Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on April 8, 2022.

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document within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance.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

For questions about this document regarding CDRH-regulated devices, Suzanne Schwartz, Office of Strategic Partnerships and Technology Innovation at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

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

Preface

Additional Copies

CDRH

Additional copies are available from the Internet. You may also send an email request to CDRH-Guidance@fda.hhs.gov to receive a copy of the guidance. Please include the document number 1825-R1 and complete title of the guidance in the request.

CBER

Additional copies are available from the Center for Biologics Evaluation and Research (CBER), 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 https://www.fda.gov/vaccines-blood-biologics/guidance-compliance-regulatory-information-biologics/biologics-guidances.

Table of Contents

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Draft Guidance for Industry and Food and Drug Administration Staff

This draft guidance, when finalized, will represent the current thinking of the Food and Drug Administration (FDA or Agency) on this topic.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

With the increasing integration of wireless, Internet- and network- connected capabilities, portable media (e.g., USB or CD), and the frequent electronic exchange of medical device-related health information, the need for robust cybersecurity controls to ensure medical device safety and effectiveness has become more important.

In addition, cybersecurity threats to the healthcare sector have become more frequent and more severe, carrying increased potential for clinical impact. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the U.S. and globally. Such cyber attacks and exploits may lead to patient harm as a result of clinical hazards, such as delay in diagnoses and/or treatment.

Increased connectivity has resulted in individual devices operating as single elements of larger medical device systems. These systems can include health care facility networks, other devices, and software update servers, among other interconnected components. Consequently, without adequate cybersecurity considerations across all aspects of these systems, a cybersecurity threat can compromise the safety and/or effectiveness of a device by compromising the functionality of any asset in the system. As a result, ensuring device safety and effectiveness includes adequate device cybersecurity, as well as its security as part of the larger system.

For the current edition of the FDA-recognized consensus standard(s) referenced in this document, see the FDA Recognized Consensus Standards Database.[1] For more information

[1] Available at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.

regarding use of consensus standards in regulatory submissions, please refer to the FDA guidance titled "Appropriate Use of Voluntary Consensus Standards in Premarket Submissions for Medical Devices"[2] and "Standards Development and the Use of Standards in Regulatory Submissions Reviewed in the Center for Biologics Evaluation and Research."[3]

The contents of this document do not have the force of law and are not meant to bind the public in any way, unless specifically incorporated into a contract. This document is intended only to provide clarity to the public regarding existing requirements under the law. FDA's guidance documents, including this draft guidance, 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. Scope

This guidance document is applicable to devices that contain software (including firmware) or programmable logic, as well as software as a medical device (SaMD). The guidance is not limited to devices that are network-enabled or contain other connected capabilities. This guidance describes recommendations regarding the cybersecurity information to be submitted for devices under the following premarket submission types[4]:

- Premarket Notification (510(k)) submissions;
- De Novo requests;
- Premarket Approval Applications (PMAs) and PMA supplements;
- Product Development Protocols (PDPs);
- Investigational Device Exemption (IDE) submissions; and
- Humanitarian Device Exemption (HDE) submissions.

This guidance applies to all types of devices within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) whether or not they require a premarket submission. Therefore, the information in this guidance should also be considered for understanding FDA's recommendations for devices for which a premarket submission is not required (e.g., for 510(k)-exempt devices).

As IDE submissions have a different benefit-risk threshold and are not marketing authorizations, specific considerations for IDE submission documentation are provided in Appendix 3. Appendix 4 contains terminology used throughout the guidance.

III. Background

[2] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/appropriate-use-voluntary-consensus-standards-premarket-submissions-medical-devices.

[3] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/standards-development-and-use-standards-regulatory-submissions-reviewed-center-biologics-evaluation.

[4] Manufacturers should also consider applying the cybersecurity principles described in this guidance to the device constituent parts of other premarket submission types (e.g., Biologics License Applications (BLAs)) and to devices exempt from premarket review.

FDA recognizes that medical device security is a shared responsibility among stakeholders throughout the use environment of the medical device system, including health care facilities, patients, health care providers, and manufacturers of medical devices. For the purposes of this guidance, the term "medical device system" includes the device and systems such as health care facility networks, other devices, and software update servers to which it is connected.

Events across the healthcare sector have stressed the importance of cybersecurity to patient safety. The WannaCry[5] ransomware[6] affected hospital systems and medical devices across the globe. Vulnerabilities identified in commonly used third-party components, like URGENT/11[7] and SweynTooth[8], have led to potential safety concerns across a broad range of devices and clinical specialties. In 2020, a ransomware attack on a German hospital highlighted the potential impacts due to delayed patient care when a cybersecurity attack forced patients to be diverted to another hospital[9].

The FDA issued a final cybersecurity guidance addressing premarket expectations in 2014 "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," and the complementary guidance "Postmarket Management of Cybersecurity in Medical Devices" ("Postmarket Cybersecurity Guidance")[10] in 2016. However, the rapidly evolving landscape, an increased understanding of emerging threats, and the need for capable deployment of mitigations throughout the total product lifecycle (TPLC) warrants an updated, iterative approach to device cybersecurity. The changes proposed since the 2014 guidance are intended to further emphasize the importance of ensuring that devices are designed securely, are designed to be capable of mitigating emerging cybersecurity risks throughout the TPLC, and to more clearly outline FDA's recommendations for premarket submission information to address cybersecurity concerns.

One way these TPLC considerations for devices can be achieved is through the implementation and adoption of a Secure Product Development Framework (SPDF). An SPDF is a set of processes that reduce the number and severity of vulnerabilities in products throughout the device lifecycle. Examples of such frameworks exist in many device sectors including the medical device sector. The recommendations contained in this guidance document, when finalized, are intended to supplement FDA's "Postmarket Management of Cybersecurity in Medical Devices," "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf

[5] Additional information on the WannaCry Ransomware attack is available at: https://h-isac.org/wannacry-ransomware-update/.

[6] Ransomware is a type of malicious software, or malware, that infects a computer and restricts users' access to it until a ransom is paid to unlock it.

[7] The FDA Safety Communication on the URGENT/11 vulnerabilities is available at: https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce.

[8] The FDA Safety Communication on the SweynTooth vulnerabilities is available at: https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication.

[9] Additional information on the German hospital ransomware attack is available at: https://www.wired.co.uk/article/ransomware-hospital-death-germany.

[10] See FDA's guidance "Postmarket Management of Cybersecurity in Medical Devices" available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

(OTS) Software"[11] and "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices."[12] When finalized, this guidance will replace the final guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[13]

The recommendations in this guidance also generally align with or expand upon the recommendations in the Pre-Market Considerations for Medical Device Cybersecurity section of the International Medical Device Regulators Forum final guidance "Principles and Practices for Medical Device Cybersecurity," issued March 2020.[14]

IV. General Principles

This section provides general principles for device cybersecurity relevant to device manufacturers. These principles, found throughout this guidance document, are important to the improvement of device cybersecurity and, when followed, are expected to have a positive impact on patient safety.

A. Cybersecurity is Part of Device Safety and the Quality System Regulations

Device manufacturers must establish and follow quality systems to help ensure that their products consistently meet applicable requirements and specifications. These quality systems requirements are found in Quality System Regulation (QSR) in 21 CFR Part 820. Depending on the device, QS requirements may be relevant at the premarket stage, postmarket stage[15], or both.

In the premarket context, in order to demonstrate a reasonable assurance of safety and effectiveness for certain devices with cybersecurity risks, documentation outputs related to the requirements of the QSR may be one source of documentation to include as part of the premarket

[11] See FDA's guidance "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software" available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software.

[12] See FDA's guidance "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-content-premarket-submissions-software-contained-medical-devices.

[13] For the 2014 guidance on premarket submissions for management of cybersecurity, see FDA's guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0.

[14] See IMDRF Guidance "Principles and Practices for Medical Device Cybersecurity" available at http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf .

[15] In the postmarket context, QSR design controls may also be important to ensure medical device cybersecurity and maintain medical device safety and effectiveness. FDA recommends that device manufacturers implement comprehensive cybersecurity risk management programs and documentation consistent with the QSR, 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).

submission[16] See also "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" (available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-content-premarket-submissions-software-contained-medical-devices), hereafter "Premarket Software Guidance." For example, 21 CFR 820.30(a) requires that for all classes of devices automated with software, a manufacturer must establish and maintain procedures to control the design of the device in order to ensure that specified design requirements are met ("QSR design controls"). As part of QSR design controls, a manufacturer must "establish and maintain procedures for validating the devices design," which "shall include software validation and risk analysis, where appropriate." 21 CFR 820.30(g). As part of the software validation and risk analysis required by 21 CFR 820.30(g), software device manufacturers may need to establish cybersecurity risk management and validation processes, where appropriate.
Software validation and risk analyses are key elements of cybersecurity analyses and demonstrating whether a connected device has a reasonable assurance of safety and effectiveness. FDA requires manufacturers to implement development processes that account for and address cybersecurity risks as part of design controls (21 CFR 820.30). For example, these processes should address the identification of security risks, the design requirements for how the risks will be controlled, and the evidence that the controls function as designed and are effective in their environment of use for ensuring adequate security.

A Secure Product Development Framework (SPDF) may be one way to satisfy QSR requirements

Cybersecurity threats have the potential to exploit one or more vulnerabilities that could lead to patient harm. The greater the number of vulnerabilities that exist and/or are identified over time in a system in which a device operates, the easier a threat can compromise the safety and effectiveness of the medical device. A Secure Product Development Framework (SPDF) is a set of processes that help reduce the number and severity of vulnerabilities in products.[17] An SPDF encompasses all aspects of a product's lifecycle, including development, release, support, and decommission. Additionally, using SPDF processes during device design may prevent the need to re-engineer the device when connectivity-based features are added after marketing and distribution, or when vulnerabilities resulting in uncontrolled risks are discovered. An SPDF can be integrated with existing processes for product and software development, risk management, and the quality system at large.

Using an SPDF is one approach to help ensure that QSR requirements are met. Because of its benefits in helping comply with QSRs and cybersecurity, FDA encourages manufacturers to use an SPDF, but other approaches might also satisfy QSR requirements.

[16] This guidance and its recommendations are not intended to suggest that FDA will evaluate an applicant's compliance with the QSR as part of its premarket submission in our determination of a device's substantial equivalence, as this is not a requirement for premarket submissions under section 513 of the FD&C Act. This guidance is intended to explain how FDA evaluates the performance of device cybersecurity and the cybersecurity outputs of activities that are part and parcel of QSR compliance, and explain how the QSR can be leveraged to demonstrate these performance outputs

[17] While the SPDF terminology has not been used in prior FDA guidance, the concepts around secure product development and risk management align with expectations in the Quality System and Labeling Regulations. As cybersecurity continues to evolve, FDA continues to align its terminology to reflect best practices.

B. Designing for Security

FDA will assess the adequacy of the device's security based on the device's ability to provide and implement the security objectives below throughout the system architecture.

Security Objectives:

- Authenticity, which includes integrity;
- Authorization;
- Availability;
- Confidentiality; and
- Secure and timely updatability and patchability.

