant to the healthcare sector are detailed in the sections that follow.

A.3.1 Department of Homeland Security

he Department of Homeland Security (DHS) is the primary federal entity charged with protecting the 16 U.S. critical infrastructure sectors, including the HPH sector, from physical and cybersecurity threats. DHS offers a number of resources to aid cybersecurity incident preparedness and response, to include training, awareness, cyber threat sharing, and more. Those most relevant to medical device cybersecurity preparedness and response are detailed below.

---

44 https://healthsectorcouncil.org/cybersecurity-working-group-primer/#Cybersecurity-Working

45 Presidential Policy Directive (PPD)–41, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

A.3.1.1 US-CERT/NCCIC

The United States–Computer Emergency Response Team (US-CERT) operates the National Cyber Command Information Center (NCCIC), a 24/7 operational cyber threat incident response center. "The NCCIC serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts."[46] It also manages the CERT function for medical devices within the United States. This includes coordinating vulnerability disclosure between security researchers and MDMs, issuing advisories and alerts regarding device vulnerabilities, and engaging the FDA and others, particularly when potential safety issues arise.

A.3.2 Department of Health and Human Services (HHS)

DHS has designated HHS as the Sector Specific Agency for the HPH sector. As such, HHS "is responsible for managing and coordinating broad-based sector security and resilience activities."[47]

A.3.2.1 ASPR

"ASPR serves as the Secretary's principal advisor on public health emergencies and leads a collaborative approach to the department's preparedness, response, and recovery portfolio. ASPR is also the lead office responsible for all Federal public health and medical response to public health emergencies and incidents covered by the National Response Framework (NRF) and National Disaster Recovery Framework."[48] The ASPR Critical Infrastructure Protection Program Office manages its cross-sector, incident preparedness, and response coordination responsibilities.

A.3.2.2 Food and Drug Administration (FDA)

The FDA, an agency within the U.S. Department of Health and Human Services, protects the public health by assuring the safety, effectiveness, and security of human and veterinary drugs, vaccines and other biological products for human use, and medical devices. The FDA's Center for Devices and Radiological Health (FDA/CDRH) is responsible for the "timely and continued access to safe, effective, and high-quality medical devices and safe radiation-emitting products."[49] Medical devices from insulin pumps to implantable cardiac pacemakers are becoming interconnected, which can lead to safer, more effective technologies. However, like computers and the networks they operate in, these devices can be vulnerable to security breaches, and exploitation of a device vulnerability could threaten the health and safety of patients. To prevent, detect, and respond to vulnerabilities and exploits, FDA has taken steps to promote a multi-stakeholder multi-faceted approach of vigilance, responsiveness, recovery, and resilience that applies through the life cycle of medical devices. FDA also coordinates with key internal offices such as the Office of Criminal Investigations (OCI), FDA's criminal law enforcement arm, which conducts criminal investigations of illegal activities involving FDA-regulated[50] products, to successfully carry out a common operating picture.

---

46 https://www.us-cert.gov/nccic

47 Healthcare and Public Health Sector-Specific Plan https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

48 Ibid.

49 https://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/default.htm

50 https://www.fda.gov/ICECI/CriminalInvestigations/ucm550316.htm#intro

A.3.2.3 Healthcare Cybersecurity and Communications Integration Center (HCCIC)

In June 2017, HHS stood up its own, healthcare-specific cybersecurity and communications integration center, known as the HCCIC. The HCCIC provides actionable cybersecurity analysis, education, and incident coordination tailored to the cybersecurity needs of the healthcare sector.

A.3.2.4 Office of Civil Rights

The HHS Office of Civil Rights (OCR) "enforces federal civil rights laws, conscience and religious freedom laws, the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule."[51] The OCR becomes involved in cyber incident response when the incident includes a PHI and/or PII breach.

A.3.3 Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. The FBI—often in partnership with other law enforcement and/or investigative organizations, such as the U.S. Secret Service and local law enforcement—may investigate cybersecurity incidents with potential medical device impacts.

A.3.4 National Cybersecurity Center of Excellence

A part of NIST, the National Cybersecurity Center of Excellence (NCCoE) is a public-private partnership that enables government, industry, and academia to collaboratively address sector-specific and cross-domain cybersecurity challenges and formulate "modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST SP 1800 series"[52] (e.g., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*[53]) which contribute directly to HDO preparedness efforts.

A.4 State and Local Governments

A.4.1 State/Local Department of Health

A state's Department of Health may offer some resources to support state and local cybersecurity preparedness, such as convening exercises or conducting training.

A.4.2 State/Local Department of Safety/Emergency Response

State and local governments may offer an emergency response organization and/or a Department of Safety, which is generally charged with active incident coordination and management during all-hazards emergencies.

51 https://www.hhs.gov/ocr/about-us/index.html

52 https://nccoe.nist.gov/about-the-center

53 https://nccoe.nist.gov/projects/use-cases/medical-devices

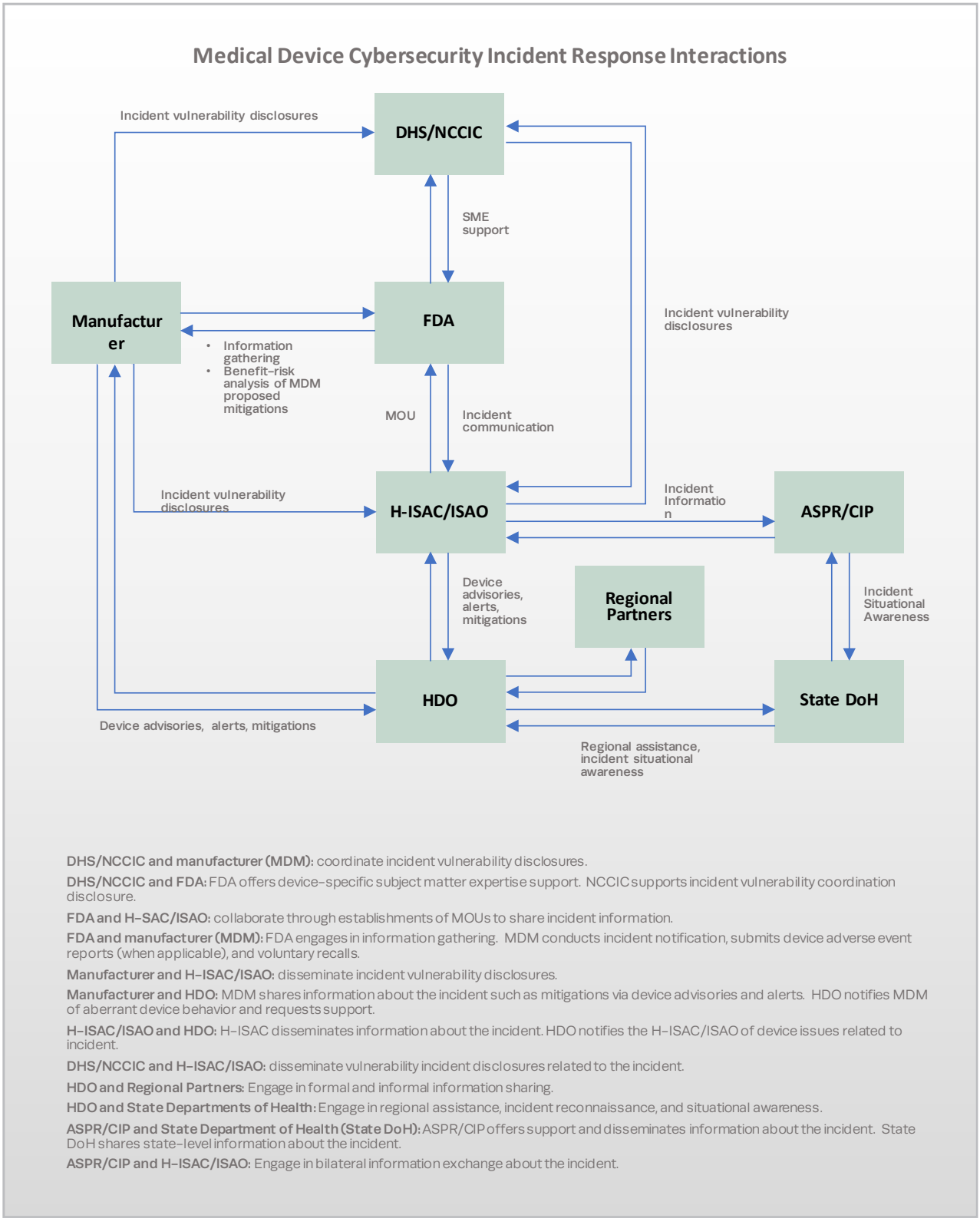
A.4.3 State Cybersecurity and Communication Integration Center State (CCICs)

Some states have established their own CCICs as command centers, similar to a security operations center, for incident coordination and response.

A.4.4 Regional Fusion Centers

To shore up regional capabilities, DHS helped stand up fusion centers in a number of regions. "Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners."[54] Fusion centers are locally owned and operated by state and local law enforcement, emergency responders, and other relevant government personnel. DHS manages the program that evaluates performance of the fusion centers. "DHS, along with other federal partners, also provides significant resources to fusion centers through training, technical assistance, information systems access, guidance, and other support."[54]

54 https://www.dhs.gov/state-and-major-urban-area-fusion-centers



DHS/NCCIC and manufacturer (MDM): coordinate incident vulnerability disclosures.

DHS/NCCIC and FDA: FDA offers device-specific subject matter expertise support. NCCIC supports incident vulnerability coordination disclosure.

FDA and H-SAC/ISAO: collaborate through establishments of MOUs to share incident information.

FDA and manufacturer (MDM): FDA engages in information gathering. MDM conducts incident notification, submits device adverse event reports (when applicable), and voluntary recalls.

Manufacturer and H-ISAC/ISAO: disseminate incident vulnerability disclosures.

Manufacturer and HDO: MDM shares information about the incident such as mitigations via device advisories and alerts. HDO notifies MDM of aberrant device behavior and requests support.

H-ISAC/ISAO and HDO: H-ISAC disseminates information about the incident. HDO notifies the H-ISAC/ISAO of device issues related to incident.

DHS/NCCIC and H-ISAC/ISAO: disseminate vulnerability incident disclosures related to the incident.

HDO and Regional Partners: Engage in formal and informal information sharing.

HDO and State Departments of Health: Engage in regional assistance, incident reconnaissance, and situational awareness.

ASPR/CIP and State Department of Health (State DoH): ASPR/CIP offers support and disseminates information about the incident. State DoH shares state-level information about the incident.

ASPR/CIP and H-ISAC/ISAO: Engage in bilateral information exchange about the incident.

Figure 3. Example Regional IR Interactions

Appendix B. Exercises

The HIMT needs to be well versed in the medical device cybersecurity supplements of the EOP, and the best way to train the HIMT, as well as to validate the EOP, is to conduct exercises.

B.1 Planning, Organization, and Management of Exercises

Exercises may be managed in different ways, depending on the goals, participants, and organizers. The following activities may take place, although they might not all be utilized, depending on the exercise.

- **Hosting:** Pre-exercise, an organization is chosen to host the exercise, which might include reserving physical spaces, setting the agenda, managing logistics, selecting dates for the exercise, etc.
- **Planning**: Pre-exercise, a planning team is identified. The planning team identifies the high-level goals for the exercise and prepares one or more simulated scenarios that involve cybersecurity. These scenarios either (1) have been encountered before or (2) have a realistic likelihood of occurring or are of significant importance to the involved HDO(s). The planning team may break down each scenario into different events or "milestones" that occur in a predetermined timeframe. Each event represents dynamic (and possibly unexpected) changes in the scenario, to which the participants must respond. Events may include "injecting" actions from other parties that are outside the participants' own control, or identifying cases in which the participants' actions do not produce the expected results.
- **Participant Identification**: Pre-exercise, the planning team identifies organizations (or sub-organizations) that will be involved in the exercise. The planning team may focus on which stakeholder roles may be necessary to conduct the exercise.
- **Scenario Development**: A scenario development team—perhaps selected from the planning team and the host—participates in the exercise by presenting scenarios, injecting predetermined events, dynamically modifying the scenario as needed to meet the exercise's goals or time limits, and otherwise guiding stakeholders or answering detailed questions about the scenario.
- **Exercise Execution**: The exercise participants meet at the arranged time and location (possibly virtual), possibly with some preparatory materials. Participants may be broken down into multiple teams or act as a single team. The scenario development team presents a scenario to the participants, starting with the initial event. Each team discusses how it would handle each event in the scenario (e.g., which stakeholders and roles would need to communicate with each other; how they would coordinate to reach a decision; whether they have sufficient information to make such decisions; and what actions they would take based on the decision). The team communicates its actions and decision process to the scenario development team, which introduces the next event, and the process repeats until the last event has been handled. Once the scenario is complete, the participants may review the gaps they discovered, or, do so later on. The development team then selects and runs the next scenario. The process is repeated as needed and as time allows.
- **Post-exercise "Hot Wash"**: Participating organizations perform internal reviews, focusing on lessons learned and areas to improve. Then, the findings are shared with the relevant parties. In some cases, post-exercise activities may be conducted at the exercise site, immediately after the exercise itself.

B.2 Scope of Participation

Each type of exercise may be conducted with different internal sub-organizations or external organizations, depending on each participant's organizational readiness and trust relationships.

B.2.1 Organizational Roles

Each exercise includes planners and participants who cover one or more organizational roles, which might include HTM, IT, legal/compliance, etc.; see Appendix A for a list of possible roles.

In some exercises, the HDO might also interact with external organizations, such as manufacturers, service providers, regulatory/government agencies, and consultants.

B.2.2 Individual HDO

In this model, the HDO identifies its own participants across the relevant business units or sub-organizations; selects representatives from each unit; plans and conducts the exercise; and shares its findings across all units..

B.2.3 Trusted HDO Partner Network

The HDO may be part of a partner network of HDOs that have built-in trust relationships. Depending on how the group shares resources and processes, a group-wide exercise may be useful.

B.2.4 External Business Partners

An HDO (or HDO group) may involve external business partners, such as MDMs or service providers, for whom exercises may be useful. Each business partner may have different degrees of trust that affect how information is shared during or after the exercise.

B.2.5 Unaffiliated Peers

The HDO may choose to participate in exercises or collaborate with other HDOs that are not organizationally related. There may be varying trust relationships with each HDO. There may be a need to utilize NDAs to limit the release of proprietary findings.

B.2.6 Regional/National Preparedness

Some exercises may be conducted on a state, regional, or national level. Governments or non-profit industry organizations may plan the exercises. Participation might be required.

B.3 Exercise Formats

Exercises may be managed and executed in several different formats.

B.3.1 Table Top

For table top exercises, all stakeholders gather in a single physical location, possibly in different teams. Each team may reflect a different stakeholder or a different organization.

B.3.2 Distributed Table Top

Distributed table top exercises may involve stakeholders in multiple locations, communicating via tele-conference, video teleconference, email, etc. There may be some separation of activities due to time zone differences. The exercise is held within a timeframe that is as narrow as possible, while ensuring that all participants can communicate and share lessons learned soon after the exercise is complete.

B.3.2 Clinical Simulation

This exercise format includes live simulation of a clinical environment such as an emergency room. Participants include clinical staff who are presented with actors simulating patient conditions needing diagnosis and treatment, possibly in the context of an emergency. However, the root cause of the patient's emergency (i.e., compromise of a medical device or cyber campaign affecting multiple systems) is unknown to the clinician 'player'. The scenario development team injects cybersecurity attacks that may manifest in a variety of ways including for example: device disabling / denial of service; manipulation of clinical data; or changing device operation. Any one of these will have a demonstrable effect on patient safety. The scenario may test at least two areas: (1) recognition by the clinical staff that a cybersecurity attack is unfolding and impacting the patient, and (2) response – how the staff treat the patient once they realize that device function is compromised. The scenario may vary widely depending on the device(s) involved in the attack.

B.3.3 Cyber Ranges/Sandboxes

A variety of participants, typically from different organizations, gather at a location that is designed to simulate an HDO environment, with a variety of connected devices. The environment may allow participants' own devices to be connected to the environment.

B.4 Resources for Developing Exercises

A number of exercise resources exist, to include those from:

- Commercial and/or non-profit organizations, such as:
  - The MITRE Corporation's *Cyber Exercise Playbook*.[55]
  - Carnegie Mellon's Software Engineering Institute's *Designing Cyber Exercises*.[56]
- DHS:
  - Homeland Security Exercise and Evaluation Program.[57]
- FBI InfraGard.

55 https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

56 http://www.dtic.mil/get-tr-doc/pdf?AD=ADA613366

57 https://preptoolkit.fema.gov/web/hseep-resources

Acronyms

Acronym	Definition
ASPR	HHS Office of the Assistant Secretary for Preparedness and Response
CCIC	Cybersecurity Communications Integration Center
CDRH	Center for Devices and Radiological Health (FDA)
CHIME	College of Healthcare Information Management Executives
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulation
CIO	Chief Information Officer
CMIO	Chief Medical Information Officer
CMS	Centers for Medicare & Medicaid Services
CONOPs	Concept of Operations
CSCSWG	Cross–Sector Cyber Security Working Group
CSF	Cyber Security Framework
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
EHNAC	Electronic Healthcare Network Accreditation Commission
EOP	Emergency Operations Plan
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FHIR	Fast Healthcare Interoperability Resources
FFRDC	Federally Funded Research and Development Center
HAN	Health Alert Network
HCC	Health Care Coalition
HCCIC	Healthcare Cyber Command Information Center
HDO	Health Delivery Organization
HHS	Department of Health and Human Services
HICS	Hospital Incident Command System
HIMSS	Healthcare Information Management and Systems Society
HIMT	Hospital Incident Management Team
HIPAA	Health Insurance Portability and Accountability Act
H–ISAC	Health Information Sharing and Analysis Center
HPH	Healthcare and Public Health
HSCC	Healthcare and Public Health Sector Coordinating Council
HVA	Hazards Vulnerability Analysis
ICS	Incident Command System
IR	Incident Response
ISAC	Information Sharing and Analysis Center

Acronym	Definition
ISAO	Information Sharing and Analysis Organization
ISO	Information Security Officer
IT	Information Technology
MDM	Medical Device Manufacturer
MDS^2	Manufacturer Disclosure Statement for Medical Device Security
NCCIC	National Cyber Command Information Center
NCCoE	National Cybersecurity Center of Excellence
NDA	Nondisclosure Agreement
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NRF	National Response Framework
OCR	Office of Civil Rights
PHI	Protected Health Information
PII	Personally Identifiable Information
POC	Point of Contact
QSR	Quality System Regulations
SBoM	Software Bill of Materials
SLA	Service Level Agreement
SLTT	State, Local, Tribal, Territorial
TRACIE	Technical Resources, Assistance Center, and Information Exchange
UCG	Unified Coordination Group
US-CERT	United States–Computer Emergency Response Team
VA	United States Department of Veterans Affairs

Glossary

Term	Definition
Advisory	Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. [CNSSI-4009]
Alert	A notification that a specific attack has been detected or directed at an organization's information systems. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Cyber Event (or Cybersecurity Event)	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). [NIST Cybersecurity Framework, Version 1.1, Draft 2]
Cyber Exercise (or Cybersecurity Exercise)	A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Exploit	A technique to breach the security of a network or information system in violation of security policy. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. [NIST SP 800-61 rev 2]
Incident Response (IR)	The activities that address the short-term, direct effects of an incident and may also support short-term recovery. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Incident Response Plan	A set of predetermined and documented procedures to detect and respond to a cyber incident. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Indicators	Technical artifacts or observables that suggest an attack is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. [NIST SP 800-150 "Guide to Cyber Threat Information Sharing"]
Mitigation	The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
NIST Cybersecurity Framework (CSF) Core Functions	The high-level constructs that characterize of an organization's cybersecurity capabilities and can be used to support cyber incident response, risk management, defensive investment, and more. [NIST Cybersecurity Framework, Version 1.1, Draft 2] **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
Preparedness	The activities to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]

Term	Definition
Recovery	The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Risk	The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Risk Assessment	The product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Risk Management	The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Significant Cyber Incident	A cyber incident that is (or a group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health safety of the American people. As it pertains to medical devices, a multi-patient attack due to the loss of authenticity, availability, integrity, and confidentiality would represent a significant cyber incident. [National Cyber Incident Response Plan]
Situational Awareness	Comprehending information about the current and developing security posture and risks, based on information gathered, observation and analysis, and knowledge or experience. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Threat	A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Vulnerability	A weakness in a system, application, or network that is subject to exploitation or misuse. [NIST SP 800-61 rev 2]