Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Document issued on: January 21, 2016

You should submit comments and suggestions regarding this draft document within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Submit electronic comments to http://www.regulations.gov. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

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. 5418, 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

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

Draft Guidance for Industry and Food and Drug Administration Staff

This draft guidance, when finalized, will represent the current thinking of the Food and Drug Administration (FDA or Agency) on this topic.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

FDA is issuing this guidance to inform industry and FDA staff of the Agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed 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. 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 the safety and effectiveness of medical devices 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 patient safety impact and the overall risk to public 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. For the majority of cases, actions taken by manufacturers to address cybersecurity vulnerabilities and exploits are considered "cybersecurity routine updates or patches," for which the FDA does not require advance notification or reporting under 21 CFR part 806. For a small subset of cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death, the FDA would require medical device manufacturers to notify the Agency.[1]

[1] *See* 21 CFR 806.10.

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 draft 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), which recognized that resilient infrastructure is essential to preserving national security, economic stability, and public health and safety in the United States. EO 13636 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) 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 their impact on medical device safety and effectiveness.

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," 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" 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), 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.[2]

The ISAOs 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. 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,

[2] *See* Homeland Security Act, 6 U.S.C. § 212 (2002).

(NH-ISAC)[3] 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.

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 voluntarily 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 VIII).

III. Scope

This guidance applies to: 1) medical devices that contain software (including firmware) or programmable logic, and 2) software that is a medical device. This guidance supplements the information addressed in the FDA guidance document titled "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software." This guidance does not apply to experimental or investigational medical devices.

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, external to the device, employed by a user in lieu of, or in the absence of sufficient controls that were designed in by a device manufacturer, and that provides supplementary or comparable cyber protection for a

[3] *See* Memorandum of Understanding between the National Health Information Sharing & Analysis Center, Inc. (NH-ISAC) and the U.S. Food and Drug Administration Center for Devices and Radiological Health.

medical device.[4] 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 essential clinical 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 that the device's essential clinical performance could be compromised by a cybersecurity vulnerability.

C. Cybersecurity Routine Updates and Patches

Cybersecurity "routine updates and patches" are updates or patches to a device to increase device security and/or remediate vulnerabilities associated with controlled risk and not to reduce a risk to health or 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 product labeling, including the instructions for use, to strengthen cybersecurity through increased end-user education and use of best practices. The concept "cybersecurity routine updates and patches" has been developed for the purpose of this guidance and are generally not required to be reported 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), ISAOs[5] and security

[4] 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.

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

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. Essential Clinical Performance

Essential clinical performance means performance that is necessary to achieve freedom from unacceptable clinical risk[6], as defined by the manufacturer. Compromise of the essential clinical performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm. The concept "essential clinical performance" has been developed for the purpose of this guidance.

F. Exploit

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

G. Remediation

Remediation is any action(s) taken to reduce the risk to the medical device's essential clinical performance to an acceptable level. Remediation actions may include complete solutions to remove a cybersecurity vulnerability from a medical device (sometimes known as official fix[7]) or compensating controls that adequately mitigate the risk (e.g., notification to customer base and user community identifying a temporary fix, or work-around). An example of remediation is a notification to the customer base and user community that discloses the vulnerability and potential impact to essential clinical performance and provides a strategy to reduce the risk to the marketed device's essential clinical performance to an acceptable level. If the customer notification does not provide a strategy to reduce the risk to the marketed device's essential clinical performance to an acceptable level, then the remediation is considered *incomplete*.

H. Threat

Threat is any circumstance or event with the potential to adversely impact the essential clinical performance of 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

[6] IEC 60601-1:2005, *Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance*, Section 3.27 defines "Essential Performance" as "performance necessary to achieve freedom from unacceptable risk." This draft guidance adapts this definition to explain "Essential Clinical Performance."

[7] "Common Vulnerability Scoring System," Version 3.0, defines "Official Fix" as "A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available."

denial of service.[8] Threats exercise vulnerabilities, which may impact the essential clinical 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 mitigate the effects of, threats to the system.[9] For medical devices, threat modeling can be used to optimize mitigations by identifying vulnerabilities and threats to a particular product, products in a product line, or from the organization's supply chain that can adversely affect patient safety.