Premarket submissions should include information that describes how the above security objectives are addressed by and integrated into the device design. The extent to which security requirements, architecture, supply chain, and implementation are needed to meet these objectives will depend on:

- the device's intended use and indications for use;
- the presence and functionality of its electronic data interfaces;
- its intended and actual environment of use;
- the type of cybersecurity vulnerabilities present;
- the exploitability of the vulnerabilities; and
- the risk of patient harm due to vulnerability exploitation.

SPDF processes aim to reduce the number and severity of vulnerabilities and thereby reduce the exploitability of a device and the associated risk of patient harm. Because exploitation of known vulnerabilities or weak cybersecurity controls should be considered reasonably foreseeable failure modes for systems, these factors should be addressed in the device design. The benefit of following an SPDF is that a device is more likely to be secure by design, such that the device is designed from the outset to be secure within its system and/or network of use.

C. Transparency

A lack of cybersecurity information, such as information necessary to integrate the device into the use environment, as well as information needed by users to maintain the device's cybersecurity over the device lifecycle, has the potential to affect the safety and effectiveness of a device. In order to address these concerns, it is important for device users to have access to information pertaining to the device's cybersecurity controls, potential risks, and other relevant information. For example:

- insufficient information pertaining to whether a device has undisclosed cybersecurity vulnerabilities or risks may be relevant to determining whether a device's safety or effectiveness could be degraded;
- user manuals that do not include sufficient information to explain how to securely configure or update the device may limit the ability of end users to appropriately manage and protect the device; and/or

- a failure to disclose all of the communication interfaces or third-party software could fail to convey potential sources of risks.

This information and other relevant information is important in helping understand a device's cybersecurity, the threats that it may be exposed to, and how those threats may be prevented or mitigated. Without it, cybersecurity risks could be undisclosed, inappropriately identified, or inappropriately responded to, among other potential impacts, which could lead to compromises in device safety and effectiveness.

FDA believes that the cybersecurity information discussed in this guidance is important for the safe and effective use of interconnected devices and should be included in device labeling, as discussed below in Section VI.

D. Submission Documentation

Device cybersecurity design and documentation is expected to scale with the cybersecurity risk of that device. Manufacturers should take into account the larger system in which the device may be used. For example, a cybersecurity risk assessment performed on a simple, non-connected thermometer may conclude that the risks are limited, and therefore such a device needs only a limited security architecture (i.e., addressing only device hardware and software) and few security controls based on the technical characteristics and design of the device. However, if a thermometer is used in a safety-critical control loop, or is connected to networks or other devices, then the cybersecurity risks for the device are considered to be greater and more substantial design controls and documentation should be submitted in the premarket submission in order to demonstrate reasonable assurance of safety and effectiveness.

Cybersecurity risks evolve over time and as a result, the effectiveness of cybersecurity controls may degrade as new risks, threats, and attack methods emerge. As cybersecurity is part of device safety and effectiveness, cybersecurity controls should take into consideration the intended and actual use environment (see section IV). In the 510(k) context, FDA evaluates the cybersecurity information submitted and the protections the cybersecurity controls provide in demonstrating substantial equivalence.[18] See section 513(i) of the FD&C Act and 21 CFR 807.100(b)(2)(ii)(B).

In addition, inadequate cybersecurity controls may cause a device to be misbranded under section 502(f) of the FD&C Act because its labeling does not bear adequate directions for use or under section 502(j) of the FD&C Act because it is dangerous to health when used in the manner recommended or suggested in the labeling, among other possible violations.

The cybersecurity information being recommended to be included in submissions as detailed in this guidance is based on risks due to cybersecurity, not on any other criteria or level of risk/concern established in a separate FDA guidance (e.g., the software risk criteria in the Premarket Software Guidance). For example, a device that is determined to have a greater software risk may only have a small cybersecurity risk due to how the device is designed. Likewise, a device with a smaller software risk may have a significant cybersecurity risk.

[18] For more information, please refer to the guidance titled, "The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)]" regarding the substantial equivalence review standard.

Therefore, the recommendations in this guidance regarding information to be submitted to the FDA are intended to address the cybersecurity risk, as assessed by the cybersecurity risk assessment, and are expected to scale based on the cybersecurity risk. The premarket submission documentation recommendations throughout this guidance apply to all premarket submissions and are intended to be used to support FDA's assessment of a device's safety and effectiveness.

V. Using an SPDF to Manage Cybersecurity Risks

The documentation recommended in this guidance is based on FDA's experience evaluating the safety and effectiveness of devices with cybersecurity vulnerabilities. However, sponsors may use alternative approaches and provide different documentation so long as their approach and documentation satisfies premarket submission requirements in applicable statutory provisions and regulations. The increasingly interconnected nature of medical devices has demonstrated the importance of addressing cybersecurity risks associated with device connectivity in device design because of the effects on safety and effectiveness.[19] Cybersecurity risks that are introduced by threats directly to the medical device or to the larger medical device system can be reasonably controlled through using an SPDF.

The primary goal of using an SPDF is to manufacture and maintain safe and effective devices. From a security context, these are also trustworthy and resilient devices. These devices can then be managed (e.g., installed, configured, updated, review of device logs) through the device design and associated labeling by the device manufacturers and/or users (e.g., patients, health care facilities). For health care facilities, these devices may also be managed within their own cybersecurity risk management frameworks, such as the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, generally referred to as the NIST Cybersecurity Framework or NIST CSF.

FDA recommends that manufacturers use device design processes such as those described in the QSR to support secure product development and maintenance. Other frameworks that satisfy the QSR and align with FDA's recommendations for using an SPDF already exist and may be used, such as the medical device-specific framework that can be found in the Medical Device and Health IT Joint Security Plan (JSP).[20] Frameworks from other sectors may also comply with the QSR, like the framework provided in ANSI/ISA 62443-4-1: 2018 Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements.[21]

The following subsections provide recommendations for using SPDF processes which FDA believes provide important considerations for the development of devices that are safe and effective, how these processes can complement the QSR, and the documentation FDA recommends manufacturers provide for review as part of premarket submissions. The

[19] Addressing cybersecurity risks is in addition to addressing other risks, including software, biocompatibility, sterilization, and electromagnetic compatibility, among others.

[20] Medical Device and Health IT Joint Security Plan (JSP) is available at https://healthsectorcouncil.org/the-joint-security-plan/.

[21] ANSI/ISA-62443-4-1: 2018 *Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements* outlines a secure product development lifecycle similar to that of the JSP.

information in these sections do not represent a complete SPDF. In addition, FDA does not recommend that manufacturers discontinue existing, effective processes.

A. Security Risk Management

To fully account for cybersecurity risks in devices, the safety and security risks of each device should be assessed within the context of the larger system in which the device operates. In the context of cybersecurity, security risk management processes are critical because, given the evolving nature of cybersecurity threats and risks, no device is, or can be, completely secure. Security risk management should be part of a manufacturer's quality system. Specifically, the QSR requires, among other things, that manufacturers' processes address design (21 CFR 820.30), validation of the production processes (21 CFR 820.70), and corrective or preventive actions (21 CFR 820.100). These processes entail the technical, personnel, and management practices, among others, that manufacturers use to manage potential risks to their devices and ensure that their devices remain safe and effective, which includes security.

The process for performing security risk management is a distinct process from performing safety risk management as described in ISO 14971:2019. This is due to the scope of possible harm and the risk assessment factors in the context of security may be different than those in the context of safety. Also, while safety risk management focuses on physical injury or damage to property or the environment, security risk management may include not only risks that can result in patient harm but also those risks that are outside of FDA's assessment of safety and effectiveness such as those related to business or reputational risks.

Effective security risk management also addresses that cybersecurity-related failures do not occur in a probabilistic manner where an assessment for the likelihood of occurrence for a particular risk could be estimated based on historical data or modeling. This non-probabilistic approach is not the fundamental approach described in safety risk management under ISO 14971:2019. Instead, security risk assessment processes focus on exploitability, or the ability to exploit vulnerabilities present within a device and/or system. Additional discussion on exploitability assessments for the security risk assessment can be found in the FDA's Postmarket Cybersecurity Guidance.[22] Exploitability for a cybersecurity risk during a premarket assessment may be different compared to a risk assessment performed for a postmarket vulnerability. For example, some of the exploitability factors discussed in the guidance (e.g., Exploit Code Maturity, Remediation Level, Report Confidence[23]) may not be applicable to unreleased software. In these instances, a premarket exploitability assessment could either assume a worst-case assessment and implement appropriate controls, or provide a justification for a reasonable exploitability assessment of the risk throughout the total product lifecycle and how the risk is controlled.

[22] See Footnote 10.

[23] These factors of exploitability are from the Common Vulnerability Scoring System (CVSS) Version 3.0 as identified in the Postmarket Cybersecurity Guidance. Additional information on CVSS is available at https://www.first.org/cvss/.

FDA recommends that manufacturers establish a security risk management process that encompasses design controls (21 CFR 820.30), validation of production processes (21 CFR 820.70), and corrective and preventive actions (21 CFR 820.100) to ensure both safety and security risks are adequately addressed. For completeness in performing risk analyses under 21 CFR 820.30(g), FDA recommends that device manufacturers conduct both a safety risk assessment per ISO 14971:2019 and a separate, accompanying security risk assessment to ensure a more comprehensive identification and management of patient safety risks. The scope and objective of a security risk management process, in conjunction with other SPDF processes (e.g., security testing), is to expose how threats, through vulnerabilities, can manifest patient harm and other potential risks. These processes should also ensure that risk control measures for one type of risk assessment do not inadvertently introduce new risks in the other. AAMI TIR57:2016 details how the security and safety risk management processes should interface to ensure all risks are adequately assessed.[24]

Known vulnerabilities should be mitigated in the design of the device. For marketed devices, if comprehensive design mitigations are not possible, compensating controls should be considered. All devices, when any known vulnerabilities are only partially mitigated or unmitigated by the device design, they should be assessed as reasonably foreseeable risks in the risk assessment and be assessed for additional control measures or risk transfer to the user/operator, or, if necessary, the patient. Risk transfer, if appropriate, should only occur when all relevant risk information is known, assessed, and appropriately communicated to users and includes risks inherited from the supply chain as well as how risk transfer will be handled when the device/system reaches end of support and end of life and whether or how the user is able to take on that role (e.g., if the user may be a patient).

Specific security risk management documentation where FDA has recommendations regarding their scope and/or content are discussed in the subsections below. The documentation FDA recommends manufacturers provide in their premarket submissions is summarized in the Security Risk Management Documentation below (Section V.A.4.).

1. Threat Modeling

Threat modeling includes a process for identifying security objectives, risks, and vulnerabilities across the system, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system throughout its lifecycle. It is foundational for optimizing system, product, network, application, and connection security when applied appropriately and comprehensively.

With respect to security risk management, and in order to identify appropriate security risks and controls for the system, FDA recommends that threat modeling be performed to inform and support the risk analysis activities. As part of the risk assessment, FDA recommends threat modeling be performed throughout the design process and be inclusive of all system elements.

[24] AAMI TIR57:2016 Principles for medical device security—Risk management describes the security risk management process and how the security risk management process should have links into the safety risk management process and vice versa.

The threat model should:

- identify system risks and mitigations as well as inform the pre- and post-mitigation risks considered as part of the security risk assessment;
- state any assumptions about the system or environment of use (e.g. hospital networks are inherently hostile, therefore manufacturers are recommended to assume that an adversary controls the network with the ability to alter, drop, and replay packets); and
- capture cybersecurity risks introduced through the supply chain, manufacturing, deployment, interoperation with other devices, maintenance/update activities, and decommission activities that might otherwise be overlooked in a traditional safety risk assessment processes.

FDA recommends that premarket submissions include threat modeling documentation to demonstrate how the risks assessed and controls implemented for the system address questions of safety and effectiveness. There are a number of methodologies and/or combinations of methods for threat modeling that manufacturers may choose to use. Rationale for the methodology(ies) selected should be provided with the threat modeling documentation. Additional recommendations on how threat modeling documentation should be submitted to FDA are discussed in Section V.B. below.

Threat modeling activities can be performed and/or reviewed during design reviews. FDA recommends that threat modeling documentation include sufficient information on threat modeling activities performed by the manufacturer to assess and review the security features built into the device such that they holistically evaluate the device and the system in which the device operates, for the safety and effectiveness of the system.

2. Third-Party Software Components

As discussed in the FDA guidances "Off-The-Shelf (OTS) Software Use in Medical Devices"[25] and "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software,"[26] medical devices commonly include third-party software components including off-the-shelf and open source software. When these components are incorporated, security risks of the software components become factors of the overall medical device system risk management processes and documentation.

As part of demonstrating compliance with quality system design controls under 21 CFR 820.30(g), and to support supply chain risk management processes, all software, including that developed by the device manufacturer ("proprietary software") and obtained from third parties should be assessed for cybersecurity risk and that risk should be addressed. Accordingly, device

[25] See FDA guidance Off-The-Shelf (OTS) Software Use in Medical Devices available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/shelf-software-use-medical-devices.

[26] See FDA guidance Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software.

manufacturers are expected to document all software components[27] of a device and to mitigate risks associated with these software components.

In addition, under 21 CFR 820.50, manufacturers must put in place processes and controls to ensure that their suppliers conform to the manufacturer's requirements. Such information is documented in the Design History File, required by 21 CFR 820.30(j), and Design Master Record, required by 21 CFR 820.181. This documentation demonstrates the device's overall compliance with the QSR, as well as that the third-party components meet specifications established for the device. Security risk assessments that include analyses and considerations of cybersecurity risks that may exist in or be introduced by third-party software and the software supply chain may help demonstrate that manufacturers have adequately ensured such compliance and documented such history.

As part of configuration management, device manufacturers should have custodial control of source code through source code escrow and source code backups.[28] While source code is not provided in premarket submissions, if this control is not available based on the terms in supplier agreements, the manufacturer should include in premarket submissions a plan of how the third-party software component could be updated or replaced should support for the software end. The device manufacturer is also expected to provide to users whatever information is necessary to allow users to manage risks associated with the device.

One tool to help manage supply chain risk as well as clearly identify and track the software incorporated into a device is a Software Bill of Materials (SBOM), as described below.

(a) Software Bill of Materials

A Software Bill of Materials (SBOM) can aid in the management of cybersecurity risks that exist throughout the software stack. A robust SBOM includes both the device manufacturer-developed components and third-party components (including purchased/licensed software and open-source software), and the upstream software dependencies that are required/depended upon by proprietary, purchased/licensed, and open-source software. An SBOM helps facilitate risk management processes by providing a mechanism to identify devices that might be affected by vulnerabilities in the software components, both during development (when software is being chosen as a component) and after it has been placed into the market throughout all other phases of a product's life.[29]

Because vulnerability management is a critical part of a device's security risk management processes, an SBOM or an equivalent capability should be maintained as part of the device's configuration management, be regularly updated to reflect any changes to the software in

[27] The use of "component" in this guidance is consistent with the definition in 21 CFR 820.3.

[28] While some suppliers may not grant access to source code, manufacturers may consider adding to their purchasing controls acquisition of the source code should the purchased software reach end of support or end of life from the supplier earlier than the intended end of support or end of life of the medical device.

[29] For additional information see the Department of Commerce National Telecommunications and Information Administration's multi-stakeholder process for software transparency. https://www.ntia.doc.gov/SoftwareTransparency

marketed devices, and should support 21 CFR 820.30(j) (Design History File) and 820.181 (Design Master Record) documentation.

To assist FDA's assessment of the device risks and associated impacts on safety and effectiveness related to cybersecurity, FDA recommends that premarket submissions include SBOM documentation as outlined below. SBOMs can also be an important tool for transparency with users of potential risks as part of labeling as addressed later in Section VI

(b) Documentation Supporting Software Bill of Materials

FDA's guidance documents "Off-The-Shelf (OTS) Software Use in Medical Devices"[30] and "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software"[31] describe information that should be provided in premarket submissions for software components for which a manufacturer cannot claim complete control of the software lifecycle. In addition to the information recommended in those guidances, for each OTS component, the following should also be provided in a machine-readable format in premarket submissions.

A. The asset(s) where the software component resides;
B. The software component name;
C. The software component version;
D. The software component manufacturer;
E. The software level of support provided through monitoring and maintenance from the software component manufacturer;
F. The software component's end-of-support date; and
G. Any known vulnerabilities.[32]

Industry-accepted formats of SBOMs can be used to provide this information to FDA; however, if any of the above elements are not captured in such an SBOM, we recommend that those items also be provided, typically as an addendum, to FDA for the purposes of supporting premarket submission review. Additional examples of the type of information to include in a SBOM can be found in the Joint Security Plan - Appendix G ("Example Customer Security Documentation")[33] and Sections 2.3.17 and 2.3.18 of the Manufacturer Disclosure Statement for Medical Device Security (referred to as MDS2 or MDS^2)[34].

As part of the premarket submission, manufacturers should also describe how the known vulnerabilities (item (G) above) were discovered to demonstrate whether the assessment methods

[30] See FDA guidance Off-The-Shelf (OTS) Software Use in Medical Devices available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/shelf-software-use-medical-devices.

[31] See FDA guidance Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software.

[32] Known vulnerabilities are vulnerabilities that are published in the public National Vulnerability Database (NVD) or similar software vulnerability and/or weakness database. NVD is available at https://nvd.nist.gov/vuln/full-listing

[33] Medical Device and Health IT Joint Security Plan (JSP) is available at https://healthsectorcouncil.org/the-joint-security-plan/.

[34] The Manufacturer Disclosure Statement for Medical Device Security is available at https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security.

were sufficiently robust. For third-party components with known vulnerabilities, device manufacturers should provide in premarket submissions:

- A safety and security risk assessment of each known vulnerability; and
- Details of applicable safety and security risk controls to address the vulnerability. If risk controls include compensating controls, those should be described in an appropriate level of detail

For additional information and discussion regarding proprietary and third-party components, see section V.B.2., Security Architecture Views, below.

3. Security Assessment of Unresolved Anomalies

FDA's Premarket Software Guidance, recommends that device manufacturers provide a list of software anomalies (e.g., bugs or defects) that exist in a product at the time of submission. For each of these anomalies, FDA recommends that device manufacturers conduct an assessment of the anomaly's impact on safety and effectiveness, and consult the Premarket Software Guidance to assess the associated documentation recommended for inclusion in such device's premarket submission.

Some anomalies discovered during development or testing may have security implications and may also be considered vulnerabilities. As a part of ensuring a complete security risk assessment under 21 CFR Part 820.30(g), the assessment for impacts to safety and effectiveness may include an assessment for the potential security impacts of anomalies. The assessment should also include consideration of any present Common Weakness Enumeration (CWE) categories.[35] For example, a clinical user may inadvertently reveal the presence of a previously unknown software anomaly during normal use, where the impact of the anomaly might occur sporadically and be assessed to be acceptable from a software risk perspective. Conversely, a threat might seek out these types of anomalies, and identify means to exploit them in order to manifest the anomaly's impact continuously, which could significantly impact the acceptability of the risk when compared to an anomaly assessment that didn't include security considerations.

The criteria and rationales for addressing the resulting anomalies with security impacts should be provided as part of the security risk assessment documentation in the premarket submission.

4. Security Risk Management Documentation

To help demonstrate the safety and effectiveness of the device, manufacturers should provide the outputs of their security risk management processes in their premarket submissions, including their security risk management plan and security risk management report. A plan and report such

[35] Examples of SW91 defect classification mapped to CWE can be found in Annex D of AAMI's SW91 Classification of Defects in Health Software. Additional information on CWE categories can be found at https://cwe.mitre.org/.

as those described in AAMI TIR57,[36] inclusive of the system threat modeling, SBOM and associated documentation, and unresolved anomaly assessment(s) described above, should be sufficient to support the security risk management process aspect of demonstrating a reasonable assurance of safety and effectiveness.[37]

The security risk management report should:

- summarize the risk evaluation methods and processes, detail the security risk assessment, and detail the risk mitigation activities undertaken as part of a manufacturer's risk management processes; and
- provide traceability between the security risks, controls and the testing reports that ensure the device is reasonably secure.

5. TPLC Security Risk Management

Cybersecurity risks may continue to be identified throughout the device's TPLC. Manufacturers should ensure they have appropriate resources to identify, assess, and mitigate cybersecurity vulnerabilities as they are identified throughout the supported device lifecycle.

As part of using an SPDF, manufacturers should update their security risk management report as new information becomes available, such as when new threats, vulnerabilities, assets, or adverse impacts are discovered during development and after the device is released. When maintained throughout the device lifecycle, this documentation (e.g., threat modeling) can be used to quickly identify vulnerability impacts once a device is released and to support timely Corrective and Preventive Action (CAPA) activities described in 21 CFR 820.100.

Over the service life of a device, FDA recommends that the risk management documentation account for any differences in the risk management for fielded devices (e.g., marketed devices or devices no longer marketed but still in use). For example, if an update is not applied automatically for all fielded devices, then there will likely be different risk profiles for differing software configurations of the device. FDA recommends that vulnerabilities be assessed for any differing impacts for all fielded versions to ensure patient risks are being accurately assessed. Additional information as to whether a new premarket submission (e.g., PMA, PMA supplement, or 510(k)) or 21 CFR Part 806 reporting is needed based on postmarket vulnerabilities and general postmarket cybersecurity risk management are discussed in the Postmarket Cybersecurity Guidance.[38]

[36] Details on the content for security risk management plans and reports beyond those specifically identified can be found in AAMI TIR57 Principles for medical device security—Risk management.

[37] While security architecture is likely captured as a component of the security risk management process, it is discussed separately for the purposes of this guidance due to the level of detail recommended to be provided by manufacturers in order to facilitate FDA review of the safety and effectiveness of the device.

[38] See Footnote 6.

To demonstrate the effectiveness of a manufacturer's processes, FDA recommends that a manufacturer track and record the measures and metrics below[39], and report them in premarket submissions and PMA annual reports (21 CFR 814.84), when available.[40] Selecting appropriate measures and metrics for the processes that define an SPDF is important to ensure that device design appropriately addresses cybersecurity in compliance with QSR. At a minimum, FDA recommends tracking the following measures and metrics:

- Percentage of identified vulnerabilities that are updated or patched (defect density).
- Time from vulnerability identification to when it is updated or patched.
- Time from when an update or patch is available to complete implementation in devices deployed in the field.

Averages of the above measures should be provided if multiple vulnerabilities are identified and addressed. These averages may be provided over multiple time frames based on volume or in response to process or procedure changes to increase efficiencies of these measures over time.

B. Security Architecture

Manufacturers are responsible for identifying cybersecurity risks in their devices and the systems in which they expect those devices to operate, and implementing the appropriate controls to mitigate those risks. These risks may include those introduced by device reliance on hospital networks, cloud infrastructure, or "other functions" (as defined in FDA's guidance "Multiple Function Device Products: Policy and Considerations), for example.[41] FDA recommends that all medical devices provide and enforce the security objectives in Section IV, above, but recognizes that implementations to address the security objectives may vary.

A security architecture, like a system architecture, defines the system and all end-to-end connections into and/or out of the system. A security architecture definition process[42] includes both high-level definitions of the devices and/or systems that interact, and detailed information on the implementations for how those interactions occur and are secured. It contains information that demonstrates that the risks considered during the risk management process are adequately controlled, which, in turn, supports the demonstration of the safety and effectiveness of the medical device system.

[39] The measures and metrics provided are examples; alternative or additional measures and metrics may also be considered and reported.

[40] If a manufacturer has not released prior products or the premarket submission does not pertain to a marketed product (e.g., PMA supplement), FDA acknowledges that these measures and metrics might not be available, but recommends that manufacturers include these as part of their risk management plan and SPDF processes.

[41] See FDA Guidance "Multiple Function Device Products: Policy and Considerations" available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/multiple-function-device-products-policy-and-considerations.

[42] NIST 800-160v1, Systems Security Engineering states that security architecture definition process generates a set of representative security views of the system architecture to inform the selection of an appropriate security architecture. The process also ascertains vulnerability and susceptibility to disruptions, hazards, and threats.

Under 21 CFR 820.30(b), a manufacturer must establish and maintain plans that describe or reference the design and development activities and define responsibility for implementation. Such plans must be reviewed, updated, and approved as design and development evolves. 21 CFR 820.30(b). Under 21 CFR 820.30(c), a manufacturer must establish and maintain procedures to ensure that the design requirements relating to a device are appropriate and address the intended use of the device, including the needs of the user and patient. Under 21 CFR 820.30(d), a manufacturer must establish and maintain procedures for defining and documenting design output in terms that allow an adequate evaluation of conformance to design input requirements. 21 CFR 820.30(d) also states that design output procedures shall contain or make reference to acceptance criteria and shall ensure that those design outputs that are essential for the proper functioning of the device are identified.

FDA recommends that these plans and procedures include design processes, design requirements, and acceptance criteria for the security architecture of the device such that they holistically address the cybersecurity considerations for the device and the system in which the device operates.

FDA recommends that premarket submissions include documentation on the security architecture as discussed throughout this section. The objective in providing security architecture information in premarket submissions is to provide to the FDA the security context and trust-boundaries of the system in terms of the interfaces, interconnections, and interactions with external entities that the system has. The details of these elements enable the identification of the parts of the system through which attacks might be executed. Thus, as a whole, these details help to provide a sufficient understanding of the system such that FDA can evaluate adequacy of the architecture itself as it relates to safety and effectiveness.

Analysis of the entire system should be performed to understand the full environment and context in which the device is expected to operate. The security architecture should include a consideration of system-level risks, including but not limited to risks related to the supply chain (e.g., to ensure the device remains free of malware, or vulnerabilities inherited from upstream dependencies such as third-party software, among others), design, production, and deployment (i.e., into a connected/networked environment).

FDA recommends that this architecture information take the form of “views,” discussed in more detail in the following sub-sections and Appendix 2, and that these views be provided during premarket submissions to demonstrate safety and effectiveness. If the documentation identified in this section already exists in other risk management documentation, FDA does not expect manufacturers to separate out this information into new document(s); such documentation can be provided and the submission can reference the relevant sections.

Throughout this section, FDA outlines the recommended security controls and recommendations on how to document the resultant security architecture in premarket submissions through specific Security Architecture Views.

1. Implementation of Security Controls

FDA considers the way in which a device addresses cybersecurity risks and the way in which the device responds when exposed to cybersecurity threats as functions of the device design. Effective cybersecurity relies upon security being "built in" to a device, and not "bolted on" after the device is designed. FDA recommends that device manufacturers' design processes include design inputs for cybersecurity controls.[43] Under 21 CFR 820.30(c), a manufacturer must establish and maintain procedures to ensure that the design requirements relating to a device are appropriate and address the intended use of the device, including the needs of the user and patient. Under 21 CFR 820.30(d), a manufacturer must establish and maintain procedures for defining and documenting design output in terms that allow an adequate evaluation of conformance to design input requirements. These output procedures shall contain or make reference to acceptance criteria and shall ensure that those design outputs that are essential for the proper functioning of the device are identified.

FDA recommends that these procedures include design requirements and acceptance criteria for the security features built into the device such that they holistically address the cybersecurity considerations for the device and the system in which the device operates.

Security controls allow manufacturers to achieve the security objectives outlined in Section IV above and are an integral part of an SPDF. FDA recommends that an adequate set of security controls will include, but not necessarily be limited to, controls from the following categories:

- Authentication;
- Authorization;
- Cryptography;
- Code, Data, and Execution Integrity;
- Confidentiality;
- Event Detection and Logging;
- Resiliency and Recovery; and
- Updatability and Patchability.

For each of the security control categories above, specific control recommendations and implementation guidance for consideration to avoid common pitfalls are detailed in Appendix 1.

Implementation of the controls should be applied across the system architecture using risk-based determinations associated with the subject connections and devices. Without adequate security controls across the system, which include management, technical, and operational controls, there is no reasonable assurance of safety and effectiveness. Additionally, deficiencies in the design of selected security controls or the implementation of those controls can have dramatic impacts on a system's ability to demonstrate or maintain its safety and effectiveness.

[43] There are useful frameworks to use in the generation of these design inputs including the OWASP Security by design principles, AAMI/ISA-62443-4-1, as well as medical device specific frameworks including the Hippocratic Oath for Connected Medical Devices, and Building Code for Medical Device Software Security. For a specific implementation of the OWASP Security by design principles, see the Medical Device and Health IT Joint Security Plan (JSP).

FDA recommends the requirements and acceptance criteria for each of the above categories be provided in premarket submissions to demonstrate safety and effectiveness. Manufacturers should submit documentation in their premarket submissions demonstrating that the security controls for the categories above and further detailed in Appendix 1 have (1) been implemented, and (2) been tested in order to validate that they were effectively implemented (see Cybersecurity Testing section, V.C, below).

Premarket documentation submitted by manufacturers may include the demonstration of comparable or additional security controls that may not be described in Appendix 1. If using alternate controls that are not described in this document, manufacturers should provide documentation and tracing of specific design features and security controls to demonstrate that they provide appropriate levels of safety and effectiveness. As cybersecurity design controls are established early in the development phase, FDA recommends that device manufacturers utilize the FDA Q-submission process to discuss with the agency design considerations for cybersecurity risk management throughout the device lifecycle.[44] Additional information on premarket documentation recommendations for design controls are discussed in the Security Architecture Views section below.

2. Security Architecture Views

In addition to the design control requirements (i.e., 21 CFR 820.30(b), 21 CFR 820.30(c), 21 CFR 820.30(d), and 21 CFR 820.30(g)) outlined above for Security Architecture, 21 CFR 820.100 requires that manufacturers establish policies, procedures, and other plans as appropriate to identify and respond to issues in devices. FDA recommends manufacturers develop and maintain security architecture view documentation as a part of the process for the design, development and maintenance of the system. If corrective and preventive actions are identified, these views can be used to help identify impacted functionality and solutions that address the risks.

FDA recommends that premarket submissions include the architecture views described in this section. These architecture views can contribute to the demonstration of safety and effectiveness in premarket submissions by illustrating how the controls to address cybersecurity risks have been applied to the system.

The security architecture may be expressed at different levels of abstraction and with different scopes or views.[45] The number and extent of the architecture views provided in the submission will be dependent on the attack surface(s) identified through threat modeling and risk assessments for the device. These views can therefore be an effective way to communicate the threat model to FDA and will naturally scale the documentation provided with the cybersecurity risk of the device.

[44] For more information, see FDA's guidance entitled "Request for Feedback on Medical Device Submissions: The Q-Submission Program," available athttps://www.fda.gov/regulatory-information/search-fda-guidance-documents/requests-feedback-and-meetings-medical-device-submissions-q-submission-program.

[45] Architecture view is defined by NIST 800-160v1 as "A work product expressing the architecture of a system from the perspective of specific system concerns."

FDA recommends providing, at minimum, the following types of views in premarket submissions:

- Global System View;
- Multi-Patient Harm View;
- Updateability/Patchability View; and
- Security Use Case View(s).

Documenting these views should include both diagrams and explanatory text. These diagrams and explanatory text should contain sufficient details to permit an understanding of how the assets within the system function holistically within the associated implementation details. For the security architecture views, manufacturers should consider the information outlined in Appendix 2 when determining the level of detail to include in premarket submissions.

These security architecture views should:

- Identify security-relevant system elements and their interfaces;
- Define security context, domains, boundaries, and external interfaces of the system;
- Align the architecture with (a) the system security objectives and requirements, (b) security design characteristics; and
- Establish traceability of architecture elements to user and system security requirements.

The extent of these security views in a premarket submission is expected to vary based on the architecture and potential cybersecurity risk posed to the device. For example, systems with network and/or cloud access would be expected to have more Security Use Case Views than a system that only has a USB interface.

(a) Global System View

A global system view should describe the overall system, including the device itself and all internal and external connections. For interconnected and networked devices, this view should identify all interconnected elements, including any software update infrastructure(s), health care facility network impacts, intermediary connections or devices, cloud connections, etc.

Depending on the complexity of the system, it may not be feasible to include all data flow specifics in a singular global system view. Additional views can be provided that detail the communication specifics as identified in Appendix 2 and do not need to be duplicated if captured in one of the other types of views detailed below.

(b) Multi-Patient Harm View

When devices are capable of connecting (wired or wirelessly) to another medical or non-medical product, to a network, or to the Internet, there is the possibility that multiple devices can be compromised simultaneously. Because of that connectivity, if a device is compromised, or if a non-device function (i.e., any function that does not fall within section 201(h) of the

FD&C Act) that could impact the device function is compromised, the device may introduce a safety risk to patients through security risk. This may change the device's intended use. For example, a non-device function could be hacked to perform a device function and ultimately harm patients.

Depending on the device risk and use environment, a multiple-device compromise may have severe impacts for multiple patients, either through impact to the device itself and/or to health care facility operations (e.g., multiparameter bedside monitors all restarting at once, leaving all monitors connected to the same network no longer monitoring patient vitals and staffing levels not able to monitor all patient vitals).

FDA recommends that manufacturers address how their device(s) and system(s) defend against and/or respond to attacks with the potential to harm multiple patients in a multi-patient harm view. This view should include the information outlined in Appendix 2. These risks, once identified, may also need to be assessed differently in the accompanying cybersecurity risk assessment due to the different nature of the risk.

(c) Updatability and Patchability View

With the need to provide timely, reliable updates to devices in order to address emerging cybersecurity risks throughout the total product lifecycle of the device, FDA recommends manufacturers provide an updateability and patchability view. This view should describe the end-to-end process that permits software updates and patches to be provided (deployed) to the device, and should include detailed information as outlined in Appendix 2.

For example, if a device manufacturer intends to push software from a software update server to an in-clinic cardiac implant programmer, "end-to-end" means the path from the update server to the in-clinic programmer. The software update path will likely include traversing technology that the device manufacturer does not control, and therefore the design should provide for the protection of the end-to-end path and take into account any additional cybersecurity risk created or posed by those non-manufacturer-controlled technologies.

(d) Security Use Case Views

In addition to the views identified above, security use case views should also be provided. Security use cases should be included for all system functionality through which a security compromise could impact the safety or effectiveness of the device. These security use cases should cover various operational states of elements in the system (e.g., power on, standby, transition states, etc.) and assess clinical functionality states of the system (e.g., programming, alarming, delivering therapy, send/receive data, reporting diagnostic results, etc.).

The number of security use cases that should be assessed will scale with the cybersecurity complexity and risk of the device. Each view should include detailed information as outlined in Appendix 2. For use cases identified that share the same security assessment, the associated diagrams and explanatory text can describe the multiple use cases covered by the view in lieu of providing duplicative information in multiple places. For example, programming commands and sending/receiving device data may share the same communication protocol and therefore may not exhibit differences between the security views for both scenarios, despite having different clinical risk assessments.

C. Cybersecurity Testing

As with other areas of product development, testing is used to demonstrate the effectiveness of design controls. While software development and cybersecurity are closely related disciplines, cybersecurity controls require testing beyond standard software verification and validation activities to demonstrate the effectiveness of the controls in a proper security context to therefore demonstrate that the device has a reasonable assurance of safety and effectiveness.

Under 21 CFR 820.30(f), a manufacturer must establish and maintain procedures for verifying the device design. Such verification shall confirm that the design output meets the design input requirements. Under 21 CFR 820.30(g), a manufacturer must establish and maintain procedures for validating its device design. Such design validation shall include software validation and risk analysis, where appropriate. FDA recommends verification and validation include sufficient testing performed by the manufacturer on the cybersecurity of the system through which the manufacturer verifies and validates their inputs and outputs, as appropriate.

Security testing documentation and any associated reports or assessments should be submitted in the premarket submission. FDA recommends that the following types of testing, among others, be provided in the submission:

a. Security requirements
    - Manufacturers should provide evidence that each design input requirement was implemented successfully.
    - Manufacturers should provide evidence of their boundary analysis and rationale for their boundary assumptions.

b. Threat mitigation
    - Manufacturers should provide details and evidence of testing that demonstrates effective risk control measures according to the threat models provided in the system, use case, and call-flow views.
    - Manufacturers should ensure the adequacy of each cybersecurity risk control (e.g., security effectiveness in enforcing the specified security policy, performance for maximum traffic conditions, stability and reliability, as appropriate).

c. Vulnerability Testing (such as section 9.4 of ANSI/ISA 62443-4-1)

- Manufacturers should provide details and evidence[46] of the following testing pertaining to known vulnerabilities:
  - Abuse case, malformed, and unexpected inputs,
    - Robustness
    - Fuzz testing
  - Attack surface analysis,
  - Vulnerability chaining,
  - Closed box testing of known vulnerability scanning,
  - Software composition analysis of binary executable files, and
  - Static and dynamic code analysis, including testing for credentials that are "hardcoded," default, easily-guessed, and easily compromised.

d. Penetration testing

- The testing should identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product. Penetration test reports should be provided and include the following elements:
  - Independence and technical expertise of testers,
  - Scope of testing,
  - Duration of testing,
  - Testing methods employed, and
  - Test results, findings, and observations.

Device manufacturers should indicate in the test reports where the testing was performed, and what level of independence those responsible for testing devices have from the developers responsible for designing devices. In some cases, it may be necessary to use third parties to ensure an appropriate level of independence between the two groups, such that vulnerabilities or other issues revealed during testing are appropriately addressed. For any third party test reports, manufacturers should provide the original third party report. For all testing, manufacturers should provide their assessment of any findings including rationales for not implementing or deferring any findings to future releases.

As identified in Sections V.A.2. and V.A.3. above, vulnerabilities and anomalies identified during testing should be assessed for their security impacts as part of the security risk management process. In non-security software testing, a benefit analysis of a discovered defect may lead to the conclusion that an anomaly does not need to be fixed, as its impact on system functionality may be small or unlikely. Conversely, in security testing, the exploitability of an anomaly may necessitate that it is mitigated because of the greater, and different type of, harm that it could facilitate.

For issues that will be addressed in future releases (i.e., remediation deferred for a future software release because current risk was assessed to be acceptable), the plans for those releases should be detailed in the premarket submission to include the vulnerabilities that future software releases will address, anticipated timelines for release, whether devices released in the interim will receive those updates, and how long it will take the update to reach the devices.

[46] For any testing tools or software used, the details provided may include, but may not be limited to, the name of the tool, version information as applicable, and any settings or configuration options for the tools used.

There are numerous authoritative resources for outlining security testing that may partially fulfill the testing outlined above.[47] FDA recommends that cybersecurity testing should occur throughout the SPDF. Security testing early in development can ensure that security issues are addressed prior to impacting release timelines and can prevent the need to redesign or re-engineer the device. After release, cybersecurity testing should be performed at regular intervals (e.g., annually) to ensure that potential vulnerabilities are identified and able to be addressed prior to their ability to be exploited.

VI. Cybersecurity Transparency

In order for users to manage security risks in devices, either by an end user or within a larger risk management framework like the NIST CSF, transparency is critical to ensure safe and effective use and integration of devices and systems. This transparency can be conveyed through both labeling and the establishment of vulnerability management plans. However, different types of users (e.g., manufacturers, servicers, patients, etc.) will have different abilities to take on a mitigation role, and the need for actions to ensure continued cybersecurity should be appropriate for the type of user.

A. Labeling Recommendations for Devices with Cybersecurity Risks

FDA regulates device labeling in several ways. For example, section 502(f) of the FD&C Act requires that labeling include adequate directions for use. Under section 502(a)(1) of the FD&C Act, a medical device is deemed misbranded if its labeling is false or misleading in any particular.

For devices with cybersecurity risks, informing users of relevant security information may be an effective way to comply with labeling requirements relating to such risks. FDA also believes that informing users of security information through labeling may be an important part of QSR design controls to help mitigate cybersecurity risks and help ensure the continued safety and effectiveness of the device. Therefore, when drafting labeling for inclusion in a premarket submission, a manufacturer should consider all applicable labeling requirements and how informing users through labeling may be an effective way to manage cybersecurity risks and/or to ensure the safe and effective use of the device. Any risks transferred to the user should be detailed and considered for inclusion as tasks during usability testing (e.g., human factors testing[48]) to ensure that the type of user has the capability to take appropriate actions to manage those risks-.

[47] The following standards may partially meet the security testing recommendations in ANSI/UL 2900 Software Cybersecurity for Network-Connectable Products and ANSI/ISA-62443-4-1-2018 Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements. Additional standards may also meet or partially meet the testing recommendations outlined in this section.

[48] See FDA Guidance "Applying Human Factors and Usability Engineering to Medical Devices" available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/applying-human-factors-and-usability-engineering-medical-devices

The recommendations below aim to communicate to users relevant device security information that may enable their own ongoing security posture, thereby helping ensure a device remains safe and effective throughout its lifecycle. The depth of detail, the exact location in the labeling for specific types of information (e.g., operator's manual, security implementation guide), and the method to provide this information should account for the intended user of the information. Instructions to manage cybersecurity risks should be understandable to the intended audience, which might include patients or caregivers with limited technical knowledge. The manufacturer may wish to employ methods to ensure certain information is available only to the user, and if it does so through an online portal, should provide an up-to-date link.[49]

FDA recommends the following be included in labeling to communicate relevant security information to users.[50]

1. Device instructions and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., anti-malware software, use of a firewall, password requirements).

2. Sufficiently detailed diagrams for users that allow recommended cybersecurity controls to be implemented.

3. A list of network ports and other interfaces that are expected to receive and/or send data. This list should include a description of port functionality and indicate whether the ports are incoming, outgoing, or both, along with approved destination end-points.

4. Specific guidance to users regarding supporting infrastructure requirements so that the device can operate as intended (e.g., minimum networking requirements, supported encryption interfaces).

5. A SBOM as specified in Section V.A.2.b or in accordance with an industry accepted format to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the device (and the connected system), and to deploy countermeasures to maintain the device's safety and effectiveness. Manufacturers should provide or make available SBOM information to users on a continuous basis. If an online portal is used, an up-to-date link should be provided. The SBOM should be in a machine readable format.

6. A description of systematic procedures for users to download version-identifiable manufacturer-authorized software and firmware, including a description of how users will know when software is available.

[49] For more information regarding FDA's policy on labeling changes and submission requirements, manufacturers can use the FDA Guidance Search Tool to identify relevant guidance documents for their product and submission type. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/.

[50] See IEC TR 80001-2-2 and IEC TR 80001-2-8 and IEC TR 80001-2-9 for further labeling information for compliance with these standards.

7. A description of how the design enables the device to respond when anomalous conditions are detected (i.e., security events) in order to maintain safety and effectiveness. This should include notification to the user and logging of relevant information. Security event types could be configuration changes, network anomalies, login attempts, or anomalous traffic (e.g., send requests to unknown entities).

8. A high-level description of the device features that protect critical functionality (e.g., backup mode, disabling ports/communications, etc.).

9. A description of backup and restore features and procedures to restore authenticated configurations.

10. A description of the methods for retention and recovery of device configuration by an authenticated authorized user.

11. A description of the secure configuration of shipped devices, a discussion of the risk tradeoffs that might have been made about hardening options implemented by the device manufacturer, and instructions for user-configurable changes. Secure configurations may include end point protections such as anti-malware, firewall/firewall rules, allow lists, deny lists, security event parameters, logging parameters, and physical security detection, among others.

12. Where appropriate for the intended use environment, a description of how forensic evidence is captured, including but not limited to any log files kept for a security event. Log file descriptions should include how and where the log file is located, stored, recycled, archived, and how it could be consumed by automated analysis software (e.g., Intrusion Detection System, IDS).

13. Where appropriate, technical instructions to permit secure network deployment and servicing, and instructions for users on how to respond upon detection of a cybersecurity vulnerability or incident.

14. Information, if known or anticipated, concerning device cybersecurity end of support and end of life. At the end of support, a manufacturer may no longer be able to reasonably provide security patches or software updates. If the device remains in service following the end of support, the manufacturer should have a pre-established and pre-communicated process for transferring the risks highlighting that the cybersecurity risks for end-users can be expected to increase over time.

15. Information on securely decommissioning devices by sanitizing the product of sensitive, confidential, and proprietary data and software.

A revision-controlled, Manufacturer Disclosure Statement for Medical Device Security (MDS2) and Customer Security Documentation as outlined in the HSCC Joint Security Plan (JSP) may address a number of the above recommendations.

B. Vulnerability Management Plans

Recognizing that cybersecurity risks evolve as technology evolves throughout a device's TPLC, FDA recommends that manufacturers establish a plan for how they will identify and communicate vulnerabilities that are identified after releasing the device with users. This plan can also support risk management processes in accordance with 21 CFR 820.30(g) and corrective and preventive action processes in accordance with 21 CFR 820.100.

FDA recommends that manufacturers submit their vulnerability communication plans as part of their premarket submissions so that FDA can assess whether the manufacturer has sufficiently addressed how to maintain the safety and effectiveness of the device after marketing authorization is achieved.

Vulnerability communication plans should include the following elements:

a) Personnel responsible;
b) Sources, methods, and frequency for monitoring for and identifying vulnerabilities (e.g., researchers, NIST NVD, third-party software manufacturers, etc.);
c) Periodic security testing to test identified vulnerability impact;
d) Timeline to develop and release patches;
e) Update processes;
f) Patching capability (i.e., rate at which update can be delivered to devices);
g) Description of their coordinated vulnerability disclosure process; and
h) Description of how manufacturer intends to communicate forthcoming remediations, patches, and updates to customers.

Additional recommendations on coordinated vulnerability disclosure plans may be found in FDA's Postmarket Cybersecurity Guidance.[51]

[51] See Footnote 10.

Appendix 1. Security Control Categories and Associated Recommendations

The following sections provide detailed descriptions of each of the security control categories introduced in Section V.B.1. as well as specific recommendations for security controls and their implementation to avoid common pitfalls.

A. Authentication

There are generally two types of authentication controls—information and entities—and a properly-secured system is able to prove the existence of both.

Authentication of *information*[52] exists where the device and the system in which it operates is able to prove that information originated at a known and trusted source, and that the information has not been altered in transit between the original source and the point at which authenticity is verified. It is important to note that while authenticity implies that data is accurate and has been safeguarded from unauthorized user modification (i.e., integrity), integrity alone does not provide assurance that the data is real and came from a trusted source. Therefore, for the purposes of this guidance, authentication is discussed as a larger security objective over integrity.

Authentication of *entities* exists where a device and the system in which it operates is able to prove the identity of an endpoint (whether hardware and/or software) from which it is sending and/or receiving information, or authorized user/operator at that endpoint.

As part of normal operations within a secure system, devices are expected to verify the authenticity of information from external entities, as well as prove the authenticity of information that they generate. A system that appropriately accounts for authenticity will evaluate and ensure authenticity for: (1) information at rest (stored); (2) information in transit (transmitted); (3) entity authentication of communication endpoints, whether those endpoints consist of software or hardware; (4) software binaries; (5) integrity of the execution state of currently running software; and (6) any other appropriate parts of the system where a manufacturer's threat model and/or risk analyses reveal the need for it.

On a technical level, the strength of a device's authentication scheme is defined by the amount of effort, including time, that an unauthorized party would need to expend to identify the decomposition of the authentication scheme. For example, this could be the time and resources necessary to determine the correct "output" of a cryptographic function from which a cryptographically-based authentication scheme is built and which an unauthorized party could use to bypass the authentication scheme and gain access to the system.

When choosing an authentication scheme, manufacturers should keep in mind the following generally applicable characteristics of different types of schemes. Implicit authentication

[52] For the purposes of this control, "information" includes the software/firmware itself, as well as input and output data.

schemes, based solely on non-cryptographic interfaces, handshakes, and/or protocols, are inherently weak because, once they are reverse-engineered, an unauthorized user can easily emulate the correct behavior and appear to be authorized. Cryptographic authentication protocols are generally superior, but they need careful design choices and implementation practices to achieve their full strength. In addition, these schemes are still limited by the confidentiality of the cryptographic keys needed to interact with the scheme, and by the integrity of the devices that hold or otherwise leverage those keys (see the cryptography subsection below). Therefore, for device operations where non-authenticated behavior could lead to harm, devices should implement additional, non-routine signals of intent based on physical actions, such as a momentary switch, to authorize the command/session.

The following list provides additional recommendations for the implementation of authentication schemes:

- Use cryptographically strong[53] authentication, where the authentication functionality resides on the device, to authenticate personnel, messages, commands updates, and as applicable, all other communication pathways. Hardware-based security solutions should be considered and employed when possible;
- Authenticate external connections at a frequency commensurate with the associated risks. For example, if a device connects to an offsite server, then the device and the server should mutually authenticate each session and limit the duration of the session, even if the connection is initiated over one or more existing trusted channels;
- Use appropriate user authentication (e.g., multi-factor authentication to permit privileged device access to system administrators, service technicians, or maintenance personnel, among others, as needed);
- Require authentication, and permission in certain instances, before permitting software or firmware updates, including those updates affecting the operating system, applications, and anti-malware functionality;
- Strengthen password protections. Do not use passwords that are hardcoded, default, easily-guessed, or easily compromised (e.g., passwords that are the same for each device; unchangeable; can persist as default; difficult to change; and/or vulnerable to public disclosure);
- Implement anti-replay measures in critical communications such as potentially harmful commands. This can be accomplished with the use of cryptographic nonces (an arbitrary number used only once in a cryptographic communication);
- Provide mechanisms for verifying the authenticity of information originating from the device, such as telemetry. This is especially important for data that, if spoofed or otherwise modified, could result in patient harm, such as the link between a continuous glucose monitor (CGM) system and an automated insulin pump;
- Do not rely on cyclic redundancy checks (CRCs) as security controls. CRCs do not provide integrity or authentication protections in a security environment. While CRCs are an error detecting code and provide integrity protection against environmental factors (e.g., noise or EMC), they do not provide protections against an intentional or malicious actor; and

[53] See the definition of security strength in Appendix 4, Terminology.

- Consider how the device and/or system should respond in event of authentication failure(s).

B. Authorization

For the purposes of this guidance, authorization is the right or permission that is granted to a system entity (e.g., a device, server, or software function) to access a system resource. More specifically, as a defensive measure, an authorization scheme enforces privileges, i.e. "rights," associated with authenticated sessions, identities and/or roles. These privileges either permit allowed behavior, or refuse disallowed behavior in order to ensure that system resources are only accessed in accepted ways, by accepted parties.

Within an adequately designed authorization scheme, the principle of least privileges[54] should be applied to users, system functions, and others, to only allow those entities the levels of system access necessary to perform a specific function.

For example, in a situation in which a malicious actor has gained access to a credential associated with patient privileges, that malicious actor should not be able to access device resources or functionality reserved for the manufacturer or for the health care provider, such as device maintenance routines or the ability to change medication dosage amounts.

While authentication schemes based on cryptographically-proven designs are generally considered more robust and are therefore preferred, meaningful authorization checks can be performed based on other compelling evidence (e.g., benefit/risk assessment in accordance with Section 6.5 of AAMI TIR57 and associated supporting justification and as evidenced through security testing). For example, a medical device programmer that is capable of Near-Field Communications (NFC) could have elevated privileges that are granted based on a signal of intent[55] over NFC that cannot physically be produced by another unauthorized device over Radio-Frequency (RF) (e.g., a home monitor).

The following list provides recommended design implementations for an authorization scheme:

- Limit authorized access to devices through the authentication of users (e.g., user ID and password, smartcard, biometric, certificates, or other appropriate authentication method);
- Use automatic timed methods to terminate sessions within the system where appropriate for the use environment;
- Employ an authorization model that incorporates the principle of least privileges by differentiating privileges based on the user role (e.g., caregiver, patient, health care provider, system administrator) or device functions; and
- Design devices to "deny by default" (i.e., that which is not expressly permitted by a device is denied by default). For example, the device should generally reject all unauthorized connections (e.g., incoming TCP, USB, Bluetooth, serial connections). Ignoring requests is one form of denying authorization.

[54] CNSSI 4009-2015 defines least privilege as "The principle that a security architecture should be designed so that each entity (e.g., user, asset) is granted the minimum system resources and authorizations that the entity needs to perform its function."

[55] Signal of intent in this use is specific to the implementation of NFC communications.

C. Cryptography

Cryptographic algorithms and protocols are recommended to be implemented to achieve the secure by design objectives outlined in Section IV. While high-quality, standardized cryptographic algorithms and protocols are readily available, several commercial products that include cryptographic protections have been shown to have exploitable vulnerabilities due to improper configurations and/or implementations.

While other sections of this guidance reference cryptographic controls, the following recommendations are specifically related to the selection and implementation of the underlying cryptographic scheme used by a device and the larger system in which it operates:

- Select industry-standard cryptographic algorithms and protocols, and select appropriate key generation, distribution, management and protection, as well as robust nonce mechanisms.
- Use current NIST recommended standards for cryptography (e.g., FIPS 140-2[56], NIST Suite B[57]), or equivalent-strength cryptographic protection that are expected to be considered cryptographically strong throughout the service life of the device.
- Design a system architecture and implement security controls to prevent a situation where the full compromise of any single device can result in the ability to reveal keys for other devices.
  - For example, avoid using master-keys stored on device, or key derivation algorithms based solely on device identifiers or other readily discoverable information.
  - Avoid using device serial numbers as keys or as part of keys. Device serial numbers may be disclosed by patients seeking additional information on their device or might be disclosed during a device recall to identify affected products and should be avoided as part of the key generation process. Public-key cryptography can be employed to help meet this objective.
- Implement cryptographic protocols that permit negotiated parameters/versions such that the most recent, secure configurations are used, unless otherwise necessary.
- Do not allow downgrades, or version rollbacks, unless absolutely necessary for safety reasons. Downgrades can allow attackers to exploit prior, less protected versions and should be avoided.

D. Code, Data, and Execution Integrity

Many cybersecurity incidents are caused, at their root, by the violation of some form of device integrity. This includes the violation of stored code, stored and operational data, or execution state. The following recommendations are provided to address each of these categories.

- **Code Integrity**

[56] NIST FIPS 140-2 Cryptographic Module Validation Program available at: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards

[57]NIST FIPS 140-2 Suite B available at: https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2851.pdf

  - Authenticate firmware and software. Verify authentication tags (e.g., signatures, message authentication codes (MACs)) of software/firmware content, version numbers, and other metadata. The version numbers intended to be installed should themselves be signed or have MACs. Devices should be electronically and visibly identifiable (e.g., Unique device identifier (UDI), model number, serial number);
  - Allow installation of cryptographically authenticated firmware and software updates, and do not allow installation where such cryptographic authentication either is absent or fails. Use cryptographically signed updates to help prevent any unauthorized reductions in the level of protection (downgrade or rollback attacks) by ensuring that the new update represents an authorized version change.
    - One possible approach for authorized downgrades would be to sign new metadata for downgrade requests which, by definition, only happen in exceptional circumstances;
  - Ensure that the authenticity of software, firmware, and configuration are validated prior to execution, e.g., "allow-listing"[58] based on digital signatures;
  - Disable or otherwise restrict unauthorized access to all test and debug ports (e.g., JTAG, UART) prior to delivering products; and
  - Employ tamper evident seals on device enclosures and their sensitive communication ports to help verify physical integrity.
- **Data Integrity**
  - Verify the integrity of all incoming data, ensuring that it is not modified in transit or at rest. Cryptographic authentication schemes verify integrity, but do not verify validity;
  - Validate that all data originating from external sources is well-formed and compliant with the expected protocol or specification. Additionally, as appropriate, validate data ranges to ensure they fall within safe limits; and
  - Protect the integrity of data necessary to ensure the safety and effectiveness of the device, e.g., critical configuration settings such as energy output.
- **Execution Integrity**
  - Use industry-accepted best practices to maintain and verify integrity of code while it is being executed on the device. For example, Host-based Intrusion Detection/Prevention Systems (HIDS/HIPS) can be used to accomplish this goal; and
  - Carefully design and review all code that handles the parsing of external data using automated (e.g., static and dynamic analyses) and manual (i.e., code review) methods.

E. Confidentiality

[58] For the purposes of this guidance, "allow-list" means "a list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system." This term is leveraged from definition of "whitelist" in NIST SP 800-128.

Manufacturers should ensure support for the confidentiality[59] of any/all data whose disclosure could lead to patient harm (e.g., through the unauthorized use of otherwise valid credentials, lack of encryption). Loss of confidentiality of credentials could be used by a threat-actor to effect multi-patient harm. Lack of encryption to protect sensitive information and or data at rest and in transit can expose this information to misuse that can lead to patient harm. For example, confidentiality is required in the handling and storage of cryptographic keys used for authentication because disclosure could lead to unauthorized use/abuse of device functionality.

The proper implementation of authorization and authentication schemes as described in Sections (a) and (b) of this appendix (Appendix 1 – Security Control Categories and Associated Recommendations) will generally assure confidentiality. However, manufacturers should evaluate and assess whether this is the case during their threat modeling and other risk management activities and make any appropriate changes to their systems to ensure appropriate confidentiality controls are in place.

F. Event Detection and Logging

Event detection and logging are critical capabilities that should be present in a device and the larger system in which it operates in order to ensure that suspected and successful attempts to compromise a medical device may be identified and tracked. These event detection capabilities and logs should include storage capabilities, if possible, so that forensic discovery may later be performed.

While many of the following recommendations are tailored for workstations, the concepts presented below also apply to embedded computing devices. Manufacturers should consider these items for all devices:

- Implement design features that allow for security compromises and suspected compromise attempts to be detected, recognized, logged, timed, and acted upon during normal use. Acting upon security events should consider the benefit/risk assessment in accordance with Section 6.5 of AAMI TIR57 in determining whether it is appropriate to affect standard device functionality during a security event.
- Ensure the design enables forensic evidence capture.[60] The design should include mechanisms to create and store log files off the device to track security events. Documentation should include how and where log files are located, stored, recycled, archived, and how they could be consumed by automated analysis software (e.g.,

[59] For the purposes of this guidance, loss of confidential protected health information (PHI) is not considered patient harm. Although protecting the confidentiality of PHI is beyond the scope of this document, it should be noted that manufacturers and other entities, depending on the facts and circumstances, may be obligated to protect the confidentiality, integrity and availability of PHI throughout the product lifecycle, in accordance with applicable federal and state laws, including the Health Insurance Portability and Accountability Act (HIPAA). For more information on HIPAA, please visit https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[60] Forensic evidence capture is a necessary part of digital forensics. NIST SP 800-86 defines digital forensics as "The application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."

Intrusion Detection System (IDS)). Examples of security events include, but are not limited to, configuration changes, network anomalies, login attempts, and anomalous traffic (e.g., sending requests to unknown entities).

- Design devices such that the potential impact of vulnerabilities is limited by specifying a secure configuration. Secure configurations may include endpoint protections, such as anti-malware, firewall/firewall rules, allow-listing, defining security event parameters, logging parameters, and/or physical security detection.
- Design devices such that they may integrate and/or leverage antivirus/anti-malware protection capabilities. These capabilities may vary depending on the type of device and the software and hardware components it contains:
  - For devices that leverage Windows Operating System:
    - Antivirus/anti-malware is recommended on the device. Manufacturers are recommended to qualify multiple options to support user preferences for different options, especially if the device is used in health care facility environments.
  - For devices that leverage other Commercial Operating Systems (i.e., Ubuntu, Unix, Linux, Apple, Android, etc.)
    - Antivirus/anti-malware may be recommended based on the environment and associated risks of the device. Different operating systems will likely follow a case-by-case determination based on network exposure and risk.
  - For devices that leverage Embedded Operating Systems (i.e., Real-Time Operating Systems, Windows embedded, etc.)
    - Antivirus/anti-malware is generally not needed unless a particular risk or threat is identified that would not be addressed by other expected security controls.
- Design devices to enable software configuration management and permit tracking and control of software changes to be electronically obtainable (i.e., machine readable) by authorized users.
- Design devices to facilitate the performance of variant analyses such that the same vulnerabilities can be identified across device models and product lines.
- Design devices to notify users when malfunctions, including those potentially related to a cybersecurity breach, are detected.
- Consider designing devices such that they are able to produce a SBOM in a machine readable[61] format.

G. Resiliency and Recovery

Devices should be designed to be resilient to possible cybersecurity incident scenarios (also known as "cyber-resiliency"). Cyber-resiliency capabilities are important for medical devices because they provide a safety margin against unknown future vulnerabilities.

The following recommendations are intended to help designers achieve cyber-resiliency:

[61] Recommendation 2.2 from the Health Care Industry and Cybersecurity Task Force (HCIC TF) Report on Improving Cybersecurity in the Health Care Industry available here: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

- Implement features that protect critical functionality and data, even when the device has been partially compromised. For example, process isolation, virtualization techniques, and hardware-backed trusted execution environments all provide mechanisms to potentially contain the impact of a successful exploitation of a device.
- Design devices to provide methods for retention and recovery of trusted default device configuration by an authenticated, authorized user.
- Design devices to specify the level of resilience, or independent ability to function, that any component of the system possesses when its communication capabilities with the rest of the system are disrupted, including disruption of significant duration.
- Design devices to be resilient to possible cybersecurity incident scenarios such as network outages, Denial of Service,[62] excessive bandwidth usage by other products, disrupted quality of service[63] (QoS), and/or excessive jitter[64] (i.e., a variation in the delay of received packets).

H. Firmware and Software Updates

Devices should be capable of being updated in a secure and timely manner to maintain safety and effectiveness throughout the product's lifecycle. Despite best efforts, undiscovered, exploitable vulnerabilities may exist in devices after they are marketed. This is especially true over the device's service life, as threats evolve over time and exploit methods change, and become more sophisticated.

FDA recommends that manufacturers should not only build in the ability for devices to be updated, but that manufacturers also plan for the rapid testing, evaluation, and patching of devices deployed in the field. The following recommendations can help to achieve this:

- Design devices to anticipate the need for software and firmware patches and updates to address future cybersecurity vulnerabilities. This will likely necessitate the need for additional storage space and processing resources.
- Consider update process reliability and how update process works in event of communication interruption or failure. This should include both considerations for hardware impacts (timing specifics of interruptions) and which phase of the update process the interruption or failure occurs.
- Consider cybersecurity patches and updates that are independent of regular feature update cycles.
- Implement processes, technologies, security architectures, and exercises to facilitate the rapid verification, validation, and distribution of patches and updates.
- Preserve and maintain full build environments and virtual machines, regression test suites, engineering development kits, emulators, debuggers, and other related tools that were used to develop and test the original product to ensure updates and patches may be applied safely and in a timely manner.

[62] Denial of Service is an attack that prevents or impairs the authorized use of the information system, resources, or services.

[63] From CNSSI 4009 Committee on National Security Systems (CNSS) Glossary.

[64] From NIST SP 800-127 Guide to Securing WiMAX Wireless Communications.

- Maintain necessary third-party licenses throughout the supported lifespan of the device. Develop contingency plans for the possibility that a third-party company goes out of business or stops supporting a licensed product. Modular designs should be considered such that third-party solutions could be readily replaced.

Appendix 2. Submission Documentation for Security Architecture Flows

In premarket submissions, FDA recommends that manufacturers provide detailed information for the views identified in Section V.B.2. Methods for providing the views and the expectations for the level of detail to provide are discussed in the sections below. In addition to diagrams and explanatory text, call-flow views can be provided to convey some of the information details expected to be addressed in the architecture views.

A. Call-Flow Diagrams

A call-flow view is a diagram with explanatory text that describes the sequence of process or protocol steps in explicit detail. For each of the views, manufacturers may provide call-flow information to detail the communications included in the associated use case.

Call-flow views should provide specific protocol details of the communication pathways between parts of the system, to include authentication or authorization procedures and session management techniques. These views should be sufficiently detailed such that engineers and reviewers should be able to logically and easily follow data, code, and commands from any asset (e.g., a manufacturer server) to any other associated asset (e.g., a medical device), while possibly crossing intermediate assets (e.g., application). The call-flow views may also include items from the information details identified below for the views identified in Section V.B.2. if the information is better represented or conveyed through a call-flow view.

B. Information Details for an Architecture View

For each view described in Section V.B.2., manufacturers should provide a system-level description and analysis inclusive of end-to-end security analyses of all the communications in the system regardless of intended use. This should include detailed diagrams and traces for all communication paths as described below. Security-relevant analysis requires the ability to construct and follow a detailed trace for important communication paths, which describes how data, code, and commands are protected between any two assets in the device's system. This analysis can also help identify the software that should be included in the SBOM for each device.

The FDA recommends that security architecture views should include at least the following:

a. Detailed diagrams and supporting explanatory text that identify all manufacturer and network assets of the system in which the device will operate, including but not limited to:

   i. Device hardware itself (including assessments for any commercial platforms);

ii. Applications, hardware, and/or other supporting assets that directly interact with the targeted device, such as configuration, installation/upgrade, and data transfer applications;

iii. Health care facility-operated assets;

iv. Communications/networking assets; and

v. Manufacturer-controlled assets, including any servers that interact with external entities (e.g., a service that collects and redistributes device data, or a firmware update server).

b. For every communication path that exists between any two assets in the security use case view (and/or explanatory text), including indirect connections when there is at least one intermediate asset (e.g., an app), the following details should be provided:

i. A list of the communication interfaces and paths, including communication paths (e.g., between two assets through an intermediary), including any unused interfaces;

ii. An indication of whether the path is used for data, code, and/or commands, and type of data/information/code being transferred;

iii. Protocol name(s), version number(s), and ports/channels/frequencies;

iv. Detailed descriptions of the primary and all available functionality for each system asset, including assessment of any functionality that is built in but not currently used or enabled (e.g., dormant application functionality or ports), including assurance that this functionality cannot be activated and/or misused;

v. Access control models or features (if any) for every asset (such as privileges, user accounts/groups, passwords);

vi. Users' roles and levels of responsibility if they interact with the assets and communication channels.

vii. Any "handoff" sequences from one communication path to another (e.g., from asset to asset, network to network, or Bluetooth to Wi-Fi), and how the data, code, and/or commands are secured/protected during handoff (i.e., how is their integrity/authenticity assured);

viii. Explanations of intended behavior in unusual/erroneous/unexpected circumstances (e.g., termination of a connection in the middle of a data transfer);

ix. Authentication mechanism (if any), including the algorithm name/version (if available), "strength" indicators (e.g., key bit length, number of computational rounds) and mode of operation (if applicable);

x. Descriptions of the cryptographic method used and the type and level of cryptographic key usage and their style of use throughout the system (e.g., one-time use, key length, the standard employed, symmetric or otherwise). Descriptions should also include details of cryptographic protection for firmware and software updates;

xi. Detailed analyses by cryptography experts if a cryptography algorithm is proprietary, or a proprietary modification of a standard algorithm;

xii. For each authenticator created, a list of where it is verified, and how verification credentials (e.g., certificates, asymmetric keys, or shared keys) are distributed to both endpoints;

xiii. A precise, detailed list of how each type of credential (e.g., password, key) is generated, stored, configured, transferred, and maintained, including both manufacturer- and health care facility-controlled assets (e.g., key management and public key infrastructure (PKI));

xiv. Identity management[65] (if any), including how identities are managed/transferred and configured (e.g., from manufacturer to programmer and from programmer to device);

xv. If communication sessions are used or supported, a detailed explanation of how sessions are established, maintained, and broken down, including but not limited to assurances of security properties such as uniqueness, unpredictability, time-stamping, and verification of session identifiers;

xvi. Precise links between diagram elements (or explanatory text), associated hazards and controls, and testing;

xvii. Explanations or links to the evidence that may be used to justify security claims and any assumptions; and

xviii. Traceability to the SBOM described in section V.B.2, above, for proprietary and third-party code.

[65] For the purposes of this guidance, "identity management" means the process that governs the authentication and authorization of users to devices and assets.

Appendix 3. Submission Documentation for Investigational Device Exemptions

FDA acknowledges the need to balance innovation and security in designs especially during clinical trials. In order to ensure security is addressed early in the device design, FDA has identified a subset of the documentation recommended throughout this guidance to submit with IDE applications.

Under 21 CFR 812.25, manufacturers must provide an investigational plan as a part of their IDE application. For devices within the scope of this guidance, FDA recommends that this investigational plan include information on the cybersecurity of the subject device.

Specifically, FDA recommends the following documentation be included as part of IDE applications:

- Inclusion of cybersecurity risks as part of Informed Consent Form (21 CFR 50.25(a)(2) and 21 CFR 812.25(g));
- Global, Multi-patient and Updateability/Patchability views (21 CFR 812.25(c), (d))
- Security Use case views for functionality with safety risks (e.g., implant programming) (21 CFR 812.25(c), (d));
- Software Bill of Materials (21 CFR 812.25(c), (d)); and
- General Labeling – Connectivity and associated general cybersecurity risks, updateability/process (21 CFR 812.25(f)).

FDA intends to review this information in the context of the overall benefit-risk assessment of investigational devices as outlined in Factors to Consider When Making Benefit-Risk Determinations for Medical Device Investigational Device Exemptions.[66] Therefore, approval of an IDE based on the documentation recommended above does not preclude the possibility of future cybersecurity questions or concerns being raised during review of a subsequent marketing application. This is, in part, due to the understanding that design changes may be needed and the temporal nature of security. Security improvements will likely be needed between the time of clinical trials and the device submitted for marketing authorization (e.g., operating system no longer supported or nearing end of support, third party software updates, etc.).

[66] See FDA Guidance "Factors to Consider When Making Benefit-Risk Determinations for Medical Device Investigational Device Exemptions" available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/factors-consider-when-making-benefit-risk-determinations-medical-device-investigational-device.

Appendix 4. Terminology

The terminology listed here are for the purposes of this guidance and are intended for use in the context of assessing medical device cybersecurity. These terms are not intended to be applied in any context beyond this guidance.

Asset – anything that has value to an individual or an organization.[67]

Authentication – the act of verifying the identity of a user, process, or device as a prerequisite to allowing access to the device, its data, information, or systems, or provision of assurance that a claimed characteristic of an entity is correct.[68]

Authenticity – information, hardware, or software having the property of being genuine and being able to be verified and trusted; confidence that the contents of a message originates from the expected party and has not been modified during transmission or storage.[69]

Authorization – the right or a permission that is granted to a system entity to access a system resource.[70],

Availability – the property of data, information, and information systems to be accessible and usable on a timely basis in the expected manner (i.e., the assurance that information will be available when needed).[71]

Compensating Controls –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.[72]

Confidentiality – the property of data, information, or system structures to be accessible only to authorized persons and entities and are processed at authorized times and in the authorized manner, thereby helping ensure data and system security. Confidentiality provides the assurance

[67] Definition is adapted from ISO/IEC 27032 Information technology — Security techniques — Guidelines for cybersecurity, clause 4.6.

[68] Definition is adapted from NIST FIPS 200 Minimum Security Requirements for Federal Information and Information Systems and from ISO/IEC 18014-2:2009(E) Information technology – Security techniques - Time-stamping Services - Part 2: Mechanisms producing independent tokens, clause 3.

[69] Adapted from NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations: Authenticity is defined as "the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication."

[70] Definition is adapted from CNSSI 4009-2015 Committee on National Security Systems (CNSS) Glossary.

[71] [ISO IEC 27000-2018, Clause 3.7: The property of being accessible and useful on demand by an authorized entity].

Definition is adapted from CNSSI 4009-2015 Committee on National Security Systems (CNSS) Glossary.

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

that no unauthorized users (i.e., only trusted users) have access to the data, information, or system structures.[73]

Configuration – the possible conditions, parameters, and specifications with which a device or system component can be described or arranged.[74]

Configuration Management - a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development lifecycle.[75]

Cryptography – the discipline that embodies the principles, means, and methods for providing information security; including confidentiality, data integrity, non-repudiation, and authenticity.[76]

Cybersecurity – the process of preventing 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.[77]

Decommission – a process in the disposition process that includes proper identification, authorization for disposition, and sanitization of the equipment, as well as removal of Patient Health Information (PHI) or software, or both.[78]

Decryption – is the cryptographic transformation of encrypted data (called "ciphertext") into non-encrypted form (called "plaintext").[79]

Disposal – a process to end the existence of a system asset or system for a specified intended use, appropriately handle replaced or retired assets, and to properly attend to identified critical disposal needs (e.g., per an agreement, per organizational policy, or for environmental, legal, safety, security aspects).[80]

Encryption – is the cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used.[81]

[73] Definition is adapted from ISO IEC 27000-2018, Clause 3.10: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
[74] Adapted Definition is adapted from NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems: Configuration is the possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.
[75] Definition is adapted from NIST SP 800-53 Rev. 4.
[76] Definition is adapted from CNSSI 4009-2015 (NIST SP 800-21 Second edition).
[77] Definition is adapted from ISO IEC 27032: 2012, Clause 4.20.
[78] Definition is adapted from Medical Device and Health IT Joint Security Plan (JSP). Available at https://healthsectorcouncil.org/the-joint-security-plan/.
[79] Definition is referenced from NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security.
[80] Definition is adapted from 6.4.14.1 Disposal process purpose ISO/IEC/IEEE 12207:2017(E).
[81] Definition is referenced from NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security.

End of support – a point beyond which the product manufacturer ceases to provide support, which may include cybersecurity support, for a product or service.

Exploitability – the feasibility or ease and technical means by which the vulnerability can be exploited by a threat.[82]

Firmware – software program or set of instructions programmed on the flash read-only memory (ROM) of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.[83]

Hardening – a process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.[84]

Hardware – the material physical components of an information system.[85]

Integrity – the property of data, information and software to be accurate and complete and have not been improperly or maliciously modified.[86]

Lifecycle – all phases in the life of a medical device, from initial conception to final decommissioning and disposal.[87]

Malware – software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.[88]

Patch – a "repair job" for a piece of programming; also known as a "fix". A patch is the immediate solution to an identified problem that is provided to users. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches.[89]

Patient harm – injury or damage to the health of patients, including death.[90]

Programmable logic – hardware that has undefined function at the time of manufacture and must be programmed with software to function (e.g., Field-programmable gate array)

[82] The definition is adapted from the Common Vulnerability Scoring System (CVSS) specification document (v3.1).
[83] Definition is adapted from NISTIR 8183. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf
[84] Definition is referenced from NIST SP 800-152.
[85] Definition is referenced from CNSSI 4009-2015 (IETF RFC 4949 Ver 2).
[86] Definition is adapted from AAMI TIR 57 Clause 2.15.
[87] Definition is referenced from ANSI/AAMI/ISO 14971 Medical Devices – Application of Risk Management to Medical Devices, clause 2.7.
[88] Definition is referenced from NIST SP 800-53 Rev. 4.
[89] Definition is adapted from NIST SP 800-45 Version 2.
[90] Patient harm from cybersecurity risks is discussed at length throughout this guidance and the FDA Guidance "Postmarket Management of Cybersecurity in Medical Devices" issued December 2016. See Footnote 6.

Resilience – the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.[91]

Secure Product Development Framework (SPDF) - a set of processes that reduce the number and severity of vulnerabilities in products. Additional information about an SPDF and its implementation is discussed in Section IV.C. and throughout the guidance.

Security Architecture – a set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected. The security architecture reflects security domains, the placement of security-relevant elements within the security domains, the interconnections and trust relationships between the security-relevant elements, and the behavior and interactions between the security-relevant elements.[92]

Security Strength – a measure of the computational complexity associated with recovering certain secret and/or security-critical information concerning a given cryptographic algorithm from known data (e.g., plaintext/ciphertext pairs for a given encryption algorithm).[93] Throughout this guidance "strong" and other iterations of this term may be used that apply to this definition.

Security Risk Management – a process (or processes) that evaluates and controls threat-based risks. For security risk management, this includes an evaluation of the impact of exploitation on the device's safety and effectiveness, the exploitability, and the severity of patient harm if exploited.

Software Bill of Materials (SBOM) – a list of software components that includes but is not limited to commercial, open source, off-the-shelf, and custom software components. See Section V.A.2 for a more complete description of an SBOM.

System – the combination of interacting elements or assets organized to achieve one or more function.[94]

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. Threats exercise vulnerabilities, which may impact the safety or effectiveness of the device.[95]

[91] As defined in NISTSP 800-53 Rev. 4 definition of Information System Resilience.

[92] Definition is referenced from NIST 800-160v1, Systems Security Engineering.

[93] Definition is referenced from NIST SP 800-108.

[94] Definition is adapted from ISO/IEC/IEEE 12207:2017.

[95] Definition is adapted from NIST SP 800-53.

Threat modeling – a methodology for optimizing system, product, network, application, and connection security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.[96]

Trustworthy Device – a medical device that: (1) is reasonably secure from cybersecurity intrusion and misuse; (2) provides a reasonable level of availability and reliability; (3) is reasonably suited to performing its intended functions; and (4) adheres to generally accepted security procedures to support correct operation.[97]

Updatability and Patchability – the ease and timeliness with which a device and related assets can be changed for any reason (e.g., feature update, security patch, hardware replacement).

Update –corrective, preventative, adaptive, or perfective modifications made to software of a medical device.[98]

Vulnerability - a weakness in an information system, system security procedure(s), internal control(s), human behavior, or implementation that could be exploited.

[96] Definition is adapted from CNSSI 4009-2015 (NIST SP 800-21 Second edition).

[97] Definition is adapted from NIST SP 800-32 Introduction to Public Key Technology and the Federal PKI Infrastructure.

[98] Definition is from IMDRF Guidance "Principles and Practices for Medical Device Cybersecurity" available at http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf.