Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

Preface

Public Comment

You may submit electronic comments and suggestions at any time for Agency consideration to http://www.regulations.gov . Submit written comments to the Division of Dockets Management, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852. Identify all comments with the docket number FDA-2015-D-5105. Comments may not be acted upon by the Agency until the document is next revised or updated.

Additional Copies

CDRH
Additional copies are available from the Internet. You may also send an e-mail request to CDRH-Guidance@fda.hhs.gov to receive an electronic copy of the guidance. Please use the document number 1400044 to identify the guidance you are requesting.

CBER
Additional copies are available from the Center for Biologics Evaluation and Research (CBER), by written request, Office of Communication, Outreach, and Development (OCOD), 10903 New Hampshire Ave., Bldg. 71, Room 3128, Silver Spring, MD 20993-0002, or by calling 1-800-835-4709 or 240-402-8010, by email, ocod@fda.hhs.gov or from the Internet at http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm.

Table of Contents

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

I. Introduction

The Food and Drug Administration (FDA) is issuing this guidance to inform industry and FDA staff of the Agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices. In addition to the specific recommendations contained in this guidance, manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device[1]. A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to health and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the overall risk to health.

This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. This guidance establishes a risk-based framework for assessing when changes to medical devices for cybersecurity vulnerabilities require reporting to the Agency and outlines circumstances in which FDA does not intend to enforce reporting requirements under 21 CFR part 806. 21 CFR part 806 requires device manufacturers or importers to report promptly to FDA certain actions concerning device corrections and removals. However, the majority of actions taken by manufacturers to address cybersecurity vulnerabilities and exploits, referred to as "cybersecurity routine updates and patches," are generally considered

[1] See FDA Guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190)

to be a type of device enhancement[2] for which the FDA does not require advance notification or reporting under 21 CFR part 806. For a small subset of actions taken by manufacturers to correct device cybersecurity vulnerabilities and exploits that may pose a risk to health, the FDA would require medical device manufacturers to notify the Agency.[3] Risks to health posed by the device may result in patient harm. This guidance recommends how to assess whether the risk[4] of patient harm is sufficiently controlled or uncontrolled. This assessment is based on an evaluation of the likelihood of exploit, the impact of exploitation on the device's safety and essential performance,[5] and the severity of patient harm if exploited.

This document is not intended to provide guidance on reporting to FDA when a device has or may have caused or contributed to a death or serious injury as required by section 519 of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and the Medical Device Reporting (MDR) Regulation in 21 CFR part 803. For an explanation of the current reporting and recordkeeping requirements applicable to manufacturers of medical devices, please refer to the Medical Device Reporting for Manufacturers Guidance (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM359566).

For the current edition of the FDA-recognized standard(s) referenced in this document, see the FDA Recognized Consensus Standards Database Web site at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm .

FDA's guidance documents, including this final guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidance means that something is suggested or recommended, but not required.

II. Background

On February 19, 2013, the President issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (EO 13636; https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf), which recognized that resilient infrastructure is essential to preserving national security, economic stability, and public health and safety in the United States. EO 13636

[2] See FDA Guidance titled: "Distinguishing Medical Device Recalls from Medical Device Enhancements" (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM418469.pdf).
[3] See 21 CFR 806.10.
[4] ANSI/AAMI/ISO 14971: 2007/(R)2010: *Medical Devices – Application of Risk Management to Medical Devices,* section 2.16 – definition of risk.
[5] ANSI/AAMI ES60601-1:2005/(R)2012 and A1:2012, C1:2009/(R)2012 and A2:2010/(R)2012 (Consolidated Text) *Medical electrical equipment— Part 1: General requirements for basic safety and essential performance* (IEC 60601-1:2005, MOD), section 3.27 defines "Essential Performance" as performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk."

states that cyber threats to national security are among the most serious, and that stakeholders must enhance the cybersecurity and resilience of critical infrastructure. This includes the Healthcare and Public Health Critical Infrastructure Sector (HPH Sector). Furthermore, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21; https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil) issued on February 12, 2013 tasks Federal Government entities to strengthen the security and resilience of critical infrastructure against physical and cyber threats such that these efforts reduce vulnerabilities, minimize consequences, and identify and disrupt threats. PPD-21 encourages all public and private stakeholders to share responsibility in achieving these outcomes.

In recognition of the shared responsibility for cybersecurity, the security industry has established resources including standards, guidelines, best practices and frameworks for stakeholders to adopt a culture of cybersecurity risk management. Best practices include collaboratively assessing cybersecurity intelligence information for risks to device functionality and clinical risk. FDA believes that, in alignment with EO 13636 and PPD-21, public and private stakeholders should collaborate to leverage available resources and tools to establish a common understanding that assesses risks for identified vulnerabilities in medical devices among the information technology community, healthcare delivery organizations (HDOs), the clinical user community, and the medical device community. These collaborations can lead to the consistent assessment and mitigation of cybersecurity threats and vulnerabilities, and their impact on medical devices, ultimately reducing potential risk of patient harm.

Cybersecurity risk management is a shared responsibility among stakeholders including the medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA. FDA seeks to encourage collaboration among stakeholders by clarifying, for those stakeholders it regulates, recommendations associated with mitigating cybersecurity threats to device functionality and device users.

As stated in the FDA guidance document titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190), when manufacturers consider cybersecurity during the design phases of the medical device lifecycle, the resulting impact is a more proactive and robust mitigation of cybersecurity risks. Similarly, a proactive and risk-based approach to the postmarket phase for medical devices, through engaging in cybersecurity information sharing and monitoring, promoting "good cyber hygiene" through routine device cyber maintenance, assessing postmarket information, employing a risk-based approach to characterizing vulnerabilities, and timely implementation of necessary actions can further mitigate emerging cybersecurity risks and reduce the impact to patients.

To further aid manufacturers in managing their cybersecurity risk, the Agency encourages the use and adoption of the voluntary "Framework for Improving Critical Infrastructure Cybersecurity" (https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf) that has been developed by the National Institute of Standards and Technology (NIST) with collective input from other government agencies and the private sector.

Critical to the adoption of a proactive, rather than reactive, postmarket cybersecurity approach is the sharing of cyber risk information and intelligence within the medical device community. This information sharing can enhance management of individual cybersecurity vulnerabilities and provide advance cyber threat information to additional relevant stakeholders to manage and enhance cybersecurity in the medical device community and HPH Sector.

Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing (EO 13691; https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari), released on February 13, 2015, encourages the development of Information Sharing Analysis Organizations (ISAOs), to serve as focal points for cybersecurity information sharing and collaboration within the private sector as well as between the private sector and government. EO 13691 also mandates that the ISAO "…protects the privacy and civil liberties of individuals, that preserves business confidentiality, [and] that safeguards the information being shared…." ISAOs gather and analyze critical infrastructure information in order to better understand cybersecurity problems and interdependencies, communicate or disclose critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of cyber threats, or voluntarily disseminate critical infrastructure information to its members or others involved in the detection and response to cybersecurity issues.[6]

The ISAOs (https://www.dhs.gov/isao) are intended to be: Inclusive (groups from any and all sectors, both non-profit and for-profit, expert or novice, should be able to participate in an ISAO); Actionable (groups will receive useful and practical cybersecurity risk, threat indicator, and incident information via automated, real-time mechanisms if they choose to participate in an ISAO); Transparent (groups interested in an ISAO model will have adequate understanding of how that model operates and if it meets their needs); and Trusted (participants in an ISAO can request that their information be treated as Protected Critical Infrastructure Information (https://www.dhs.gov/pcii-program). Such information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt from regulatory use and civil litigation if the information satisfies the requirements of the Critical Infrastructure Information Act of 2002 (6 U.S.C. §§ 131 et seq.)).

The FDA Center for Devices and Radiological Health has entered into a Memorandum of Understanding with one such ISAO, the National Health Information Sharing & Analysis Center, (NH-ISAC)[7] in order to assist in the creation of an environment that fosters stakeholder collaboration and communication, and encourages the sharing of information about cybersecurity threats and vulnerabilities that may affect the safety, effectiveness, integrity, and security of the medical devices and the surrounding Health IT infrastructure.

---

[6] See Homeland Security Act (https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf), 6 U.S.C. § 212 (2002).

[7] See Memorandum of Understanding between the National Health Information Sharing & Analysis Center, Inc. (NH-ISAC), The Medical Device Innovation, Safety and Security Consortium (MDISS), and the U.S. Food and Drug Administration Center for Devices and Radiological Health (http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm524376.htm).

The Agency wishes to promote collaboration among the medical device and Health IT community to develop a shared understanding of the risks posed by cybersecurity vulnerabilities to medical devices and foster the development of a shared understanding of risk assessment to enable stakeholders to consistently and efficiently assess patient safety and public health risks associated with identified cybersecurity vulnerabilities and take timely, appropriate action to mitigate the risks. This approach will also enable stakeholders to provide timely situational awareness to the HPH community and take efforts to preemptively address the cybersecurity vulnerability through appropriate mitigation and/or remediation before it impacts the safety, effectiveness, integrity or security of medical devices and the Health IT infrastructure.

The Agency considers voluntary participation in an ISAO a critical component of a medical device manufacturer's comprehensive proactive approach to management of postmarket cybersecurity threats and vulnerabilities and a significant step towards assuring the ongoing safety and effectiveness of marketed medical devices. For companies that actively participate in such a program, and follow other recommendations in this guidance, the Agency does not intend to enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act (FD&C Act) (see Section VII).

More information about active participation in an ISAO can be found in Section IX.

III. Scope

This guidance applies to any marketed and distributed medical device including: 1) medical devices that contain software (including firmware) or programmable logic; and 2) software that is a medical device, [8] including mobile medical applications.[9] In addition, this guidance applies to medical devices that are considered part of an interoperable[10] system and to "legacy devices," i.e., devices that are already on the market or in use.

This guidance supplements the information addressed in the FDA guidance document titled "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software"

[8] Under section 201(h) of the FD&C Act, device is defined as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar related article, including a component part or accessory which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals." In addition, please note that the International Medical Device Regulators Forum (IMDRF) Software as a Medical Device (SaMD) December 9, 2013, section 5.1 defines "Software as a Medical Device" as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf).

[9] See FDA Guidance: "Mobile Medical Applications" (http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf).

[10] See FDA Guidance "Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices" (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649).

(http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm).

This guidance does not apply to investigational devices.[11]

IV. Definitions

For the purposes of this guidance, the following definitions are used:

A. Compensating Controls

A cybersecurity compensating control is a safeguard or countermeasure deployed, in lieu of, or in the absence of controls designed in by a device manufacturer. These controls are external to the device design, configurable in the field, employed by a user, and provide supplementary or comparable cyber protection for a medical device[12]. For example, a manufacturer's assessment of a cybersecurity vulnerability determines that unauthorized access to a networked medical device will most likely impact the device's safety or essential performance. However, the manufacturer determines that the device can safely and effectively operate without access to the host network, in this case the hospital network. The manufacturer instructs users to configure the network to remove the ability of unauthorized/unintended access to the device from the hospital network. This type of counter measure is an example of a compensating control.

B. Controlled Risk

Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a device's particular cybersecurity vulnerability.

C. Cybersecurity Routine Updates and Patches

Cybersecurity "routine updates and patches" are changes to a device to increase device security and/or remediate only those vulnerabilities associated with controlled risk of patient harm. These types of changes are not to reduce uncontrolled risk of patient harm, and therefore not to reduce a risk to health or to correct a violation of the FD&C Act. They include any regularly scheduled security updates or patches to a device, including upgrades to the software, firmware, programmable logic, hardware, or security of a device to increase device security, as well as updates or patches to address vulnerabilities associated with controlled risk performed earlier than their regularly scheduled deployment cycle even if they are distributed to multiple units. Cybersecurity routine updates and patches are generally considered to be a type of device enhancement that may be applied to vulnerabilities associated with controlled risk and is not considered a repair. Cybersecurity routine updates and patches may also include changes to

[11] Manufacturers may also consider applying the cybersecurity principles described in this guidance as appropriate to Investigational Device Exemption submissions and to devices exempt from premarket review.

[12] This definition is adapted from NIST Special Publication "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST SP 800-53A Rev. 4.

product labeling, including the instructions for use, to strengthen cybersecurity through increased end-user education and use of best practices. Because "cybersecurity routine updates and patches are generally considered to be device enhancements, manufacturers are generally not required to report these updates and patches as corrections under 21 CFR part 806. See Section VII for more details on reporting requirements for vulnerabilities with controlled risk. Security updates made to remediate vulnerabilities associated with a reasonable probability that use of, or exposure to, the product will cause serious adverse health consequences or death are not considered to be cybersecurity routine updates or patches.

D. Cybersecurity Signal

A cybersecurity signal is any information which indicates the potential for, or confirmation of, a cybersecurity vulnerability or exploit that affects, or could affect a medical device. A cybersecurity signal could originate from traditional information sources such as internal investigations, postmarket surveillance, or complaints, and/or security-centric sources such as CERTS (Computer/Cyber, Emergency Response/Readiness Teams), such as ICS-CERT[13], ISAOs[14], threat indicators, and security researchers. Signals may be identified within the HPH Sector. They may also originate in another critical infrastructure sector (e.g., defense, financial) but have the potential to impact medical device cybersecurity.