J. Uncontrolled Risk

Uncontrolled risk is present when there is unacceptable residual risk that the device's essential clinical performance could be compromised due to insufficient compensating controls and risk mitigations.

K. Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat.[10]

V. General Principles

FDA recognizes that medical device cybersecurity is a shared responsibility between 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) in the development and implementation of their comprehensive cybersecurity programs. Alignment of the NIST Framework for Improving Critical Infrastructure

[8] 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).

[9] *See* "Threat Modeling" as defined in the Open Web Application Security Project (OWASP).

[10] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Revision 1.

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" clarifies recommendations for manufacturers to address cybersecurity 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.

For additional information see FDA guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

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).

These 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 impact patient safety. 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;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;

- Adopting a coordinated vulnerability disclosure policy and practice; 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 a cybersecurity ISAO as 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 incorporates elements consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond, and Recover).

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 safety concerns. Rather it is the impact of the vulnerability on the essential clinical performance of the device which may trigger patient safety concerns. Vulnerabilities that do not appear to currently impact essential clinical performance should be assessed by the manufacturer for future impact.

C. Defining Essential Clinical Performance

Essential clinical performance means performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer. Compromise of the essential clinical performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm.

Manufacturers should define, as part of risk management, the essential clinical performance of their device, the resulting severity outcomes if compromised, and the risk acceptance criteria. Defining essential clinical performance requirements, severity outcomes, and mapping

requirements allows manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

When defining essential clinical performance, manufacturers should consider the requirements necessary to achieve device safety and effectiveness. Understanding and defining essential clinical performance is of importance in assessing a vulnerability's impact on device performance, and in determining whether proposed or implemented remediation can provide assurance that the cybersecurity risk to the essential clinical performance is reasonably controlled. Importantly, acceptable mitigations will vary according to the device's essential clinical performance. For example, a cybersecurity vulnerability affecting the essential clinical performance of a thermometer may be quite different than a cybersecurity vulnerability affecting the essential clinical performance of an insulin infusion pump.

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 manufacturers to 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 to the device's essential clinical performance* by considering:

1) The exploitability of the cybersecurity vulnerability, and

2) The severity of the health impact to patients 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

and 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[11]:

- 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)

Other vulnerability scoring systems may also be adapted for assessing the exploitability of medical device cybersecurity vulnerabilities.

B. Assessing Severity Impact to Health

Manufacturers should also have a process for assessing the severity impact to health, 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

[11] For a full description of each factor, see "Common Vulnerability Scoring System," Version 3.0: Specification Document.

C. Evaluation of Risk to Essential Clinical Performance

A key purpose of conducting the cyber-vulnerability risk assessment is to evaluate whether the risk to essential clinical performance of the device is controlled (acceptable) or uncontrolled (unacceptable). One method of assessing the acceptability of risk to essential clinical performance is by indicating in a matrix in which combinations of "exploitability" and "severity impact to health" represent risks that are controlled or uncontrolled. A manufacturer can then conduct assessments of the exploitability and severity impact to health and then use such a matrix to assess the risk to essential clinical performance for the identified cybersecurity vulnerabilities.

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

The following figure shows a possible evaluation approach and the relationship between exploitability and impact to health. It can be used to assess the risk to the device's essential clinical performance 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 essential clinical performance, and the situation. Risk mitigations, including compensating controls, should be implemented when necessary to bring the residual risk to an acceptable level.

Figure – Evaluation of Risk to Essential Clinical Performance. The figure shows the relationship between exploitability and risk to health, and can be used to assess the risk to the device's essential clinical performance from a cybersecurity vulnerability. The figure can be used to categorize the risk to essential clinical performance 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 impact to health can help determine the extent of the compromise to the essential clinical performance of a device 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. In addition, manufacturers should:

- Proactively practice good cyber hygiene, and reduce cybersecurity risks even when residual risk is acceptable;
- Remediate cybersecurity vulnerabilities to reduce the risk of compromise to essential clinical performance 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, such as a work-around or temporary fix, to adequately mitigate the cybersecurity vulnerability risk, especially when an "official fix" may not be feasible or immediately practicable. In addition, manufacturers should consider the level of knowledge and expertise needed to properly implement the recommended fix;
- Provide users with relevant information on recommended work-arounds, temporary fixes and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use.

In addition to the general recommendations described above, Sections VII.A. and VII.B. below clarify specific recommendations for managing controlled and uncontrolled risks to essential clinical performance.[12]

[12] Please note that manufacturers and user facilities may have additional reporting requirements from sources other than FDA.

A. Controlled Risk to Essential Clinical Performance

Controlled risk is present when there is sufficiently low (acceptable) residual risk that the device's essential clinical performance could be compromised by the vulnerability.

Manufacturers are encouraged to 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:

- Changes to a device that are made solely to strengthen cybersecurity are typically considered device enhancements[13], which may include cybersecurity routine updates and patches, and are generally not required to be reported, under 21 CFR 806.10;
- 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 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 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 may not require reporting under 21 CFR part 806.

- 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 determined that the malware has actively collected browsing information, but that the device's essential clinical performance is not impacted by such collection. The manufacturer's risk assessment determines that the risk due to the vulnerability is controlled. Since essential clinical performance was not impacted, the manufacturer can update the product and it will be considered a

[13] *See* FDA guidance titled "Distinguishing Medical Device Recalls from Medical Device Enhancements."

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 Essential Clinical Performance

Uncontrolled risk is present when there is unacceptable residual risk that the device's essential clinical performance could be compromised due to insufficient risk mitigations and compensating controls. If the risk to essential clinical performance is assessed as uncontrolled, additional risk control measures should be applied.

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 compromise to essential clinical performance to an acceptable level;
- While an official fix may not be feasible or immediately practicable, manufacturers should identify and implement risk mitigations and compensating controls, such as a work-around or temporary fix, to adequately mitigate the risk;
- Manufacturers should report these vulnerabilities to the FDA according to 21 CFR part 806, unless reported under 21 CFR parts 803 or 1004. However, the FDA does not intend to enforce reporting requirements under 21 CFR part 806 if all of the following circumstances are met:
    1) There are no known serious adverse events or deaths associated with the vulnerability,
    2) Within 30 days of learning of the vulnerability, the manufacturer identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users, and
    3) The manufacturer is a participating member of an ISAO, such as NH-ISAC;
- 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, 510(k), etc.) to the FDA;
- The customer base and user community should be provided with relevant information on recommended work-arounds, temporary fixes and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use;
- 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 to its essential clinical performance 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 That Must Be Remediated and Response Actions:

- A manufacturer is made aware of open, unused communication ports. 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 essential clinical performance. Although there are no reported serious adverse events or deaths associated with the vulnerability, the risk assessment concludes the risk to the device's essential clinical performance is uncontrolled. The manufacturer develops and implements a software update to close the unused communication port(s) and notifies device users (e.g., Healthcare Delivery Organizations (HDOs)) to facilitate the remediation. The manufacturer identifies and implements compensating controls to bring the residual risk to an acceptable level and notifies users within 30 days of becoming aware of the vulnerability. The manufacturer is also a participating member of an ISAO and the manufacturer did not submit an 806 report to the Agency. For Class III devices, the manufacturer does submit a summary of the remediation as part of their periodic (annual) report to FDA. Under these circumstances, FDA does not intend to enforce the reporting requirements under 21 CFR part 806.

- 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, and cannot be mitigated by the device's design controls. The risk assessment concludes that the exploitability of the vulnerability is moderate and the risk to the device's essential clinical performance is uncontrolled. The manufacturer notifies appropriate stakeholders, and distributes a validated emergency patch. The manufacturer is not a participating member of an ISAO and 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 failures 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 essential clinical 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 to essential clinical performance is uncontrolled. Although the manufacturer does not currently have a software update to mitigate the impact of this vulnerability on the device's essential clinical performance, the manufacturer notifies the customer base 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 to essential clinical performance is controlled with this additional mitigation. If the company took this action to mitigate the risk within 30 days of learning of the vulnerability and is a 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 essential clinical performance and may have contributed to a patient death. The manufacturer notifies the customer base and user community, and develops a validated emergency patch within 30 days of learning of the vulnerability. The manufacturer is a participating member of an ISAO. Because there has been a serious adverse event or death associated with the vulnerability, the manufacturer files a report in accordance with 21 CFR 806.10 to notify FDA and complies with reporting requirements under 21 CFR part 803.

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 to essential clinical performance 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;

690 - Identification of event(s) related to the rationale/reason for the change (e.g., MDR
691 number(s), recall number);
692 - Unique Device Identification (UDI) should be included, if available;
693 - A link to an ICS-CERT advisory, if applicable;
694 - The date and name of the ISAO to which the vulnerability was reported, if any;
695 and
696 - Reference to other relevant submission (PMA Supplement[14], 30-Day Notice, 806
697 report, etc.), if any, or the scientific and/or regulatory basis for concluding that the
698 change did not require a submission/report.
699
700

[14] *See* 21 CFR 814.39.

IX. 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), be included as part of a manufacturer's cybersecurity risk management program.

A. Identify

(1) Defining Essential Clinical Performance

Essential clinical performance means performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer. Compromise of the essential clinical performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm.

Manufacturers should define the essential clinical performance of their device, the resulting severity outcomes if compromised, and the risk acceptance criteria. Defining essential clinical performance requirements, severity outcomes, and mapping requirements allows manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

When defining essential clinical performance, manufacturers should consider the requirements necessary to achieve device safety and effectiveness. Understanding and defining essential clinical performance is of importance in assessing vulnerability impact on device performance, and in determining whether proposed or implemented remediations can provide assurance that the cybersecurity risk to the essential clinical performance is reasonably controlled. Importantly, acceptable mitigations will vary according to the device's essential clinical performance. For example, mitigation for a cybersecurity vulnerability affecting the essential clinical performance of a thermometer may be quite different than a mitigation considered for an insulin infusion pump.

(2) 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 30111:2013: *Information Technology – Security Techniques – Vulnerability Handling Processes* that may be a useful resource for manufacturers. Manufacturers should develop strategies to enhance their ability to detect signals (e.g., participating in an ISAO). 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

(1) Vulnerability Characterization and Assessment

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)[15] 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.

(2) Risk Analysis and Threat Modeling

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.[16] 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.

[15] "Common Vulnerability Scoring System," Version 3.0, Scoring Calculator.
[16] *See* "Threat Modeling" as defined in the Open Web Application Security Project.

(3) Analysis of Threat Sources[17]

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[18]. 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.

(4) 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.

(5) Impact Assessment on All Devices

FDA recommends manufacturers to 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

(1) Compensating Controls Assessment (Detect/Respond)

FDA recommends manufacturers to implement device-based features as a primary mechanism to mitigate the impact of a vulnerability to essential clinical performance. Manufacturers should assess and prescribe to users, compensating controls such that the risk to essential clinical performance is further mitigated by a defense-in-depth strategy. Section VII describes recommendations for remediating and reporting identified cybersecurity vulnerabilities, including the development, implementation and user notification concerning official fixes, temporary fixes, and work-arounds. Manufacturers

[17] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Revision 1.

[18] 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.

should also adopt a coordinated vulnerability disclosure policy. FDA has recognized ISO/IEC 29147:2014: *Information Technology – Security Techniques – Vulnerability Disclosure* that may be a useful resource for manufacturers.

(2) Risk Mitigation of Essential Clinical Performance

Once the preceding information has been assessed and characterized, manufacturers should determine if the risk levels presented by the vulnerability to the essential clinical performance 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 to improve the performance or quality of a device that do not impact the essential clinical performance of the device are considered device enhancements, not recalls. Cybersecurity routine updates and patches are generally considered a type of device enhancement. For further information on distinguishing between device enhancements and recalls, see FDA guidance titled Distinguishing Medical Device Recalls from Medical Device Enhancements."