E. Exploit

An exploit is an instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat and could impact the safety or essential performance of a medical device or use a medical device as a vector to compromise a connected device or system.

F. Patient Harm

Harm[15] is the physical injury or damage to the health of people, or damage to property or the environment. Patient harm is defined as physical injury or damage to the health of patients, including death. Risks to health posed by the device may result in patient harm. This guidance outlines the assessment of whether the risk[16] of patient harm is sufficiently controlled or uncontrolled. This assessment is based on an evaluation of the likelihood of exploit, the impact of exploitation on the device's safety and essential performance, and the severity of patient harm if exploited (see section VI).

Other harms, such as loss of confidential information, including compromise of protected health information (PHI), are not considered "patient harms" for the purposes of this guidance.

---

[13] ICS-CERT - Industrial Control Systems Cyber Emergency Response Team

[14] *See* Department of Homeland Security, "Frequently Asked Questions about Information Sharing and Analysis Organizations (ISAOs)."

[15] ANSI/AAMI/ISO 14971: 2007/(R)2010: *Medical Devices – Application of Risk Management to Medical Devices,* section 2.2 – definition of harm.

[16] ANSI/AAMI/ISO 14971: 2007/(R)2010: *Medical Devices – Application of Risk Management to Medical Devices,* section 2.16 – definition of risk.

Nevertheless, the FDA recommends that manufacturers consider protecting the confidentiality of such information as part of their overall comprehensive risk management program. Although protecting the confidentiality of PHI is beyond the scope of this document, it should be noted that manufacturers and/or other entities, depending on the facts and circumstances, may be obligated to protect the confidentiality, integrity and availability of PHI throughout the product life cycle, including disposal, in accordance with applicable federal and state laws, including the Health Information Portability and Accountability Act (HIPAA).[17] Changes to a device that are made solely to address loss of confidentiality are typically considered to be device enhancements.

G. Remediation

Remediation is any action(s) taken to reduce an uncontrolled risk of patient harm posed by a device cybersecurity vulnerability to an acceptable level. Remediation actions may include complete solutions to remove a cybersecurity vulnerability from a medical device or compensating controls that adequately mitigate the risk (e.g., notification to customers and the user community identifying a control the user can implement). An example of remediation is a notification to the customers and the user community that discloses the vulnerability, the impact to the device, the potential for patient harm, and provides a strategy to reduce the risk of patient harm to an acceptable and controlled level. If the customer notification does not provide a strategy to reduce the risk of patient harm to an acceptable and controlled level, then the remediation is considered incomplete.

H. Threat

Threat is any circumstance or event with the potential to adversely impact the device, organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[18] Threats exercise vulnerabilities, which may impact the safety or essential performance of the device.

I. Threat Modeling

Threat modeling is a methodology for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or

[17] The HHS Office for Civil Rights enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information that covered entities or their business associates create, receive, maintain, or transmit; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. See Health information Privacy at: http://www.hhs.gov/ocr/privacy/index.html.

[18] NIST SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009. Note: Adapted from NIST definition (SP 800-53).

mitigate the effects of, threats to the system.[19] For medical devices, threat modeling can be used to strengthen security by identifying vulnerabilities and threats to a particular product, products in a product line, or from the organization's supply chain that can cause patient harm.

J. Uncontrolled Risk

Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigations.

K. Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, human behavior, or implementation that could be exploited by a threat.

V. General Principles

FDA recognizes that medical device cybersecurity is a shared responsibility among stakeholders including health care facilities, patients, providers, and manufacturers of medical devices. Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or networks to security threats. This in turn may have the potential to result in patient illness, injury or death.

Effective cybersecurity risk management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity. An effective cybersecurity risk management program should incorporate both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to obsolescence It is recommended that manufacturers apply the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond and Recover; https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf in the development and implementation of their comprehensive cybersecurity programs. Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity five core functions to management of cybersecurity in medical devices is discussed in the Appendix in greater detail.

A. Premarket Considerations

The FDA guidance document titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf) clarifies recommendations for manufacturers to address cybersecurity

[19] See "Threat Modeling" as defined in the Open Web Application Security Project (OWASP; https://www.owasp.org/index.php/Category:Threat_Modeling).

during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks. Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g). The approach should appropriately address the following elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

B. Postmarket Considerations

Because cybersecurity risks to medical devices are continually evolving, it is not possible to completely mitigate risks through premarket controls alone. Therefore, it is essential that manufacturers implement comprehensive cybersecurity risk management programs and documentation consistent with the Quality System Regulation (21 CFR part 820), including but not limited to complaint handling (21 CFR 820.198), quality audit (21 CFR 820.22), corrective and preventive action (21 CFR 820.100), software validation and risk analysis (21 CFR 820.30(g)) and servicing (21 CFR 820.200).

Cybersecurity risk management programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm. Manufacturers should respond in a timely fashion to address identified vulnerabilities. Critical components of such a program include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Maintaining robust software lifecycle processes that include mechanisms for:
    - monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle;
    - design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to Off-the-shelf software;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling
- Note: The FDA has recognized ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes;
- Using threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the cybersecurity risk;

- Adopting a coordinated vulnerability disclosure policy and practice. The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure which may be a useful resource for manufacturers; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

Postmarket cybersecurity information may originate from an array of sources including independent security researchers, in-house testing, suppliers of software or hardware technology, health care facilities, and information sharing and analysis organizations. It is strongly recommended that manufacturers participate in an ISAO that shares vulnerabilities and threats that impact medical devices. Sharing and dissemination of cybersecurity information and intelligence pertaining to vulnerabilities and threats across multiple sectors is integral to a successful postmarket cybersecurity surveillance program.

To manage postmarket cybersecurity risks for medical devices, a company should have a structured and systematic approach to risk management and quality management systems consistent with 21 CFR part 820. For example, such a program should include:

- Methods to identify, characterize, and assess a cybersecurity vulnerability.
- Methods to analyze, detect, and assess threat sources. For example:
    - A cybersecurity vulnerability might impact all of the medical devices in a manufacturer's portfolio based on how their products are developed; or
    - A cybersecurity vulnerability could exist vertically (i.e., within the components of a device) which can be introduced at any point in the supply chain for a medical device manufacturing process.

It is recommended as part of a manufacturer's cybersecurity risk management program that the manufacturer incorporate elements consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond, and Recover; https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf).

FDA recognizes that medical devices and the surrounding network infrastructure cannot be completely secured. Design, architecture, technology, and software development environment choices may result in the inadvertent incorporation of vulnerabilities. The presence of a vulnerability does not necessarily trigger patient harm concerns. Rather it is the impact of the vulnerability on the safety and essential performance of the device which may present a risk of patient harm. Vulnerabilities that do not appear to currently present a risk of patient harm should be assessed by the manufacturer for future impact.

C. Maintaining Safety and Essential Performance

Compromise of safety or essential performance of a device can result in patient harm and may require intervention to prevent patient harm.

Manufacturers should define, as part of the comprehensive cybersecurity risk management, the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria. These steps allow manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

Threat modeling is important in understanding and assessing the exploitability of a device vulnerability and potential for patient harm. Threat modeling can also be used in determining whether a proposed or implemented remediation can provide assurance that the risk of patient harm due to a cybersecurity vulnerability is reasonably controlled. Importantly, acceptable mitigations will vary depending upon the severity of patient harm that may result from exploitation of a vulnerability affecting the device. For example, a cybersecurity vulnerability affecting the temperature reading of a thermometer may have different risks than a cybersecurity vulnerability affecting the dosage of an insulin infusion pump because of the severity of patient harm.

VI. Medical Device Cybersecurity Risk Management

As part of their risk management process consistent with 21 CFR part 820, a manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls. This process should include risk analysis, risk evaluation, risk control, and incorporation of production and post-production information. Elements identified in the Appendix of this guidance should be included as part of the manufacturer's cybersecurity risk management program to support an effective risk management process. Manufacturers should have a defined process to systematically conduct a risk evaluation and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk. It is not possible to describe all hazards, associated risks, and/or controls associated with medical device cybersecurity vulnerabilities in this guidance. It is also not possible to describe all scenarios where risk is controlled or uncontrolled. Rather, FDA recommends that manufacturers define and document their process for objectively assessing the cybersecurity risk for their device(s).

As outlined below, it is recommended that such a process focus on assessing the *risk of patient harm* by considering:

1) The exploitability of the cybersecurity vulnerability, and
2) The severity of patient harm if the vulnerability were to be exploited.

Such analysis should also incorporate consideration of compensating controls and risk mitigations.

A. Assessing Exploitability of the Cybersecurity Vulnerability

Manufacturers should have a process for assessing the exploitability of a cybersecurity vulnerability. In many cases, estimating the probability of a cybersecurity exploit is very difficult due to factors such as; complexity of exploitation, availability of exploits, and exploit toolkits. In the absence of data on the probability of the occurrence of harm, conventional medical device risk management approaches suggest using a "reasonable worst-case estimate" or setting the default value of the probability to one. While these approaches are acceptable, FDA suggests that manufacturers instead consider using a cybersecurity vulnerability assessment tool or similar scoring system for rating vulnerabilities and determining the need for and urgency of the response.

One such tool, the "Common Vulnerability Scoring System," Version 3.0, for example, provides numerical ratings corresponding to high, medium and low by incorporating a number of factors in assessing exploitability including:[20]

- Attack Vector (physical, local, adjacent, network)
- Attack Complexity (high, low)
- Privileges Required (none, low, high)
- User Interaction (none, required)
- Scope (changed, unchanged)
- Confidentiality Impact (high, low, none)
- Integrity Impact (none, low, high)
- Availability Impact (high, low, none)
- Exploit Code Maturity (high, functional, proof-of-concept, unproven)
- Remediation Level (unavailable, work-around, temporary fix, official fix, not defined)
- Report Confidence (confirmed, reasonable, unknown, not defined)

In using any vulnerability scoring system (or tool), weighting of the individual factors that contribute to the composite score should be carefully considered.

Other resources that may aid in the triage of vulnerabilities are: AAMI TIR57: Principles for medical device security – Risk management[21], IEC 80001: Application of risk management for IT Networks incorporating medical devices[22], the National Vulnerability Database[23] (NVD), the Common Vulnerabilities and Exposures[24] (CVE), Common Weakness Enumeration[25] (CWE), Common Weakness Scoring System[26] (CWSS), Common Attack Pattern Enumeration and

[20] For a full description of each factor, see "Common Vulnerability Scoring System," Version 3.0: Specification Document (https://www.first.org/cvss/specification-document).
[21] AAMI TIR57: Principles for medical device security—Risk management - See more at: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729#sthash.CqfSLyu9.dpuf
[22] IEC/TR 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices
23 National Vulnerability Database (NVD; https://nvd.nist.gov/).
[24] Common Vulnerabilities and Exposures (CVE; https://cve.mitre.org/).
[25] Common Weakness Enumeration (CWE; http://cwe.mitre.org/index.html).
[26] Common Weakness Scoring System (CWSS; http://cwe.mitre.org/cwss/cwss_v1.0.1.html).

Classification[27] (CAPEC), Common Configuration Enumeration[28] (CCE) Common Platform Enumeration[29] (CPE).

B. Assessing Severity of Patient Harm

Manufacturers should also have a process for assessing the severity of patient harm, if the cybersecurity vulnerability were to be exploited. While there are many potentially acceptable approaches for conducting this type of analysis, one such approach may be based on qualitative severity levels as described in ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – Application of Risk Management to Medical Devices:

Common Term	Possible Description
Negligible:	Inconvenience or temporary discomfort
Minor:	Results in temporary injury or impairment not requiring professional medical intervention
Serious:	Results in injury or impairment requiring professional medical intervention
Critical:	Results in permanent impairment or life-threatening injury
Catastrophic:	Results in patient death

C. Evaluation of Risk of Patient Harm

A key purpose of conducting the cyber-vulnerability risk assessment is to evaluate whether the risk of patient harm is controlled (acceptable) or uncontrolled (unacceptable). One method of assessing the acceptability of risk involves using a matrix with combinations of "exploitability" and "severity of patient harm" to determine whether the risk of patient harm is controlled or uncontrolled. A manufacturer can then conduct assessments of the exploitability and severity of patient harm and then use such a matrix to assess the risk of patient harm for the identified cybersecurity vulnerabilities.

For risks that remain uncontrolled, additional remediation should be implemented.

The following figure is an example matrix that shows a possible approach to evaluate the relationship between exploitability and patient harm. It can be used to assess the risk of patient harm from a cybersecurity vulnerability as controlled or uncontrolled. While in some cases the evaluation will yield a definite determination that the situation is controlled or uncontrolled, it is possible that in other situations this determination may not be as distinct. Nevertheless, in all cases, FDA recommends that manufacturers make a binary determination that a vulnerability is either controlled or uncontrolled using an established process that is tailored to the product, its safety and essential performance, and the situation. Risk mitigations, including compensating controls, should be implemented when necessary to bring the residual risk to an acceptable level.

[27] Common Attack Pattern Enumeration and Classification (CAPEC; http://capec.mitre.org/).
[28] Common Configuration Enumeration (CCE; https://nvd.nist.gov/cce/index.cfm).
[29] Common Platform Enumeration (CPE; https://nvd.nist.gov/cpe.cfm).

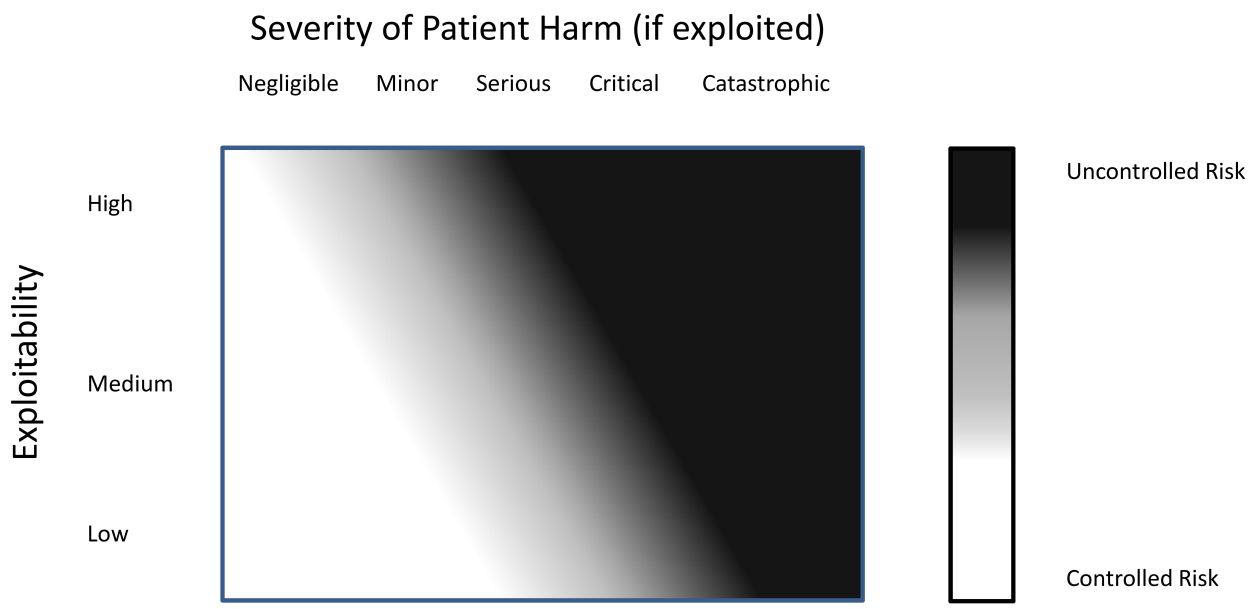

Figure – Evaluation of Risk of Patient Harm. The figure shows the relationship between exploitability and severity of patient harm, and can be used to assess the risk of patient harm from a cybersecurity vulnerability. The figure can be used to categorize the risk of patient harm as controlled or uncontrolled.

VII. Remediating and Reporting Cybersecurity Vulnerabilities

Based on the vulnerability assessment described in the previous section, the exploitability of an identified vulnerability and its severity of patient harm can help determine the risk of patient harm and can be categorized as either "controlled" (acceptable residual risk) or "uncontrolled" (unacceptable residual risk). When determining how to manage a cybersecurity vulnerability, manufacturers should incorporate already implemented compensating controls and risk mitigations into their risk assessment.

FDA encourages efficient, timely and ongoing cybersecurity risk management for marketed devices by manufacturers. For cybersecurity routine updates and patches, the FDA will, typically, not need to conduct premarket review to clear or approve the medical device software changes.[30] In addition, manufacturers should:

- Adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the initial vulnerability report to the vulnerability submitter[31,32];

[30] Premarket notification (510(k)) would be required for countermeasures that would be considered significant changes or modifications to a device's design, components, method of manufacture or intended use (See 21 CFR 807.81(a)(3)).
[31] ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure which may be a useful resource for manufacturers.

- Proactively practice good cyber hygiene, reassess risk assessments regularly, and seek opportunities to reduce cybersecurity risks even when residual risk is acceptable;
- Remediate cybersecurity vulnerabilities to reduce the risk of patient harm to an acceptable level;
- Conduct appropriate software validation under 21 CFR 820.30(g) to assure that any implemented remediation effectively mitigates the target vulnerability without unintentionally creating exposure to other risks;
- Properly document the methods and controls used in the design, manufacture, packaging, labeling, storage, installation and servicing of all finished devices as required by 21 CFR part 820;
- Identify and implement compensating controls to adequately mitigate the cybersecurity vulnerability risk, especially when new device design controls[33] may not be feasible or immediately practicable. In addition, manufacturers should consider the level of knowledge and expertise needed to properly implement the recommended control;
- Provide users with relevant information on recommended device and compensating controls and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use; and
- Recognize that some changes made to strengthen device security might also significantly affect other device functionality (e.g., use of a different operating system) and assess the scope of change to determine if additional premarket or postmarket regulatory actions are appropriate.

In addition to the general recommendations described above, Sections VII.A and VII.B. below clarify specific recommendations for managing controlled and uncontrolled risks of patient harm.[34] While FDA recognizes that multi-stakeholder engagement is necessary to fully address cybersecurity risks, the examples provided in the controlled risk and uncontrolled risk sections below clarify FDA's regulatory expectations for medical device manufacturers.

A. Controlled Risk of Patient Harm

Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to the vulnerability.

Manufacturers are encouraged to proactively promote good cyber hygiene and reduce cybersecurity risks even when residual risk is acceptable. The following are recommendations for changes or compensating control actions taken to address vulnerabilities associated with controlled risk:

[32] ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes.
[33] See 21 CFR part 820.30(g) Design controls
[34] Please note that manufacturers and user facilities may have additional reporting requirements from sources other than FDA.

- Changes to a device that are made solely to strengthen cybersecurity are typically considered device enhancements[35], which may include cybersecurity routine updates and patches, and are generally not required to be reported, under 21 CFR part 806.
- Even when risks are controlled, manufacturers may wish to deploy an additional control(s) as part of a "defense-in-depth" strategy. Typically, these changes would be considered a cybersecurity routine update or patch, a type of device enhancement;
- Device changes made solely to address a vulnerability that, if exploited, could lead to compromise of PHI, would typically be considered a cybersecurity routine update or patch;
- For premarket approval (PMA) devices with periodic reporting requirements under 21 CFR 814.84, newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of cybersecurity routine updates and patches should be reported to FDA in a periodic (annual) report. See Section VIII for recommended content to include in the periodic report.

Examples of Vulnerabilities Associated with Controlled Risk and their Management:

- A device manufacturer receives a user complaint that a gas blood analyzer has been infected with malware and there was concern that the malware may alter the data on the device. The outcome of a manufacturer investigation and impact assessment confirms the presence of malware and finds that the malware does not result in the manipulation of unencrypted data stored and flowing through the device. The device's safety and essential performance is not impacted by the malware and the manufacturer's risk assessment determines that the risk of patient harm due to the vulnerability is controlled. The device manufacturer communicates to users on how to remove the malware and decides to develop a defense-in-depth strategy; these changes would be considered a cybersecurity routine update and patch, a type of device enhancement.

- A researcher publicly discloses exploit code for a four year old vulnerability in commercial off-the-shelf database software. The vulnerable version of the software is in a percentage of the manufacturer's installed base and in two separate product lines including a multi-analyte chemistry analyzer. The manufacturer determines that the vulnerability is the result of a misconfigured database setting and could allow an unauthorized user to view patient health information in the database. The vulnerability does not permit the unauthorized user the ability to edit data in the database. Thus, the manufacturer determines the vulnerability has acceptable and controlled risk of patient harm. The manufacturer notifies their customers and the user community of the issue, details the secure configuration setting, and documents the effectiveness of the cybersecurity routine update for the configuration setting.

[35] *See* FDA guidance titled "Distinguishing Medical Device Recalls from Medical Device Enhancements" (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM418469.pdf)

- A device manufacturer is notified of an open, unused communication port by the U.S. Department of Homeland Security Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT). Subsequent analyses show that a design feature of the device prevents unauthorized remote firmware download onto the device. The threat is mitigated substantially by the need for physical access due to this device feature and the residual risk of patient harm is considered "acceptable." The manufacturer takes steps to further enhance the device's security by taking steps to close the unused communication port(s) and provide adequate communication to device users (e.g., user facilities) to facilitate the patch. If the manufacturer closes the open communication ports, the change would be considered a cybersecurity routine update or patch, a type of device enhancement. The change does not require reporting under 21 CFR part 806 (see the "Distinguishing Medical Device Recalls from Medical Enhancements Guidance" [http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm418469.pdf] for additional clarity of reporting requirements and recommendations for device enhancements).

- A device manufacturer receives a user complaint that a recent security software scan of the PC component of a class III medical device has indicated that the PC is infected with malware. The outcome of a manufacturer investigation and impact assessment confirms the presence of malware and that the primary purpose of the malware is to collect internet browsing information. The manufacturer also determines that the malware has actively collected browsing information, but that the device's safety and essential performance is not and would not be impacted by such collection. The manufacturer's risk assessment determines that the risk of patient harm due to the vulnerability is controlled. Since the risk of patient harm is controlled, the manufacturer can update the product and it will be considered a cybersecurity routine update or patch. In this case, the manufacturer does not need to report this software update to the FDA in accordance with 21 CFR 806.10. Because the device is a class III device, the manufacturer should report the changes to the FDA in its periodic (annual) report required for holders of an approved PMA under 21 CFR 814.84.

B. Uncontrolled Risk to Safety and Essential Performance

Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to insufficient risk mitigations and compensating controls. In assessing risk, manufacturers should consider the exploitability of the vulnerability and the severity of patient harm if exploited. If the risk of patient harm is assessed as uncontrolled, additional risk control measures should be applied.

Manufacturers should remediate uncontrolled risks as quickly as possible. The following are recommendations for changes or compensating control actions to address vulnerabilities associated with uncontrolled risk:

- Manufacturers should remediate the vulnerabilities to reduce the risk of patient harm to an acceptable level;

- While fixing the vulnerability may not be feasible or immediately practicable, manufacturers should identify and implement risk mitigations and compensating controls to adequately mitigate the risk;
- Customers and the user community should be provided with relevant information on recommended controls and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use;
- Manufacturers must report these vulnerabilities to the FDA according to 21 CFR part 806, unless reported under 21 CFR parts 803 or 1004[36]. However, the FDA does not intend to enforce reporting requirements under 21 CFR part 806 for specific vulnerabilities with uncontrolled risk when the following circumstances are met:
    1) There are no known serious adverse events or deaths associated with the vulnerability;
    2) As soon as possible but no later than 30 days after learning of the vulnerability, the manufacturer communicates with its customers and user community regarding the vulnerability, identifies interim compensating controls, and develops a remediation plan to bring the residual risk to an acceptable level. Controls should not introduce more risk to the device's safety and essential performance than the original vulnerability. The manufacturer must document[37] the timeline rationale for its remediation plan.[38] The customer communication should, at minimum:
        a. Describe the vulnerability including an impact assessment based on the manufacturer's current understanding,
        b. State that manufacturer's efforts are underway to address the risk of patient harm as expeditiously as possible,
        c. Describe compensating controls, if any, and
        d. State that the manufacturer is working to fix the vulnerability, or provide a defense-in-depth strategy to reduce the probability of exploit and/or severity of harm, and will communicate regarding the availability of a fix in the future.
    3) As soon as possible but no later than 60 days after learning of the vulnerability, the manufacturer fixes the vulnerability, validates the change, and distributes the deployable fix to its customers and user community such that the residual risk is brought down to an acceptable level. In some circumstances, a compensating control could produce a long-term solution provided the risk of patient harm is brought to an acceptable level. Controls should not introduce more risk to the device's safety and essential performance than the original vulnerability. Additionally, the manufacturer should follow-up with end-users as needed beyond the initial 60 day period;[39]

[36] See 21 CFR 806.10(f).
[37] See 21 CFR 820.100 Corrective action and preventive action.
[38] See 21 CFR 7.42 Recall strategy for elements of a remediation plan
[39] See 21 CFR 7 (b)(3) – Effectiveness checks.

4) The manufacturer actively participates as a member of an ISAO that shares vulnerabilities and threats that impact medical devices, such as NH-ISAC (see section IX) and provides the ISAO with any customer communications upon notification of its customers;

- Remediation of devices with annual reporting requirements (e.g., class III devices) should be included in the annual report;
- The manufacturer should evaluate the device changes to assess the need to submit a premarket submission (e.g., PMA supplement[40], 510(k), etc.) to the FDA;
- For PMA devices with periodic reporting requirements under 21 CFR 814.84, information concerning cybersecurity vulnerabilities, and the device changes and compensating controls implemented in response to this information should be reported to FDA in a periodic (annual) report. See Section VIII for recommended content to include in the periodic report.

In the absence of remediation, a device with uncontrolled risk of patient harm may be considered to have a reasonable probability that use of, or exposure to, the product will cause serious adverse health consequences or death. The product may be considered in violation of the FD&C Act and subject to enforcement or other action.

Examples of Vulnerabilities Associated with Uncontrolled Risk of Patient Harm That Must Be Remediated and Response Actions:

- A manufacturer is made aware of open, unused communication ports. The manufacturer acknowledges receipt of the vulnerability report to the submitter/identifier and subsequent analysis determines that the device's designed-in features do not prevent a threat from downloading unauthorized firmware onto the device, which could be used to compromise the device's safety and essential performance. Although there are no reported serious adverse events or deaths associated with the vulnerability, the risk assessment concludes the risk of patient harm is uncontrolled. The manufacturer communicates with its customers, the ISAO, and user community regarding the vulnerability, identifies and implements interim compensating controls, develops a remediation plan, and notifies users within 30 days of becoming aware of the vulnerability. Furthermore, within 60 days of becoming aware of the vulnerability, the manufacturer develops a more permanent solution/fix (in this case a software update to close the unused communication port(s)), validates the change, distributes the deployable fix or work around to its customers, and implements all other aspects of its remediation plan. If the manufacturer actively participates as a member of an ISAO and shares information about the vulnerability within the ISAO, FDA does not intend to enforce compliance with the reporting requirements in 21 CFR part 806. For class III devices, the manufacturer does submit a summary of the remediation as part of its periodic (annual) report to FDA.

[40] See 21 CFR 814.39, see also FDA webpage titled, "PMA Supplements and Amendments" (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm050467.htm).

- A manufacturer becomes aware of a vulnerability via a researcher that its class III medical device (e.g., implantable defibrillator, pacemaker, etc.) can be reprogrammed by an unauthorized user. If exploited, this vulnerability could result in permanent impairment, a life-threatening injury, or death. The manufacturer is not aware that the vulnerability has been exploited and determines that the vulnerability is related to a hardcoded password. The risk assessment concludes that the exploitability of the vulnerability is moderate and the risk of patient harm is uncontrolled. The manufacturer notifies appropriate stakeholders, and distributes a validated emergency patch within 60 days. The manufacturer does not actively participate as a member of an ISAO and therefore reports this action to the FDA under 21 CFR 806.10.

- A vulnerability known to the security community, yet unknown to a medical device manufacturer, is incorporated into a class II device during development. Following clearance, the manufacturer becomes aware of the vulnerability and determines that the device continues to meet its specifications, and that no device malfunctions or patient injuries have been reported. There is no evidence that the identified vulnerability has been exploited. However, it was determined that the vulnerability introduced a new failure mode to the device that impacts its essential performance, and the device's design controls do not mitigate the risk. The manufacturer conducts a risk assessment and determines that without additional mitigations, the risk of patient harm is uncontrolled. Since the manufacturer does not currently have a software update to mitigate the impact of this vulnerability on the device's essential performance, within 30 days of learning of the vulnerability the manufacturer notifies its customers, the ISAO, and user community of the cybersecurity risk and instructs them to disconnect the device from the hospital network to prevent unauthorized access to the device. The company's risk assessment concludes that the risk of patient harm is controlled with this additional mitigation. The manufacturer determines that removal of the device from the network is not a viable long-term solution and distributes a patch within 60 days of learning of the vulnerability. If the company is an active participating member of an ISAO, FDA does not intend to enforce compliance with the reporting requirement under 21 CFR part 806.

- A hospital reports that a patient was harmed after a medical device failed to perform as intended. A manufacturer investigation determines that the medical device malfunctioned as a result of exploitation of a previously unknown vulnerability in its proprietary software. The outcome of the manufacturer's investigation and impact assessment determines that the exploit indirectly impacts the device's safety and essential performance and may have contributed to a patient death. The manufacturer files a report in accordance with reporting requirements under 21 CFR part 803. The manufacturer also determines the device would be likely to cause or contribute to a serious injury or death if the malfunction were to recur; therefore, the manufacturer notifies its customers and user community, develops a validated emergency patch and files a report in accordance with 21 CFR 806.10 to notify FDA.

VIII. Recommended Content to Include in PMA Periodic Reports

For PMA devices with periodic reporting requirements under 21 CFR 814.84, information concerning cybersecurity vulnerabilities, and device changes and compensating controls implemented in response to this information should be reported to FDA in a periodic (annual) report.

It is recommended that the following information be provided for changes and compensating controls implemented for the device:

- A brief description of the vulnerability prompting the change including how the firm became aware of the vulnerability;
- A summary of the conclusions of the firm's risk assessment including whether the risk of patient harm was controlled or uncontrolled;
- A description of the change(s) made, including a comparison to the previously approved version of the device;
- The rationale for making the change;
- Reference to other submissions/devices that were modified in response to this same vulnerability;
- Identification of event(s) related to the rationale/reason for the change (e.g., MDR number(s), recall number);
- Unique Device Identification (UDI)[41] should be included, if available;
- A link to an ICS-CERT advisory or other government or ISAO alert (https://ics-cert.us-cert.gov/advisories), if applicable;
- All distributed customer notifications;
- The date and name of the ISAO to which the vulnerability was reported, if any; and
- Reference to other relevant submission (PMA Supplement[42], 30-Day Notice, 806 report, etc.), if any, or the scientific and/or regulatory basis for concluding that the change did not require a submission/report.

IX. Criteria for Defining Active Participation by a Manufacturer in an ISAO

Active participation by a manufacturer in an ISAO can assist the company, the medical device community and the HPH Sector by proactively addressing cybersecurity vulnerabilities and minimizing exploits through the timely deployment of risk control measures including communication and coordination with patients and users.

[41] See the web page titled "Unique Device Identification – UDI" http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/ for more information

[42] See 21 CFR 814.39.

FDA intends to consider the following in determining whether a manufacturer is an active participant in an ISAO:

1. The manufacturer is a member of an ISAO that shares vulnerabilities and threats that impact medical devices;
2. The ISAO has documented policies pertaining to participant agreements, business processes, operating procedures, and privacy protections;
3. The manufacturer shares vulnerability information with the ISAO, including any customer communications pertaining to cybersecurity vulnerabilities; and
4. The manufacturer has documented processes for assessing and responding to vulnerability and threat intelligence information received from the ISAO. This information should be traceable to medical device risk assessments, countermeasure solutions, and mitigations.

Manufacturers that wish to be considered by FDA to be active participants in an ISAO are recommended to maintain objective evidence documenting that they meet the four criteria above.

X. Appendix: Elements of an Effective Postmarket Cybersecurity Program

It is recommended that the following elements, consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond, and Recover; https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf), be included as part of a manufacturer's cybersecurity risk management program.

A. Identify

i. Maintaining Safety and Essential Performance

Compromise of safety or essential performance of a device can result in patient harm and may require intervention to prevent patient harm.

Manufacturers should define, as part of their comprehensive cybersecurity risk management plan, the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria. These steps allow manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

Threat modeling is important to understanding and assessing the exploitability of a device vulnerability and its potential for patient harm. Threat modeling can also be used in determining whether a proposed or implemented remediation can provide assurance that the risk of patient harm due to a cybersecurity vulnerability is reasonably controlled. Importantly, acceptable mitigations will vary depending upon the severity of patient harm that may result from exploitation of a vulnerability affecting the device. For example, a cybersecurity vulnerability affecting the temperature reading of a thermometer may have different risks than a cybersecurity vulnerability affecting the dosage of an insulin infusion pump because of the severity of patient harm.

ii. Identification of Cybersecurity Signals

Manufacturers are required to analyze complaints, returned product, service records, and other sources of quality data to identify existing and potential causes of nonconforming product or other quality problems (21 CFR 820.100). Manufacturers are encouraged to actively identify cybersecurity signals that might affect their product, and engage with the sources that report them. It is important to recognize that signals can originate from sources familiar to the medical device workspace such as internal investigations, post market surveillance and or/complaints. It is also important to recognize that cybersecurity signals may originate from cybersecurity-centric sources such as Cyber Emergency

Response Teams (CERTS), ISAOs, security researchers, or from other critical infrastructure sectors such as the Defense or Financial Sectors. Irrespective of the originating source, a clear, consistent and reproducible process for intake and handling of vulnerability information should be established and implemented by the manufacturer. FDA has recognized ISO/IEC 29147:2014, *Information Technology - Security Techniques - Vulnerability Disclosure* and ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes that may be useful resources for manufacturers. Manufacturers should develop strategies to enhance their ability to detect signals (e.g., participating in an ISAO for medical devices). Manufacturers can also enhance their postmarket detection of cybersecurity risks by incorporating detection mechanisms into their device design and device features to increase the detectability of attacks and permit forensically sound evidence capture.

B. Protect/Detect

i. Vulnerability Characterization and Assessment

The FDA recommends that manufacturers characterize and assess identified vulnerabilities because it will provide information that will aid manufacturers to triage remediation activities. When characterizing the exploitability of a vulnerability, the manufacturer should consider factors such as remote exploitability, attack complexity, threat privileges, actions required by the user, exploit code maturity, and report confidence. Scoring systems such as the "Common Vulnerability Scoring System" (CVSS)[43] provide a consistent framework for assessing exploitability by quantifying the impact of the factors that influence exploitability. See Section VI for additional guidance on vulnerability risk assessment.

ii. Risk Analysis and Threat Modeling

The FDA recommends that manufacturers conduct cybersecurity risk analyses that include threat modeling for each of their devices and to update those analyses over time. Risk analyses and threat modeling should aim to triage vulnerabilities for timely remediation. Threat modeling is a procedure for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. Threat modeling provides traditional risk management and failure mode analysis paradigms, and a framework to assess threats from active adversaries/malicious use. For each vulnerability, a summary report should be produced that concisely summarizes the risk analysis and threat modeling information. Due to the cyclical nature of the analyses, the information should be traceable to related documentation.

[43] "Common Vulnerability Scoring System," Version 3.0, Scoring Calculator (https://www.first.org/cvss/calculator/3.0).

iii. Analysis of Threat Sources[44]

The FDA recommends manufacturers to analyze possible threat sources. A threat source is defined as the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.[45] Analysis of threat sources, as part of risk analysis and threat modeling provides a framework for risk introduced by an active adversary. Therefore, characterization of threat sources will be advantageous to manufacturers in accessing risks not covered by traditional failure mode analysis methods.

iv. Incorporation of Threat Detection Capabilities

Medical devices may not be capable of detecting threat activity and may be reliant on network monitoring. Manufacturers should consider the incorporation of design features that establish or enhance the ability of the device to detect and produce forensically sound postmarket evidence capture in the event of an attack. This information may assist the manufacturer in assessing and remediating identified risks.

v. Impact Assessment on All Devices

The FDA recommends that manufacturers have a process to assess the impact of a cybersecurity signal horizontally (i.e., across all medical devices within the manufacturer's product portfolio and sometimes referred to as variant analyses) and vertically (i.e., determine if there is an impact on specific components within the device). A signal may identify a vulnerability in one device, and that same vulnerability may impact other devices including those in development, or those not yet cleared, approved or marketed. Therefore, it will be advantageous to manufacturers to conduct analyses for cybersecurity signals such that expended detection resources have the widest impact.

C. Protect/Respond/Recover

i. Compensating Controls Assessment (Detect/Respond)

- The FDA recommends that manufacturers implement device-based features, i.e. device design controls[46], as a primary mechanism to mitigate the risk of patient harm. Manufacturers should assess and provide users with compensating controls such that the risk of patient harm is further mitigated. In total, these efforts represent a defense-in-depth strategy for medical device cybersecurity. Section VII describes recommendations for

[44] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Revision 1 (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf).
[45] National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, Revision 4, Appendix B (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).
[46] See 21 CFR 820.30(g).

remediating and reporting identified cybersecurity vulnerabilities, including the development, implementation and user notification concerning fixes. Manufacturers should also adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the vulnerability to the vulnerability submitter within a specified time frame.[47,48] The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure that may be a useful resource for manufacturers.

D. Risk Mitigation of Safety and Essential Performance

Once the preceding information has been assessed and characterized, manufacturers should determine if the risk of patient harm presented by the vulnerability are adequately controlled by existing device features and/or manufacturer defined compensating controls (i.e., residual risk levels are acceptable). Actions taken should reflect the magnitude of the problem and align with the risks encountered. Manufacturers should also include an evaluation of residual risk, benefit/risk, and risk introduced by the remediation. Manufacturers should design their devices to ensure that risks inherent in remediation are properly mitigated including ensuring that the remediation is adequate and validated, that the device designs incorporate mechanisms for secure and timely updates.

Changes made for vulnerabilities of controlled risk are generally considered device enhancements, not recalls. Cybersecurity routine updates and patches are generally considered a type of device enhancement.

[47] The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure

[48] ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes