Contains Nonbinding Recommendations

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

---

Guidance for Industry and Food and Drug Administration Staff

Document issued on February 3, 2026.

This document supersedes "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," issued June 27, 2025.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 800-835-4709 or 240-402-8010, or by email at industry.biologics@fda.hhs.gov.

U.S. FOOD & DRUG ADMINISTRATION

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

GRZAN

Preface

Public Comment

You may submit electronic comments and suggestions at any time for Agency consideration 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 FDA-2021-D-1158. Comments may not be acted upon by the Agency until the document is next revised or updated.

Additional Copies

CDRH

Additional copies are available from the Internet. You may also send an email request to CDRH-Guidance@fda.hhs.gov to receive a copy of the guidance. Please include the document number GUI00001825 and complete title of the guidance in the request.

CBER

Additional copies are available from the Office of Communication, Outreach, and Development (OCOD), Center for Biologics Evaluation and Research (CBER), Food and Drug Administration, by calling 800-835-4709 or 240-402-8010, by email, industry.biologics@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

I. Introduction 1
II. Scope 2
III. Background 3
IV. General Principles 5
A. Cybersecurity is Part of Device Safety and the Quality Management System Regulation (QMSR) 5
1. A Secure Product Development Framework (SPDF) may be one way to satisfy the QMSR 6
B. Designing for Security 7
C. Transparency 8
D. Submission Documentation 8
V. Using an SPDF to Manage Cybersecurity Risks 9
A. Security Risk Management 10
1. Threat Modeling 12
2. Cybersecurity Risk Assessment 13
3. Interoperability Considerations 14
4. Third-Party Software Components 15
5. Security Assessment of Unresolved Anomalies 18
6. TPLC Security Risk Management 18
B. Security Architecture 19
1. Implementation of Security Controls 21
2. Security Architecture Views 22
C. Cybersecurity Testing 25
VI. Cybersecurity Transparency 27
A. Labeling Recommendations for Devices with Cybersecurity Risks 27
B. Cybersecurity Management Plans 30
VII. Cyber Devices 30
A. Who is Required to Comply with Section 524B of the FD&C Act 31
B. Devices Subject to Section 524B of the FD&C Act 31
C. Documentation Recommendations to Comply with Section 524B of the FD&C Act 32
1. Plans and Procedures (Section 524B(b)(1)) 32

2. Design, Develop, and Maintain Processes and Procedures to Provide a Reasonable Assurance of Cybersecurity (Section 524B(b)(2)) 34
3. Software Bill of Materials (SBOM) (Section 524B(b)(3)) 34
D. Modifications 35
1. Changes That May Impact Cybersecurity 35
2. Changes Unlikely to Impact Cybersecurity 35
E. Reasonable Assurance of Cybersecurity of Cyber Devices 36
Appendix 1. Security Control Categories and Associated Recommendations 38
A. Authentication 38
B. Authorization 40
C. Cryptography 41
D. Code, Data, and Execution Integrity 42
E. Confidentiality 43
F. Event Detection and Logging 43
G. Resiliency and Recovery 45
H. Firmware and Software Updates 45
Appendix 2. Submission Documentation for Security Architecture Flows 47
A. Diagrams 47
B. Information Details for an Architecture View 47
Appendix 3. Submission Documentation for Investigational Device Exemptions 50
Appendix 4. General Premarket Submission Documentation Elements and Scaling with Risk 51
Appendix 5. Terminology 54

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

---

Guidance for Industry and Food and Drug Administration Staff

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

I. Introduction

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 and other 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. Cyber 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 incidents 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 healthcare 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. For more information

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" and "Standards Development and the Use of Standards in Regulatory Submissions Reviewed in the Center for Biologics Evaluation and Research."

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

II. Scope

This guidance is applicable to devices with cybersecurity considerations, including but not limited to devices that include a device software function[1] or that contain software (including firmware) or programmable logic. 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, when submitted to the Center for Devices and Radiological Health (CDRH) or the Center for Biologics Evaluation and Research (CBER):

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

Furthermore, this guidance applies to all types of devices within the meaning of section 201(h) of the FD&C Act, including devices that meet the definition of a biological product under section 351 of the Public Health Service Act, whether or not they require a premarket submission. Therefore, the recommendations in this guidance also apply to devices for which a premarket submission is not required (e.g., for 510(k)-exempt devices). This guidance also applies to cyber devices, as defined in section 524B of the FD&C Act, which are a subset of devices.

Generally, the recommendations in this guidance apply to the device constituent part of a combination product[2] (such as drug-device and biologic-device combination products) when the

[1] For the purposes of this guidance, "device software function" means a software function that meets the definition of a device in section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). For the purposes of this guidance, the term "function" is a distinct purpose of the product, which could be the intended use or a subset of the intended use of the product. For more information, see FDA's guidance "Multiple Function Device Products: Policy and Considerations."

[2] 21 CFR 3.2(e).

device constituent part presents cybersecurity considerations,[3] including but not limited to devices that include a device software function or that contain software (including firmware) or programmable logic. For more information, contact the FDA review division that will have the lead review for the combination product.[4]

As IDE submissions have a different benefit-risk threshold and are not marketing authorizations, specific recommendations for IDE submission documentation are provided in Appendix 3. Additionally, Appendix 5 contains terminology used throughout the guidance.

III. Background

FDA recognizes that medical device cybersecurity is a shared responsibility among interested parties throughout the use environment of the medical device system, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices. For the purposes of this guidance, the term "medical device system" includes the device and systems—such as healthcare 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 that are used in various 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]

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," hereafter referred to as the "Postmarket Cybersecurity Guidance," 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 since the 2014 guidance are intended to further emphasize the importance of ensuring that devices are designed securely, are designed to

[3] 21 CFR 4.2.
[4] This guidance has been prepared by CDRH and CBER, in consultation with the Center for Drug Evaluation and Research (CDER) and the Office of Combination Products (OCP).
[5] For more information on the WannaCry Ransomware attack, see Indicators Associated With WannaCry Ransomware.
[6] For the purposes of this guidance, we consider "ransomware" an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. This definition is cited from the Cybersecurity & Infrastructure Security Agency's (CISA's) webpage Ransomware 101.
[7] For more information, see FDA's Cybersecurity webpage.
[8] For more information, see FDA's SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication.
[9] For more information on the German hospital ransomware attack, see The untold story of a cyberattack, a hospital and a dying woman.

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).[10] An SPDF, as described in this guidance, is a set of processes that reduces the number and severity of vulnerabilities in products throughout the device lifecycle. Examples of such frameworks exist in many sectors including the medical device sector.

Risk management for device manufacturers is the essential systematic practice of identifying, analyzing, evaluating, controlling, and monitoring risk throughout the product lifecycle to ensure that the devices they manufacture are safe and effective. FDA issued a final rule[11] amending the device current good manufacturing practice (cGMP) requirements of the Quality System (QS) Regulation under 21 CFR 820 to align more closely with the international consensus standard for Quality Management Systems (QMS) for medical devices used by many other regulatory authorities around the world. This revised Part 820 is referred to as the Quality Management System Regulation (QMSR).

The QMSR incorporates by reference the 2016 edition of ISO 13485.[12] By incorporating ISO 13485 by reference, we are explicitly requiring current internationally recognized regulatory expectations for QMS for devices subject to FDA's jurisdiction. Of particular note for this guidance, ISO 13485, incorporated into the QMSR by reference, incorporates risk management throughout its requirements.[13]

The recommendations contained in this guidance are intended to supplement FDA's Postmarket Cybersecurity Guidance, and "Content of Premarket Submissions for Device Software Functions," hereafter referred to as the "Premarket Software Guidance." This guidance replaces the 2014 final guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

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 (IMDRF) final guidance "Principles and Practices for Medical Device Cybersecurity," issued in March 2020.

---

[10] See Appendix 5, Terminology.

[11] See 89 FR 7496. This final rule took effect on February 2, 2026, and amends the majority of the requirements previously in 21 CFR Part 820 (Part 820) and incorporates by reference the 2016 edition of the International Organization for Standardization (ISO) 13485, Medical devices - Quality management systems – Requirements for regulatory purposes, in Part 820. As stated in the final rule, the requirements in ISO 13485 are, when taken in totality, substantially similar to the requirements of the previous Part 820, providing a similar level of assurance in a firm's quality management system and ability to consistently manufacture devices that are safe and effective and otherwise in compliance with the FD&C Act.

[12] All references to ISO 13485 in this guidance are to ISO 13485:2016, *Medical devices — Quality management systems — Requirements for regulatory purposes*.

[13] See 89 FR 7496 at 7505.

Additionally, section 3305 of the Food and Drug Omnibus Reform Act of 2022 ("FDORA"), enacted on December 29, 2022, added section 524B "Ensuring Cybersecurity of Medical Devices" to the FD&C Act. Effective March 29, 2023, with respect to premarket submissions for "cyber devices," section 524B(a) provides that sponsors must include information to ensure the device meets the cybersecurity requirements under section 524B(b).[14] Under section 524B(a) of the FD&C Act, a person who submits a 510(k), PMA, PDP, De Novo, or HDE for a device that meets the definition of a cyber device, as defined under section 524B(c), is required to submit information to ensure that cyber devices meet the cybersecurity requirements under section 524B(b).[15] Section 524B(c) of the FD&C Act defines "cyber device" as a device that "(1) includes software validated, installed, or authorized by the sponsor as a device or in a device; (2) has the ability to connect to the internet; and (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats" (see Section VII.B for more information on the term "cyber device"). The recommendations in this guidance are intended to help manufacturers meet their obligations under section 524B of the FD&C Act.

IV. General Principles

This section provides general principles for device cybersecurity relevant to device manufacturers. The principles in this guidance are important to the improvement of device cybersecurity and, when followed, are expected to have a positive impact on the safety and effectiveness of the device. The recommendations in this guidance cover all relevant cybersecurity considerations that may affect device safety and effectiveness, including but not limited to software, hardware, and firmware.

A. Cybersecurity is Part of Device Safety and the Quality Management System Regulation (QMSR)

Device manufacturers must establish and follow quality management systems to help ensure that their products consistently meet applicable requirements and specifications. The quality management systems requirements are found in the QMSR in 21 CFR Part 820, which incorporates by reference ISO 13485. Depending on the device, QMS requirements may be relevant at the premarket stage, postmarket stage,[16] or both.

[14] While section 524B(b)(4) of the FD&C Act authorizes FDA to promulgate additional cybersecurity requirements via regulation, FDA is not required to promulgate a regulation to elaborate on the new requirements specified in section 524B of the FD&C Act.

[15] In addition to the cybersecurity requirements set forth in section 524B(b) of the FD&C Act, section 524B(b)(4) of the FD&C Act requires cyber device manufacturers to comply with any other such requirements FDA sets forth in regulations "to demonstrate reasonable assurance that the device and related systems are cybersecure."

[16] In the postmarket context, design and development 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 QMSR, including but not limited to complaint handling (ISO 13485 Subclause 8.2.2 and 21 CFR 820.35(a)), quality audit (Subclause 8.2.4), analysis of data and improvement (Subclauses 8.4 and 8.5), software validation (Subclause 7.3.7), risk management (Subclause 7.1), and servicing (Subclause 7.5.4 and 21 CFR 820.35(b)).

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 ongoing requirements of the QMSR may be one source of documentation to include as part of the premarket submission.[17] This guidance is intended to explain how such documentation that may be relevant for QMSR compliance can also be used to show how a sponsor or manufacturer is addressing cybersecurity considerations relevant to a device. For example, 21 CFR 820.10(c) requires that for all classes of devices automated with software, a manufacturer must comply with the requirements in Design and Development, Clause 7.3 and its subclauses of ISO 13485.[18] As part of design and development, "[d]esign and development validation shall be performed in accordance with planned and documented arrangements to ensure that the resulting product is capable of meeting the requirements for the specified application or intended use" (Subclause 7.3.7). Design and development validation includes validation of device software. In addition, Subclause 7.1 of ISO 13485 specifies that the "organization shall document one or more processes for risk management in product realization." As part of the software validation required by Subclause 7.3.7, and risk management, including the requirements of Subclause 7.1, software device manufacturers may need to establish cybersecurity risk management and validation processes, where appropriate. See also FDA's guidance titled "Content of Premarket Submissions for Device Software Functions."

Software validation and risk management are key elements of cybersecurity analyses and demonstrating whether a device has a reasonable assurance of safety and effectiveness. FDA requires manufacturers to implement development processes that account for and address software risks throughout the design and development process, as discussed in ISO 13485 regarding design and development, which may include cybersecurity considerations.[19] 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.

1. A Secure Product Development Framework (SPDF) may be one way to satisfy the QMSR

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. An SPDF is a set of processes that help identify and reduce the number and severity of vulnerabilities in products. An SPDF encompasses all aspects of a product's lifecycle, including design, development, release, support, and decommission. Additionally, using SPDF processes during device design may prevent the need to re-engineer

[17] The recommendations in this guidance are not intended to suggest that FDA will evaluate an applicant's compliance with the QMSR as part of its premarket submission under section 510(k) of the FD&C Act in our determination of a device's substantial equivalence, as this is not a requirement for such decision under section 513(i) 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 QMSR compliance, and explain how the QMSR can be leveraged to demonstrate these performance outputs.

[18] References to clauses and subclauses in this guidance are to clauses and subclauses of ISO 13485:2016, unless otherwise specified.

[19] See Subclause 7.3 of ISO 13485.

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 management system at large.

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

B. Designing for Security

When reviewing premarket submissions, FDA intends to assess device cybersecurity based on a number of factors, including, but not limited to, the device's ability to provide and implement the security objectives below throughout the device architecture. The security objectives below generally may apply broadly to devices within the scope of this guidance, including, but not limited to, devices containing artificial intelligence (AI) and cloud-based services.

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 but may not be limited to:

- The device's intended use, indications for use, and reasonably foreseeable misuse;
- The presence and functionality of its electronic data interfaces;
- Its intended and actual environment of use;[20]
- The risks presented by cybersecurity vulnerabilities;
- 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 medical device system and the associated risk of patient harm. Because exploitation of known vulnerabilities or weak cybersecurity controls should be considered reasonably foreseeable failure modes for medical device systems, these factors should be addressed in the device design.[21] One of the key benefits of using an SPDF is that a medical

[20] Manufacturers may not be able to account for all potential environments of use, but should consider the range of use environments and ensure the risks are identified and controlled for the worst-case environments of use (e.g., least secure expected network configuration(s)).

[21] For more information on reasonably foreseeable misuse, see the IMDRF final guidance "Principles and Practices for Medical Device Cybersecurity."

device system 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 throughout the device lifecycle.

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 medical device system'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 to the medical device system, and other relevant information. For example:

- A failure to disclose all of the communication interfaces or third-party software could fail to convey potential sources of risks;
- Insufficient information pertaining to whether a device has known but not disclosed cybersecurity vulnerabilities or risks may be relevant to determining whether a device's safety or effectiveness could be degraded; and/or
- Labeling that does 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 medical device system.

This information and other relevant information are important in helping users understand a medical device system's resilience to cybersecurity threats, 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 devices and should be included in device labeling, as discussed below in Section VI.

D. Submission Documentation

Device cybersecurity design and documentation are 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 and development activities should result. Submitters should consider including in premarket submissions to FDA documentation generated from those design and development activities used during the development of a device with cybersecurity risks as a way to demonstrate reasonable assurance of safety and effectiveness. This guidance identifies the

cybersecurity information FDA recommends to help support a premarket submission for devices within the scope of this guidance, including but not limited to cyber devices.[22]

As cybersecurity is part of device safety and effectiveness, cybersecurity controls established during premarket development should also take into consideration the intended and actual use environment (see Section IV.B). Cybersecurity risks evolve over time and as a result, the effectiveness of cybersecurity controls may degrade as new risks, threats, and attack methods emerge. In the 510(k) context, FDA evaluates the cybersecurity information submitted and the protections the cybersecurity controls provide in demonstrating substantial equivalence (see section 513(i) of the FD&C Act and 21 CFR 807.100(b)(2)(ii)(B)).[23]

In addition, inadequate cybersecurity information in the device labeling may cause a device to be misbranded under section 502(f) of the FD&C Act if 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. For cyber devices, failure to comply with any requirement under section 524B(b)(2)of the FD&C Act (relating to ensuring device cybersecurity) is considered a prohibited act under section 301(q) of the FD&C Act.

This guidance recommends cybersecurity information be included in submissions based on cybersecurity risks, not on any other criteria or level of risk/concern established in a separate FDA guidance (e.g., the risk-based approach in the Premarket Software Guidance to help determine a device's Documentation Level). 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. Therefore, the recommendations in this guidance regarding information to be submitted to FDA are intended to address the cybersecurity risk, as assessed by the cybersecurity risk assessment during development of a device, 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.

For cyber devices, some of the information recommended in this guidance may help manufacturers meet their obligations for what is required to be in premarket submissions under section 524B of the FD&C Act.

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 satisfy premarket submission requirements in applicable statutory provisions and

[22] As previously discussed, section 524B of the FD&C Act requires the submission of certain documentation for cyber devices. See Section VII of this guidance for more information on cyber devices.

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

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.[24] Cybersecurity risks 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 standpoint, 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, healthcare facilities). For healthcare facilities, these devices can also be managed within their own cybersecurity risk management frameworks, such as the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, generally referred to as the NIST Cybersecurity Framework or NIST CSF.[25]

FDA recommends that manufacturers use device design processes such as those described in the QMSR, including ISO 13485, to support secure product development and maintenance. To preserve flexibility for manufacturers, manufacturers may use other existing frameworks that satisfy the QMSR and align with FDA's recommendations for using an SPDF. Possible frameworks to consider include, but are not limited to, the medical device-specific framework that can be found in the Medical Device and Health IT Joint Security Plan (JSP2) [26] and IEC 81001-5-1. Frameworks from other sectors may also comply with the QMSR, like the framework provided in ANSI/ISA 62443-4-1 *Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements*.[27]

The following subsections provide recommendations for using SPDF processes that FDA believes provide important considerations for the development of devices that are safe and effective, how these processes can complement the QMSR, and the documentation FDA recommends manufacturers provide for review as part of premarket submissions. These recommendations may be helpful for manufacturers of cyber devices that must "design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure . . ." pursuant to section 524B(b)(2) of the FD&C Act (see Section VII.C.2). The information in these sections does not represent a complete SPDF. For more information on SPDFs, see earlier in Section V. In addition, FDA does not recommend that manufacturers discontinue existing, effective processes.

A. Security Risk Management

To fully account for cybersecurity risks in medical device systems, 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

[24] Addressing cybersecurity risks is in addition to addressing other risks, including software, biocompatibility, sterilization, and electromagnetic compatibility, among others.
[25] For more information, please see the NIST Cybersecurity Framework.
[26] See the Medical Device and Health IT Joint Security Plan version 2 (JSP2).
[27] ANSI/ISA-62443-4-1 *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 JSP2.

because, given the evolving nature of cybersecurity threats and risks, no device is, or can be, completely secure. Security risk management should be an integrated part of a manufacturer's entire quality management system, addressed throughout the TPLC.[28] The quality management system 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 are, and once on the market, remain, safe and effective, which includes security.

Performing security risk management is distinct from performing safety risk management as described in ISO 14971. The distinction in the performance of these processes is due to the fact that in the security context versus the safety context, the scope of possible harm and the risk assessment factors may be different. Also, while safety risk management focuses on physical injury, damage to property or the environment, or delay and/or denial of care due to device or system unavailability, security risk management may include risks that can result in indirect or direct patient harm. Additionally, risks that are outside of FDA's assessment of safety and effectiveness, such as those related to business or reputational risks, may also exist.

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. For example, AAMI TIR57 and ANSI/AAMI SW96 detail how the security and safety risk management processes should interface to ensure all risks are adequately assessed.[29] FDA recommends that security risk management processes, as detailed in the QMSR and ISO 13485,[30] be established or incorporated into those that already exist, and should address the manufacturer's design, manufacturing, and distribution processes, as well as updates across the TPLC. The processes in ISO 13485, as incorporated by reference in the QMSR, that may be relevant in this context include, but are not limited to design and development (Subclause 7.3 of ISO 13485), production processes (Subclause 7.5), and improvement (including corrective actions and preventive actions) (Subclause 8.5) to ensure both safety and security risks are adequately addressed. For completeness in performing risk management under Subclause 7.1, FDA recommends that device manufacturers conduct both a safety risk assessment and a separate, accompanying security risk assessment to ensure a more comprehensive identification and management of patient safety risks.

A device should be designed to eliminate or mitigate known vulnerabilities. For marketed devices, if comprehensive design mitigations are not possible, compensating controls should be considered. For 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

---

[28] The TPLC processes include design and development, manufacturing, postmarket monitoring, delivering device software and firmware updates, and servicing, among others.

[29] AAMI TIR57 *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. ANSI/AAMI SW96 *Standard for medical device security - Security risk management for device manufacturers* (https://doi.org/10.2345/9781570208621.ch1) describes specific requirements for managing security related risk across the total product life cycle utilizing the risk management framework defined by ISO 14971 *Medical devices - Applications of risk management to medical devices.*

[30] See 21 CFR Part 820.

risk assessment and be assessed for additional control measures or risk transfer[31] 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 or manufacturer-controlled assets of the medical device system reach 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).

To document the security risk management activities for a medical device system, FDA recommends that manufacturers generate a security risk management plan and report such as that described in AAMI TIR57 and ANSI/AAMI SW96.[32] Manufacturers should include their security risk management reports—including the outputs of their security risk management processes—in their premarket submissions to help demonstrate the safety and effectiveness of the device. A security risk management report, such as that described in AAMI TIR57 and ANSI/AAMI SW96, should be sufficient to support the security risk management process aspect of demonstrating a reasonable assurance of safety and effectiveness. Such report should include the documentation elements for the system threat modeling, cybersecurity risk assessment, Software Bill of Materials (SBOM), component support information, vulnerability assessments, and unresolved anomaly assessment(s) described in the sections below.[33] In the subsections below, we discuss FDA's recommendations regarding the scope and/or content of specific security risk management documentation elements.

In addition to containing the documentation elements listed above, the security risk management report should:

- Summarize the risk evaluation methods and processes;
- Detail the residual risk conclusion from the security risk assessment;
- Detail the risk mitigation activities undertaken as part of a manufacturer's risk management processes; and
- Provide traceability between the threat model, cybersecurity risk assessment, SBOM, and testing documentation as discussed later in this guidance as well as other relevant cybersecurity risk management documentation.

1. Threat Modeling

Threat modeling includes a process for identifying security objectives, risks, and vulnerabilities across the medical device system, and then defining countermeasures to prevent, mitigate,

[31] For the purposes of this guidance, we consider "risk transfer" to include actions taken to manage risk that shifts some or all of the risk to another user, asset, system, network, or geographic area. This definition is adapted from the DHS Risk Lexicon.

[32] 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* and ANSI/AAMI SW96 *Standard for medical device security - Security risk management for device manufacturers*. https://doi.org/10.2345/9781570208621.ch1

[33] 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.

monitor, or respond to the effects of threats to the medical device 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 medical device 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 medical device system elements.

The threat model should:

- Identify medical device system risks and mitigations as well as inform the pre- and post-mitigation risks considered as part of the cybersecurity risk assessment;
- State any assumptions about the medical device 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 process.

FDA recommends that premarket submissions include threat modeling documentation to demonstrate how the medical device system has been analyzed to identify potential security risks that could impact safety and effectiveness. There are a number of methodologies and/or combinations of methods for threat modeling that manufacturers may choose to use.[34] 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 device.

2. Cybersecurity Risk Assessment

As a part of security risk management, security risks and controls should be assessed for residual risks as part of a cybersecurity risk assessment. Effective security risk assessments address the fact that cybersecurity-related failures can occur either intentionally or unintentionally. Accordingly, cybersecurity risks are difficult to predict, meaning that it is not possible to assess

[34] The MDIC/MITRE Playbook for Threat Modeling Medical Devices is an educational resource that discusses the threat modeling process, different threat modeling techniques, and provides fictional medical device examples.

and quantify the likelihood of an incident occurring based on historical data or modeling (also known as a "probabilistic manner"). This non-probabilistic approach is not the fundamental approach performed in safety risk management under ISO 14971 and further underscores why safety and security risk management are distinct but connected processes. Instead, security risk assessment processes focus on exploitability, or the ability to exploit vulnerabilities present within a device and/or system. FDA recommends that manufacturers assess identified risks according to the level of risk posed from the device and the system in which it operates. Additional discussion on exploitability assessments for the security risk assessment can be found in FDA's Postmarket Cybersecurity Guidance.

The premarket assessment of exploitability of a cybersecurity risk may be different from the exploitability assessment of a vulnerability discovered postmarket. 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 TPLC and how the risk is controlled.

Acceptance criteria for cybersecurity risks should carefully consider the TPLC of the medical device system, as it might be more difficult to mitigate cybersecurity issues once the device is marketed. As discussed above in Sections IV.B and V.A, known vulnerabilities should be assessed as reasonably foreseeable risks. The cybersecurity risk assessment for vulnerabilities identified during cybersecurity testing should also consider the TPLC of the device as the exploitability of the vulnerability is likely to increase over the device lifecycle. If a penetration tester, for example, was able to exploit a vulnerability, the ability of a threat actor to exploit that vulnerability is likely to increase over the device lifecycle. Furthermore, vulnerabilities identified in CISA's Known Exploited Vulnerabilities Catalog should be designed out of the device, as they are already being exploited and expose the medical device system and users to the risk.

FDA recommends that the cybersecurity risk assessment provided in premarket submissions capture the risks and controls identified from the threat model. The methods used for scoring the risk pre- and post-mitigation and the associated acceptance criteria as well as the method for transferring security risks into the safety risk assessment process should also be provided as part of the premarket submission.

3. Interoperability Considerations

Interoperability is an important consideration when assessing the cybersecurity of the end-to-end medical device system. As identified in FDA's guidance "Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices," hereafter referred to as the "Interoperability Guidance," interoperable medical devices have the ability to exchange and use information through an electronic interface with another medical or nonmedical product, system, or device.

As part of a medical device system, a device may have cybersecurity considerations from interoperable functionality, including but not limited to interfaces with:

- Other medical devices and accessories;

- "Other functions" as identified in FDA's guidance "Multiple Function Device Products: Policy and Considerations;"
- Healthcare infrastructure (e.g., network, Electronic Medical Records, medical imaging systems); and
- General-purpose computing platforms.

While cybersecurity controls may increase the complexity of interfaces to allow for interoperability, when properly implemented, the cybersecurity controls can help ensure that these capabilities remain safe and effective. Cybersecurity controls should be used as a means to allow for the safe and effective exchange and use of information. Additionally, cybersecurity controls should not be intended to prohibit a user from accessing their device data.

When common technology and communication protocols are used to enable interoperability (e.g., Bluetooth, Bluetooth Low Energy, network protocols), device manufacturers should assess whether added security controls beneath such communication are needed to ensure the safety and effectiveness of the device (e.g., added security controls beneath Bluetooth Low Energy to protect against risks if vulnerabilities in the Bluetooth Low Energy protocol or supporting technology are discovered).

In addition to the recommendations in the Interoperability Guidance, manufacturers should consider the appropriate cybersecurity risks and controls associated with the interoperability capabilities and document these considerations as recommended throughout this guidance.

4. Third-Party Software Components

As discussed in FDA's guidance "Off-The-Shelf (OTS) Software Use in Medical Devices," medical devices commonly include third-party software components,[35] including off-the-shelf and open source software. When these components are incorporated, security risks of the software components should become factors of the overall medical device system risk management processes and documentation.

As part of demonstrating compliance with design and development under Subclause 7.3 of ISO 13485, and to support supply chain risk management processes, all software, including those developed by the device manufacturer ("proprietary software") or obtained from third parties, should be assessed for cybersecurity risk. Device manufacturers should document all software components of a device and address or otherwise mitigate risks associated with these software components.

In addition, under Subclause 7.4 of ISO 13485, a manufacturer must put in place processes and controls to ensure that its suppliers conform to the manufacturer's requirements. Such information is documented in the Design and Development Files, required by Subclause 7.3.10, and Medical Device File, required by Subclause 4.2.3. This documentation demonstrates the device's overall compliance with the QMSR, 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

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

and the software supply chain may help demonstrate that manufacturers have adequately ensured such compliance and documented such history.

Software is updated over time to provide additional features, address security concerns, and otherwise be maintained. These changes may introduce new considerations or risks that must be accounted for as part of risk management. As a result, device manufacturers should establish and maintain custodial control of device source code (the original "copy" of the software) throughout the lifecycle of a device as part of configuration management.[36] This may be accomplished through different methods, such as source code escrow or source code backups, among others.[37]

Manufacturers may not have control of source code due to licensing restrictions, terms of supplier agreements, or other challenges. While source code is not required to be provided in premarket submissions, manufacturers should include plans for how third-party software components could be updated or replaced if support ends or other software issues arise in premarket submissions. The device manufacturer should also provide users with whatever information they may need in the device labeling to allow them to manage risks associated with the software components, including known vulnerabilities, configuration specifications, and other relevant security and risk management considerations.

One tool to help manage supply chain risk as well as clearly identify and track the software incorporated into a device is an SBOM, as described below.

(a) Software Bill of Materials (SBOM)

An 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 and the systems in which they operate 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.[38]

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 marketed devices, and should support documentation, such as the types detailed in Subclause

---

[36] 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.

[37] Source code escrow involves depositing a copy of a relevant piece of software's source code (and related technical components and documentation) with an independent third party ("escrow agent"). Source code backup involves storing (and updating as needed) a separate copy of the source code.

[38] For additional information, see the Department of Commerce National Telecommunications and Information Administration's multi-stakeholder process for software transparency available on the following website NTIA Software Component Transparency.

7.3.10 (Design and Development Files) and Subclause 4.2.3 (Medical Device File) of ISO 13485.

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. For cyber devices, an SBOM is required (see section 524B(b)(3) of the FD&C Act and Section VII.C.3 of this guidance). 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 document "Off-The-Shelf (OTS) Software Use in Medical Devices" describes information that should be provided in premarket submissions for software components for which a manufacturer cannot claim complete software lifecycle control. In addition to the information recommended in that guidance, manufacturers should provide machine-readable SBOMs consistent with the minimum elements (also referred to as "baseline attributes") identified in the October 2021 National Telecommunications and Information Administration (NTIA) Multistakeholder Process on Software Component Transparency document "Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)."

In addition to the minimum elements identified by NTIA, for each software component contained within the SBOM, manufacturers should include in the premarket submission:

- The software level of support provided through monitoring and maintenance from the software component manufacturer (e.g., the software is actively maintained, no longer maintained, abandoned); and
- The software component's end-of-support date.

When provided, manufacturers may choose to provide these additional elements as part of the SBOM, or they may provide it separately, such as in an addendum. Industry-accepted formats of SBOMs are encouraged.

If a manufacturer is unable to provide the SBOM information to FDA, the manufacturer should provide a justification for why the information cannot be included in the premarket submission.

As part of the premarket submission, manufacturers should also identify all known vulnerabilities associated with the device and the software components, including those identified in CISA's Known Exploited Vulnerabilities Catalog. For each known vulnerability, manufacturers should describe how the vulnerabilities were discovered to demonstrate whether the assessment methods were sufficiently robust. For components with known vulnerabilities, device manufacturers should provide in premarket submissions:

- A safety and security risk assessment of each known vulnerability (including device and system impacts); 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.

5. Security Assessment of Unresolved Anomalies

FDA's Premarket Software Guidance recommends that device manufacturers provide a list of software anomalies that exist in a product at the time of submission. For each anomaly, FDA recommends that device manufacturers conduct an evaluation of the anomaly's impact on the device's 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 Subclause 7.1 of ISO 13485, 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.[39]

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 documentation in the premarket submission.

6. 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 documentation 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, cybersecurity risk assessment) can be used to quickly identify vulnerability impacts once a device is released and, when appropriate, to support timely improvement, through corrective actions and preventive actions, described in Subclause 8.5 of ISO 13485.

[39] Examples of SW91 defect classification mapped to CWE can be found in Annex D of AAMI SW91 *Classification of Defects in Health Software*. For additional information on CWE categories, see CWE Common Weakness Enumeration.

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 is discussed in the Postmarket Cybersecurity Guidance.

To demonstrate the effectiveness of a manufacturer's processes, FDA recommends that a manufacturer track and record the measures and metrics below,[40] and provide them in premarket submissions and PMA annual reports (21 CFR 814.84), when available.[41] 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 the QMSR. At a minimum, FDA recommends tracking the following measures and metrics, or those that provide equivalent information:

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

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. 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

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

[41] If a manufacturer has not marketed prior versions 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.

[42] NIST 800-160 vol. 1 rev. 1, *Engineering Trustworthy Secure Systems* 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

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.

Subclause 7.3.1 of ISO 13485 requires manufacturers to document procedures for design and development. Under Subclause 7.3.2, 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 maintained and updated as design and development progresses (Subclause 7.3.2). Under Subclause 7.3.3, a manufacturer must determine and maintain inputs related to product requirements to ensure that the design requirements relating to a device are appropriate and address the intended use of the device. Under Subclause 7.3.4, design and development outputs must be in a form suitable for verification against the design and development inputs, and records must be maintained. Subclause 7.3.4 also states that design and development outputs shall contain or make reference to product acceptance criteria and shall ensure that those design outputs that are essential for its safe and proper use 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 all medical devices provide and enforce the security objectives in Section IV, above, but recognizes that implementations to address the security objectives may vary.

FDA recommends that premarket submissions include documentation on the security architecture. The objective in providing security architecture information in premarket submissions is to provide to FDA the security context and trust-boundaries of the medical device system in terms of the interfaces, interconnections, and interactions that the medical device system has with external entities. The details of these elements enable the identification of the parts of the medical device system in or through which incidents might occur. 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.

Manufacturers should analyze the entire system 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," and that these views be provided during premarket submissions to demonstrate safety and effectiveness.[43] If the documentation identified in this section already exists in other risk management documentation,

disruptions, hazards, and threats. For additional information, see NIST 800-160 vol. 1 rev. 1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[43] Views are discussed in more detail in the following subsections and Appendix 2.

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.

Below, FDA outlines the recommended security controls and ways 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 and development inputs for cybersecurity controls.[44]

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 and are an integral part of an SPDF. FDA recommends that an adequate set of security controls should 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 to avoid common pitfalls are detailed in Appendix 1.

Implementation of security 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 medical device 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 device's ability to demonstrate or maintain its safety and effectiveness.

[44] 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, Building Code for Medical Device Software Security, and IEC 81001-5-1. For a specific implementation of the OWASP Security by design principles, see the Medical Device and Health IT Joint Security Plan version 2 (JSP2).

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 the recommendations in Appendix 1, have (1) been implemented, and (2) been tested in order to validate that they were effectively implemented. For more information on cybersecurity testing, see Section V.C, below.

Manufacturers may include the demonstration of security controls that are comparable or in addition to those described in Appendix 1 in their premarket submissions. 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 the associated risks in order to demonstrate that they provide appropriate levels of safety and effectiveness. As cybersecurity design and development activities are established early in the development phase, FDA recommends that device manufacturers utilize the FDA Q-submission process to discuss design considerations for cybersecurity risk management throughout the device lifecycle with the agency.[45] Additional information on premarket documentation recommendations for design and development are discussed in the Security Architecture Views section below.

2. Security Architecture Views

In addition to the design and development requirements,[46] Subclause 8.5 of ISO 13485 requires that manufacturers establish and maintain procedures for implementing improvement, including corrective action and preventive action. The requirements under Subclause 8.4 for analyzing quality data to identify existing and potential causes of quality problems are used to determine the need for improvement under Subclause 8.5. FDA recommends that manufacturers develop and maintain security architecture view documentation as a part of the process for the design, development, and maintenance of the medical device 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 medical device system.

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

[45] For more information, see FDA's guidance "Requests for Feedback and Meetings for Medical Device Submissions: The Q-Submission Program."
[46] See Subclause 7.3 of ISO 13485.

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 in premarket submissions 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 medical device system function holistically within the associated implementation details. For the security architecture views, manufacturers should follow the recommendations outlined in Appendix 2 when determining the level of detail to include in premarket submissions.

These security architecture views should:

- Identify security-relevant medical device system elements and their interfaces;
- Define security context, domains, boundaries, critical user roles, and external interfaces of the medical device system;
- Align the architecture with (a) the medical device system security objectives and requirements, (b) security design characteristics in order to address the identified threats; and
- Establish traceability of architecture elements to user and medical device system security requirements. Such traceability should exist throughout the cybersecurity risk management documentation.

If a particular view sufficiently captures the risks of another view identified above, we do not expect manufacturers to duplicate documentation. Similarly, if threat modeling documentation sufficiently captures the view, we do not expect manufacturers to duplicate documentation. Additionally, if one of the views listed above is not appropriate, manufacturers should instead provide an explanation for why the view is not included in the premarket submission.

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

(a) Global System View

A global system view should describe the overall medical device 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), healthcare facility network impacts, intermediary connections or devices, cloud connections, and patient home network impact.

Depending on the complexity of the medical device 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 recommended 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 functionality. 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 healthcare 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 the system(s) in which they operate 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 recommended 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 TPLC 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 (i.e., deployed) to the device, and should include detailed information as recommended 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 that programs the implanted device. The software update path will likely include traversing technology that the device manufacturer does not control, and therefore the device 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 medical device 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 medical device system (e.g., power on, standby, transition states) and assess clinical functionality states of the medical device system (e.g., programming, alarming, delivering therapy, send/receive data, reporting diagnostic results).

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 recommended 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 and development activities. 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 Subclause 7.3.6 of ISO 13485, 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 Subclause 7.3.7, a manufacturer must establish and maintain procedures for validating its device design. FDA recommends verification and validation include sufficient testing performed by the manufacturer on the cybersecurity of the medical device 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 considered for inclusion in the submission:

- 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.
- Threat mitigation;
    - Manufacturers should provide details and evidence of testing that demonstrates effective risk control measures according to the threat models provided in the global system, multi-patient harm, updatability and patchability, and security use case 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).
- Vulnerability Testing (described in ANSI/ISA 62443-4-1); and
    - Manufacturers should provide details and evidence[47] of the following testing and analyses:
        - Abuse or misuse cases, 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.
- 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 by whom the testing was performed (e.g., independent internal testers, external testers) 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 discussed 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 medical device 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.

[47] 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.

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 premarket submission should contain plans for those releases. Such plans should 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.

There are numerous authoritative resources for outlining security testing that may partially fulfill the testing outlined above.[48]

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 commensurate with the risk (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

Cybersecurity transparency is critical to ensure safe and effective use and integration of devices and systems.[49] This transparency can be conveyed through both device labeling and the establishment of manufacturer vulnerability management plans. However, different types of users (e.g., manufacturers, servicers, patients) 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. Manufacturers of cyber devices should consider the recommendations in this section as they "design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure . . ." (section 524B(b)(2) of the FD&C Act; see Section VII.C.2).

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.

[48] The following standards may partially meet the security testing recommendations: ANSI/UL 2900 *Software Cybersecurity for Network-Connectable Products*, ANSI/ISA 62443-4-1 *Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements*, in addition to IEC 81001-5-*1 Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle*. Additional standards may also meet or partially meet the testing recommendations outlined in this section.

[49] Users often manage security risks in medical device systems by an end user or within a larger risk management framework like the NIST CSF.

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 design and development activities 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)[50] to ensure that the type of user has the capability to take appropriate actions to manage those risks.

The recommendations below aim to communicate to users the 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 ensure that users have up-to-date links that contain accurate information.[51]

The following are examples of information that may be included in labeling to communicate relevant security information to users:[52]

- 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).
- Sufficiently detailed diagrams for users that allow recommended cybersecurity controls to be implemented.
- 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.
- Specific guidance to users regarding supporting infrastructure requirements so that the device can operate as intended (e.g., minimum networking requirements, supported

[50] See FDA's Guidance "Applying Human Factors and Usability Engineering to Medical Devices."
[51] For more information regarding FDA's policy on labeling changes and submission requirements, manufacturers can use the Search for FDA Guidance Documents tool to identify relevant guidance documents for their product and submission type.
[52] See IEC TR 80001-2-2 *Application of risk management for IT-networks incorporating medical devices*—the relevant parts covering communication of medical device security needs, risks and controls; IEC TR 80001-2-8 *Application of risk management for IT-networks incorporating medical devices*— the relevant parts covering standards for establishing the security capabilities identified in IEC 80001-2-2; and IEC TR 80001-2-9 *Application of risk management for IT-networks incorporating medical devices*— the relevant parts covering use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities for further labeling information for compliance with these standards.

encryption interfaces). Where appropriate, such guidance should include 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.

- An SBOM as specified in Section V.A.4 or in accordance with an industry accepted format to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the medical device 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, manufacturers should ensure that users have up-to-date links that contain accurate information. The SBOM should be in a machine-readable format.
- 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.
- A description of how the design enables the device to respond when anomalous conditions are detected (i.e., security events). 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).
- A high-level description of the device features that protect critical functionality (e.g., backup mode, disabling ports/communications).
- A description of backup and restore features and procedures to restore authenticated configurations.
- A description of methods for retention and recovery of device configuration by an authenticated authorized user.
- A description of the secure configuration of shipped devices, instructions for user-configurable changes, and identification of user-configurable changes that could increase security risk for the medical device system. 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, and resetting of credentials, among others.
- 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, where, and in what format the log file is located, stored, recycled, archived, and how it could be consumed by automated analysis software (e.g., Intrusion Detection System (IDS) or Security Information and Event Management (SIEM)).
- Information, if known or anticipated, concerning device cybersecurity (including components) 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.
- 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 Medical Device and Health IT Joint Security Plan version 2 (JSP2) may address a number of the above recommendations.

B. Cybersecurity 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 to the relevant parties the vulnerabilities that are identified after releasing the device in accordance with Subclause 8.4 and Subclause 8.5 of ISO 13485, and 21 CFR Part 806, as appropriate. This plan can also support security risk management processes that are described throughout the QMSR and ISO 13485, as incorporated by reference in the QMSR.

FDA recommends that manufacturers submit their cybersecurity management 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. For cyber devices, "a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures" is required (see section 524B(b)(1) of the FD&C Act and Section VII.C.1 of this guidance).

Cybersecurity management plans should include the following elements:

- Personnel responsible;
- Sources, methods, and frequency for monitoring and identifying vulnerabilities (e.g., researchers, NIST national vulnerability database (NIST NVD), third-party software manufacturers);
- Identify and address vulnerabilities identified in CISA's Known Exploited Vulnerabilities Catalog;
- Periodic security testing;
- Timeline to develop and release patches;
- Update processes;
- Patching capability (i.e., rate at which update can be delivered to devices);
- Description of their coordinated vulnerability disclosure process; and
- Description of how the 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.

VII. Cyber Devices

This section identifies the cybersecurity information FDA considers to generally be necessary to support obligations under section 524B of the FD&C Act for cyber devices. This section provides recommendations specifically for cyber devices. Manufacturers of cyber devices should also consider the recommendations throughout this guidance to help meet their obligations under section 524B.

A. Who is Required to Comply with Section 524B of the FD&C Act

Under section 524B(a) of the FD&C Act, a person, including a manufacturer,[53] who submits a premarket application or submission under any of the following pathways—510(k),[54] PMA,[55] PDP, De Novo, or HDE[56]—for a device that meets the definition of a "cyber device," as defined in section 524B(c), is required to include such information as FDA may require to ensure that the cyber device meets the cybersecurity requirements under section 524B(b).

B. Devices Subject to Section 524B of the FD&C Act

Section 524B of the FD&C Act and its requirements apply to "cyber devices." Section 524B(c) defines a "cyber device" as a device that meets all of the following criteria "(1) includes software validated, installed, or authorized by the sponsor as a device or in a device; (2) has the ability to connect to the internet; and (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats."

Informed in part by the definitions recognized by NIST for the term "software," FDA considers a "cyber device" to include devices that are or contain software, including software that is firmware or programmable logic.[57] FDA also considers the "ability to connect to the internet" to include devices that are able to connect to the internet, whether intentionally or unintentionally, through any means (including at any point identified in the evaluation of the threat surface[58] of the device and the environment of use). It is well-demonstrated that if a device has the ability to connect to the Internet, it is possible that it can be connected to the Internet, regardless of whether such connectivity was intended by the device sponsor.[59]

---

[53] Section 524B(a) of the FD&C Act places obligations on the "person" who submits a specific type of device marketing application. Section 524B(b) of the FD&C Act places obligations on a "sponsor." For the purposes of this guidance, we assume that the manufacturer is the entity submitting the application and use the term accordingly throughout the guidance in lieu of the term "person" or "sponsor." However, if another person submits the application or submission enumerated under section 524B(a) of the FD&C Act to the Agency, that person should follow the guidance for manufacturers herein. Whatever person submits the application for a cyber device is subject to the requirements of section 524B.

[54] For the purposes of this guidance, "510(k)" refers to the original, special, and abbreviated 510(k) submissions.

[55] For the purposes of this guidance, "PMA" refers to the original PMA and supplement PMAs.

[56] For the purposes of this guidance, "HDE" refers to the original HDE and supplement HDEs.

[57] NIST defines a programmable logic controller (PLC) as "[a] solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing." A PLC is therefore a combination of two components: (1) the hardware controller, and (2) the "user-programmable memory," or programmable logic, that instructs the hardware controller to execute specified functions. NIST defines software as, among other things, "computer programs and data stored in hardware – typically in read only memory or programmable read-only memory." Programmable logic is therefore a specific type of computer program and/or data stored on hardware, and is thus a type of software. See the NIST Computer Security Resource Center Glossary for more information on NIST's definitions of these terms.

[58] For the purposes of this guidance "threat surface" is synonymous with the term "attack surface," however, FDA uses the term "threat surface" rather than "attack surface," because cyber threats need not necessarily be an "attack" to pose a risk to a medical device and its related system.

[59] For more information, see WannaCry Ransomware Encrypted Hospital Medical Devices and Indicators Associated With WannaCry Ransomware (Update I).

FDA considers devices that include any of the following features to have the ability to connect to the internet. The list below is illustrative, not exhaustive:

- Network, server, or Cloud Service Provider connections;
- Radio-frequency communications (e.g., Wi-Fi, cellular, Bluetooth, Bluetooth Low Energy);
- Magnetic inductive communications;[60] and
- Hardware connectors capable of connecting to the internet (e.g., USB, ethernet, serial port).[61]

C. Documentation Recommendations to Comply with Section 524B of the FD&C Act

For applicable premarket submission types, manufacturers must provide documentation to comply with the requirements under section 524B of the FD&C Act. Recommendations regarding the documentation to support each of the requirements are discussed in the sections below.

1. Plans and Procedures (Section 524B(b)(1))

Section 524B(b)(1) of the FD&C Act requires manufacturers of cyber devices to submit to FDA "a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures" in their premarket submissions. We recommend that the plan contain the information recommended for the Cybersecurity Management Plan described in Section VI.B. In particular, such a plan should address the items discussed below.

First, FDA considers that coordinated vulnerability disclosure (CVD) and related procedures, as required in section 524B(b)(1) of the FD&C Act, could include:

- Coordinated disclosure of vulnerabilities and exploits identified by external entities (including third-party software suppliers and researchers);
- Disclosure of vulnerabilities and exploits identified by the manufacturer of cyber devices; and
- Manufacturer procedures to carry out disclosures of the vulnerabilities and exploits, as identified above.[62]

[60] For example, magnetic inductive communication allows wireless data transmission between an implantable medical device and an external programmer. A transmitter coil in the external programmer sends data by modulating magnetic fields which then induces an electrical current in the receiver coil of the implantable medical device. The induced current carries encoded data, which allows communication, between the external programmer and the implantable medical device.

[61] For example, a device may need to be serviced via a USB connection. While the connection may be brief, the ability to connect is present and the device is therefore considered to have the ability to connect to the internet.

[62] For the purposes of this guidance, manufacturer procedures to carry out disclosures of the vulnerabilities and exploits may include procedures to inform device users, customers, patients, and other relevant healthcare parties.

Second, plans required by section 524B(b)(1) of the FD&C Act should also describe the timeline, with associated justifications, to develop and release required updates and patches:

- Section 524B(b)(2)(A) of the FD&C Act requires manufacturers of cyber devices to make available updates and patches[63] to the device and related systems[64] for known unacceptable vulnerabilities, with these updates and patches made available on a reasonably justified regular cycle.[65]
    - A "known unacceptable vulnerability" in section 524B(b)(2)(A) contrasts with a "critical vulnerability that could cause uncontrolled risks" in section 524B(b)(2)(B). A known unacceptable vulnerability could include a vulnerability that could not cause uncontrolled risks; a vulnerability that is not currently known to cause uncontrolled risks; or a vulnerability that could present controlled risk, as described in FDA's Postmarket Cybersecurity Guidance. Updates and/or patches to address these vulnerabilities may be intended to maintain the supportability of software. Generally, software should be regularly updated to maintain the supportability of the software. For examples of vulnerabilities associated with controlled risk, see the Postmarket Cybersecurity Guidance. Updates and patches to address these types of vulnerabilities are not to reduce uncontrolled risk, and therefore not to reduce a risk to health or to correct a violation of the FD&C Act. See below for more information on section 524B(b)(2)(B) of the FD&C Act.
- Section 524B(b)(2)(B) of the FD&C Act requires manufacturers of cyber devices to make available updates and patches to the device and related systems to address as soon as possible out of cycle,[66] critical vulnerabilities that could cause uncontrolled risks.
    - In general, this includes vulnerabilities that could cause uncontrolled risks, as described in FDA's Postmarket Cybersecurity Guidance. For examples of vulnerabilities associated with uncontrolled risks, see the Postmarket Cybersecurity Guidance.

---

[63] An update is defined by NIST as "[a] patch, upgrade, or other modification to code that corrects security and/or functionality problems in software" (see NIST Computer Security Resource Center Glossary). Patches are defined by CISA as "software and operating system (OS) updates that address security vulnerabilities within a program or product" (see Understanding Patches and Software Updates). We consider an update or patch that would satisfy the requirements under section 524B(b)(2)(A)-(B) for updates or patches as an action that modifies device code to address a cyber risk.

[64] For the purposes of this guidance, we refer to the evaluation of "related systems" to the extent needed to determine that the device, as it interacts with related systems, remains cybersecure. Related systems are further described in Section VII.C.2, below.

[65] The justification for the regular cycle should typically be included in the cybersecurity management plan. The length of the regular cycle may vary depending on numerous factors for the particular device. One of the primary factors that may influence the length of the cycle is risk. For example, an interconnected thermometer whose functionality is limited to taking and reporting patient temperature may have lower risk of harm if exploited than an interconnected surgery robot, whose risk of harm may be significantly higher. At the same time, exploitation of a seemingly lower-risk device may provide opportunities to affect other devices within the environment of use, leading to significantly greater risk of harm if these other devices or the larger environment are exploited or disrupted. Manufacturers should fully consider the risks to and from their devices, within the larger context(s) of the environment(s) in which they will be intended to operate, and design and deploy regular update cycles that provide a reasonable assurance of cybersecurity.

[66] For example, a manufacturer may make updates outside of the planned reasonably justified regular cycle to remediate an uncontrolled risk.

Third, we recommend that manufacturers of cyber devices anticipate and make appropriate updates to these plans,[67] as well as to the processes and procedures discussed in Section VII.C.2 below,[68] as new information becomes available, such as when new risks, threats, vulnerabilities, assets, or adverse impacts are discovered throughout the total product lifecycle. To support such efforts, manufacturers should also create or update appropriate documentation (e.g., threat modeling, cybersecurity risk assessment) and maintain it throughout the device lifecycle. Doing so will allow manufacturers to quickly identify vulnerability impacts once a device is released and could also help satisfy the patching requirements of section 524B(b)(2)(A)-(B) of the FD&C Act.

The required plans,[69] as well as the processes and procedures discussed in Section VII.C.2 below,[70] also should, as appropriate, account for any differences in the risk management for fielded devices (e.g., differences between marketed devices and 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 the differing software configurations of the device. Vulnerabilities should be assessed for any differing impacts for all fielded versions to ensure patient risks are being accurately assessed.

2. Design, Develop, and Maintain Processes and Procedures to Provide a Reasonable Assurance of Cybersecurity (Section 524B(b)(2))

Manufacturers of cyber devices must "design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure . . ." (section 524B(b)(2) of the FD&C Act). FDA considers related systems to include, among other things, manufacturer-controlled elements, such as other devices, software that performs "other functions" as described in FDA's Guidance "Multiple Function Device Products: Policy and Considerations," software/firmware update servers, and connections to healthcare facility networks. In the design, development and maintenance of a cyber device, manufacturers should consider the cybersecurity risks of related systems to the cyber device and implement appropriate security controls to mitigate those risks. The documentation recommendations identified in this guidance and summarized in Appendix 4 should be considered and used to demonstrate reasonable assurance that the device and related systems are cybersecure as required by section 524B(b)(2).

3. Software Bill of Materials (SBOM) (Section 524B(b)(3))

Section 524B(b)(3) of the FD&C Act requires manufacturers of cyber devices to provide an SBOM, including commercial, open-source, and off-the-shelf software components. To assist with complying with this requirement, we recommend that a cyber device provide SBOMs that contain the information recommended in Section V.A.4.b.

---

[67] See section 524B(b)(1) of the FD&C Act.
[68] See section 524B(b)(2) of the FD&C Act.
[69] See section 524B(b)(1) of the FD&C Act.
[70] See section 524B(b)(2) of the FD&C Act.

D. Modifications

As previously stated, the requirements under section 524B of the FD&C Act apply to a manufacturer who submits an application or submission under any of the following pathways—510(k), PMA, PDP, De Novo or HDE—for a device that meets the definition of a cyber device. Therefore, a manufacturer required to submit an application or submission under one of the enumerated pathways for a device modification would also need to comply with the requirements in section 524B of the FD&C Act.[71] In keeping with least burdensome principles,[72] the information we recommend that manufacturers of cyber devices provide will generally differ based on the type of change and whether such change impacts the cybersecurity of the device. Overall, we recommend that manufacturers use the recommendations below to determine the information FDA recommends manufacturers of cyber devices provide to demonstrate they have met the new requirements under section 524B when submitting a premarket submission for a device modification.

1. Changes That May Impact Cybersecurity

In general, changes that may impact cybersecurity and may require premarket submission could include changes to authentication or encryption algorithms, new connectivity features, or changing software update process/mechanisms. For these types of changes, see Section VII.C for required and recommended documentation to be included with each premarket submission (see section 524B of the FD&C Act).

2. Changes Unlikely to Impact Cybersecurity

In general, changes unlikely to impact cybersecurity could include changes in materials, sterilization method changes, or a change to an algorithm without change to architecture/software structure/connectivity.

For these types of changes, FDA recommends that manufacturers of cyber devices provide the following information to meet their premarket submission requirements in section 524B of the FD&C Act:

- 524B(b)(1)
    - If not previously provided, manufacturers must provide a plan as described in section 524B(b)(1) of the FD&C Act; we recommend that it contain the information as described in Section VII.C.1, above.
    - If a plan described in Section VII.C.1, above, was previously provided, the manufacturer should provide a reference to the prior submission and a summary of any changes to the plan.

[71] For more information on when to submit an application for a device modification, see other FDA guidances, including "Deciding When to Submit a 510(k) for a Software Change to an Existing Device" and "Modifications to Devices Subject to Premarket Approval (PMA) - The PMA Supplement Decision-Making Process."

[72] For more information on FDA's least burdensome provisions, see FDA's guidance "The Least Burdensome Provisions: Concept and Principles."

- 524B(b)(2)
    - Instead of the full documentation described as required or recommended in Section VII.C.2, above, manufacturers may provide the following information:
        - Description of whether there are currently any "critical vulnerabilities that could cause uncontrolled risks."[73]
        - Description of whether any vulnerabilities with uncontrolled risk were remediated in the device since the last authorization. If so, manufacturers should describe how remediation was performed following the recommendations in FDA's Postmarket Cybersecurity Guidance.
- 524B(b)(3)
    - Section 524B(b)(3) of the FD&C Act requires manufacturers of cyber devices to provide an SBOM, including commercial, open-source, and off-the-shelf software components. To assist with complying with this requirement, we recommend that a manufacturer of a cyber device provide an SBOM that contains the information recommended in Section V.A.4.b above.

In general, in its cybersecurity review, FDA intends to focus substantive review on modifications to cybersecurity controls or modifications that are likely to affect cybersecurity. However, regardless of the type of change being proposed to the device in the premarket submission, FDA intends to take into account known cybersecurity concerns that are applicable to such device when conducting its premarket reviews and in determining whether the device has a reasonable assurance of cybersecurity.

E. Reasonable Assurance of Cybersecurity of Cyber Devices

Section 3305(c) of FDORA provides that nothing in section 524B of the FD&C Act "shall be construed to affect the Secretary's authority related to ensuring that there is a reasonable assurance of the safety and effectiveness of devices, which may include ensuring that there is a reasonable assurance of the cybersecurity of certain cyber devices . . ." FDA interprets this provision to mean that a "reasonable assurance of cybersecurity" can be part of FDA's determination of a device's safety and effectiveness. Moreover, a determination that there is a reasonable assurance of cybersecurity is relevant to the various premarket pathways and authorization under them, specifically, FDA's review of a 510(k), PMA, PDP, De Novo, and HDE. With the exponential growth of interconnected devices on the market over the past few years (see Section I), ensuring cybersecurity has become essential to FDA's ability to protect the public health and provide reasonable assurance of safety and effectiveness of devices.

When evaluating a 510(k) submission, FDA considers changes to the environment of use (e.g., changes in technology the subject device will interact with or operate within, and any new risks

[73] Section 524B(b)(2)(B) of the FD&C Act requires manufacturers to make available postmarket updates and patches to the cyber device and related systems to address, as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks, among other requirements. See Section VII.C.1 for more information on "critical vulnerabilities that could cause uncontrolled risks."

or vulnerabilities the device will be exposed to), new risks or vulnerabilities in the technological characteristics compared to the predicate device submission (e.g., changes to level of support for component software, vulnerabilities in communication protocols or technology used by the subject device), and how the subject device design and/or performance testing (e.g., see the cybersecurity testing recommendations in Section V.C) address these new risks or vulnerabilities.[74] For example, if in reviewing the 510(k) for an alarm for a central nursing station software, FDA identifies that the device has increased risks compared to its predicate because it does not have the necessary encryption to protect against a recently identified cyber threat, FDA may ask for additional performance data (e.g., see the documentation recommendations in Section V). If the data provided is inadequate, FDA would likely make a determination that the new device is not substantially equivalent (NSE) to the predicate device because this threat, if exploited, could negatively impact the safety and effectiveness of the device because alarm accuracy is essential for healthcare providers to effectively monitor the health of patients in a hospital.

[74] For more information about current review practices for 510(k) submission, see FDA's guidance "The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)]."

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*[75] exists where the device and the system in which it operates are 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 should verify the authenticity of information from external entities, as well as prove the authenticity of information that they generate. A medical device system that appropriately accounts for authenticity can evaluate and ensure authenticity for:

- Information at rest (stored);
- Information in transit (transmitted);
- Entity authentication of communication endpoints, whether those endpoints consist of software or hardware;
- Software binaries;
- Integrity of the execution state of currently running software; and
- Any other appropriate parts of the medical device 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 medical device system.

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

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

- Implicit authentication 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. For more information on cryptography, see Appendix 1 subsection C., 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[76] 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 authorization 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 several methods including the use of cryptographic nonces (an arbitrary number used only once in a cryptographic communication);

[76] See the definition of security strength in Appendix 5, Terminology.

- 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 clinician programmer or monitoring device and an implanted device like a pacemaker, defibrillator, or neurostimulator; or the link between a continuous glucose monitor 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
- 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 a 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[77] 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 healthcare 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 AAMI TIR57 or ANSI/AAMI SW96 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[78] 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:

[77] The NIST Computer Security Resource Center Glossary defines "least privilege" as "A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks"

[78] For the purposes of this guidance, "signal of intent" is specific to the implementation of NFC communications.

- 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 medical device 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, healthcare 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.

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 140-3[79]) or equivalent-strength cryptographic protection that are expected to be considered cryptographically strong throughout the service life of the device.
    - Manufacturers should not implement cryptographic algorithms that have been deprecated or disallowed in applicable standards or best practices (e.g., NIST SP 800-131A, Transitioning the Use of Cryptographic Algorithms and Key Lengths). Implementation of algorithms with a status of "legacy use" should be discussed with FDA during a pre-submission meeting.
- 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.
    - For example, 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

[79] See NIST FIPS 140-3 *Security Requirements for Cryptographic Modules*. https://doi.org/10.6028/NIST.FIPS.140-3

products and should be avoided as part of the key generation process (e.g., 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, and log and document the event. Downgrades can allow attackers to exploit prior, less protected versions and should be avoided.

D. Code, Data, and Execution Integrity

Many cyber 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**
  - Hardware-based security solutions should be considered and employed when possible;
  - 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),[80] 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"[81] 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 data integrity, but do not verify data validity. Therefore, the integrity of all incoming data should be verified to ensure that it is not modified in transit or at rest;

[80] For more information regarding UDI, see FDA's webpage UDI Rule, Guidances, Training, and Other Resources.
[81] 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 the definition of "whitelist" in NIST SP 800-128. https://doi.org/10.6028/NIST.SP.800-128

- 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

Manufacturers should ensure support for the confidentiality[82] 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 will generally ensure 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 medical device 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 the following for all devices:

---

[82] For the purposes of this guidance, loss of confidential health information is generally not considered to be a direct impact on safety and effectiveness. 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 see the Summary of the HIPAA Security Rule.

- 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 AAMI TIR57 or ANSI/AAMI SW96 in determining whether it is appropriate to affect standard device functionality during a security event.
- Ensure the design enables forensic evidence capture.[83] The design should include mechanisms to securely 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., 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, physical security detection, and/or HIDS/HIPS.
- 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 healthcare facility environments.
    - For devices that leverage other Commercial Operating Systems (e.g., Ubuntu, Unix, Linux, Apple, Android):
        - 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 (e.g., Real-Time Operating Systems, Windows embedded):
        - Antivirus/malware detection/protection software 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.

[83] 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." https://doi.org/10.6028/NIST.SP.800-86

- Design devices to notify users when malfunctions or anomalous device behavior, including those potentially related to a cybersecurity breach, are detected.
- Consider designing devices such that they are able to produce an SBOM in a machine readable format.

G. Resiliency and Recovery

Devices should be designed to be resilient to possible cyber incident scenarios (also known as "cyber-resiliency") and maintain availability. 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:

- 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 medical device system possesses when its communication capabilities with the rest of the medical device system are disrupted, including disruption of significant duration.
- Design devices to be resilient to possible cyber incident scenarios such as network outages, Denial of Service, excessive bandwidth usage by other products, disrupted quality of service (QoS), and/or excessive jitter (i.e., a variation in the delay of received packets).
- Design devices to be resilient to possible noise items (e.g., scanning).

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.
- 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.
- Implement a secure process and mechanism for providing validated software updates and patches for users.

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 recommendations 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. Diagrams

FDA recommends that manufacturers provide diagrams to help describe the medical device system architecture, interfaces, communication protocols, threats, and cybersecurity controls used throughout the system. Different diagramming methods can be used to describe the architecture, including data flow diagrams, state diagrams, swim-lane diagrams, and call-flow diagrams, among others. Architecture views should include diagram(s) with explanatory text that describes the sequence of process or protocol steps in explicit detail for an associated use case.

Architecture views should provide specific protocol details of the communication pathways between parts of the medical device 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 diagrams may also include items from the information details identified below for the architecture views identified in Section V.B.2 if the information is better represented or conveyed through a diagram than explanatory text alone.

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 medical device 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 medical device system. This analysis can also help identify the software that should be included in the SBOM for each device.

FDA recommends that security architecture views should consider the following examples of information for inclusion:

- Detailed diagrams and supporting explanatory text that identify all medical device system assets, including but not limited to:
    - Device hardware itself (including assessments for any commercial platforms);

    - Applications, hardware, and/or other supporting assets that directly interact with the targeted device, such as configuration, installation/upgrade, and data transfer applications;
    - Healthcare facility-operated assets;
    - Communications/networking assets; and
    - Manufacturer-controlled assets, including any servers that interact with external entities (e.g., a server that collects and redistributes device data, or a firmware update server).
- 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:
    - A list of the communication interfaces and paths, including communication paths (e.g., between two assets through an intermediary), and any unused interfaces;
    - An indication of whether the path is used for data, code, and/or commands, and type of data/information/code being transferred;
    - Protocol name(s), version number(s), and ports/channels/frequencies;
    - Detailed descriptions of the primary and all available functionality for each medical device 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;
    - Access control models or features (if any) for every asset (such as privileges, user accounts/groups, passwords);
    - Users' roles and levels of responsibility if they interact with the assets and communication channels;
    - 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 ensured);
    - Explanations of intended behavior in unusual/erroneous/unexpected circumstances (e.g., termination of a connection in the middle of a data transfer);
    - 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);
    - Descriptions of the cryptographic method used and the type and level of cryptographic key usage and their style of use throughout the medical device 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;
    - Detailed analyses by cryptography experts if a cryptography algorithm is proprietary, or a proprietary modification of a standard algorithm;
    - 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;

- 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 healthcare facility-controlled assets (e.g., key management and public key infrastructure (PKI));
- Identity management[84] (if any), including how identities are managed/transferred and configured (e.g., from manufacturer to programmer and from programmer to device);
- 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;
- Include any security configuration settings and their default values;
- Precise links between diagram elements (or explanatory text), associated hazards and controls, and testing;
- Explanations or links to the evidence that may be used to justify security claims and any assumptions; and
- Traceability of the asset to the SBOM component described in Section V.B.2, above, for proprietary and third-party code, when appropriate.

[84] 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 understands 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 investigational 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 FDA's guidance "Factors to Consider When Making Benefit-Risk Determinations for Medical Device Investigational Device Exemptions." 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 cybersecurity. Cybersecurity improvements will likely be needed between the time of clinical trials and when the device is submitted for marketing authorization (e.g., operating system no longer supported or nearing end of support, third-party software updates).

Appendix 4. General Premarket Submission Documentation Elements and Scaling with Risk

As stated in Section IV.D and throughout the guidance, device cybersecurity design and documentation are expected to scale with the cybersecurity risk of that device. While documentation breadth is expected to scale, each type of documentation identified throughout the guidance is recommended for all premarket submissions for devices with potential cybersecurity risks. As mentioned previously, the submission documentation recommendations in this guidance are intended to help manufacturers meet their obligations for cyber devices under section 524B of the FD&C Act.

Table 1 below summarizes the specific documentation elements identified throughout the guidance for premarket submissions, the associated sections of the guidance for the document, and whether the documentation is recommended for IDE submissions. While documentation elements are identified for the security risk management report, manufacturers can provide the documentation elements in a way that is consistent with their existing documentation processes.

This table is not intended to serve as merely a deliverable checklist, as the processes outlined throughout the guidance are intended to help align generation of these documents and their resultant content with FDA's recommendations. This table represents one possible way to organize the recommended information.

The below documentation will naturally scale with the level of cybersecurity risk. This will be most evident in the breadth of the Threat Modeling and Architecture Views documentation.

- For example, a device with either only one hardware connection (e.g., USB port) or a SaMD product with limited other software dependencies and connectivity will likely only need to have single architecture view for each of the global system, multi-patient harm, and updateability/patchability views; the security use case view(s) will likely be limited to a smaller subset of unique views to address the available connectivity and software.
- For a device with greater complexities such as, but not limited to, networking, wireless connections, cloud, and/or commercial operating systems, multiple architecture views may be needed for the multi-patient harm and updateability/patchability views as there may be multiple ways to cause multi-patient harm or update elements of the device. Additionally, many security use case views will likely be needed to convey the various unique security and clinical use cases throughout the architecture.

Table 1. Recommended Premarket Submission Documentation

Type of Premarket Submission Documentation	Guidance Section(s)	IDE Submission*
Cybersecurity Risk Management Report	Sections V, VI.B	Could be helpful to submit, but not specifically recommended

Type of Premarket Submission Documentation	**Guidance Section(s)**	**IDE Submission***
- Threat Model (may include Architecture Views)	Sections V.A.1, V.A.3, V.A.4, V.A.5, V.B.2, Appendix 1, Appendix 2	Could be helpful to submit, but not specifically recommended (see Architecture View recommendations)
- Cybersecurity Risk Assessment	Sections V.A.2, V.A.3, V.A.4, V.A.5, V.A.6	Could be helpful to submit, but not specifically recommended
- SBOM	Sections V.A.4, VI.A	Recommended
- Vulnerability Assessment and Software Support	Section V.A.4	Could be helpful to submit, but not specifically recommended
- Unresolved Anomalies Assessment	Section V.A.5	Could be helpful to submit, but not specifically recommended
- Traceability	Sections V.A, V.A.1, V.A.2, V.A.3, V.A.4. V.A.5, V.A.6, V.B.1, V.B.2, V.C, VI.A	Could be helpful to submit, but not specifically recommended
Measures and Metrics	Section V.A.6	Could be helpful to submit, but not specifically recommended
Architecture Views	Section V.B	Recommended • Global, Multi-patient and Updateability/Patchability views • Security Use Case views for functionality with safety risks
- Requirements	Sections V.B.1, Appendix 1	Recommended • Global, Multi-patient and Updateability/Patchability views • Security Use Case views for functionality with safety risks
- Architecture Views (may be included in Threat Model)	Sections V.A.1, V.B.2, Appendix 1, Appendix 2	Recommended • Global, Multi-patient and Updateability/Patchability views • Security Use Case views for functionality with safety risks
Testing	Section V.C	Could be helpful to submit, but not specifically recommended

Type of Premarket Submission Documentation	**Guidance Section(s)**	**IDE Submission***
Labeling	Section VI.A	Recommended • Informed Consent Form to include cybersecurity risks • General Cybersecurity Labeling - Connectivity and associated general cybersecurity risks, updateability/process
Cybersecurity Management Plans	Section VI.B	Could be helpful to submit, but not specifically recommended

*For the purposes of this table, "recommended" refers to the elements of an IDE submission FDA discusses in Appendix 3 of this document; "could be helpful to submit, but not specifically recommended" refers to additional elements that could be helpful to FDA if submitted, but are not specifically recommended in Appendix 3. If a device-specific guidance contains additional or different recommendations to those in this table, the device-specific recommendations should be followed. If a manufacturer is unsure, they should utilize the FDA Q-submission process.

Appendix 5. 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.

Anomaly – any condition that deviates from the expected behavior based on user needs, requirements, specifications, design documents, or standards.

Asset – anything that has value to an individual or an organization.[85]

Attack Surface Analysis – evaluation of attack surface to determine all avenues of ingress and egress to and from a system including common vulnerabilities and exposed ports and services.[86]

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.[87]

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 originate from the expected party and has not been modified during transmission or storage.[88]

Authorization – the right or a permission that is granted to a system entity to access a system resource.[89]

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).[90]

Boundary Analysis – the process of uniquely assigning information resources to an information system, which defines the security boundary for that system.[91]

Closed Box Testing – a method of software testing that examines the functionality of an application without peering into its internal structures of workings.[92]

---

[85] Definition is adapted from ISO/IEC 27032 *Information technology — Security techniques — Guidelines for cybersecurity*.
[86] Definition is adapted from ANSI/ISA 62443-1-1.
[87] Definition is adapted from NIST Computer Security Resource Center Glossary.
[88] Definition is adapted from NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5
[89] Definition is adapted from CNSSI 4009 *Committee on National Security Systems (CNSS) Glossary*.
[90] Definition is adapted from ISO IEC 27000, and CNSSI 4009 CNSS Glossary.
[91] Definition is adapted from NIST Special Publication 800-18 Revision *1 Guide for Developing Security Plans for Federal Information Systems*.
[92] Definition is adapted from CNSSI 4009 *CNSS Glossary*.

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.[93]

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 that no unauthorized users (i.e., only trusted users) have access to the data, information, or system structures.[94]

Configuration – the possible conditions, parameters, and specifications with which a device or system component can be described or arranged.[95]

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.[96]

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

Cryptography – the discipline that embodies the principles, means, and methods for providing information security; including confidentiality, data integrity, non-repudiation, and authenticity.[97]

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.[98]

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.[99]

---

[93] Definition is adapted from NIST SP 800-53A *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53Ar5

[94] Definition is adapted from ISO IEC 27000: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

[95] Definition is adapted from NIST SP 800-128 *Guide for Security-Focused Configuration Management of Information Systems*. https://doi.org/10.6028/NIST.SP.800-128

[96] Definition is adapted from NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5.

[97] Definition is adapted from CNSSI 4009 *CNSS Glossary*.

[98] Definition is adapted from ISO IEC 27032 *Information technology — Security techniques — Guidelines for cybersecurity*.

[99] Definition is adapted from Medical Device and Health IT Joint Security Plan version 2 (JSP2).

Denial of Service – prevention or impairment to the authorized use of the information system, resources, or services.[100]

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, or security aspects).[101]

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.[102]

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.[103]

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.[104]

Fuzz Testing – process of creating malformed or unexpected data or call sequences to be consumed by the entity under test to verify that they are handled appropriately.[105]

Hardware – the material physical components of an information system.

Integrity – the property of data, information and software to be accurate and complete and have not been improperly or maliciously modified.[106]

Least Privilege – a security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.[107]

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

---

[100] Definition is adapted from NIST Computer Security Resource Center Glossary.
[101] Definition is adapted from ISO/IEC/IEEE 12207 *Systems and Software Engineering – Software Life Cycle Processes.*
[102] Definition is cited from NIST SP 800-82 *Guide to Operational Technology (OT) Security*. https://doi.org/10.6028/NIST.SP.800-82r3
[103] Definition is adapted from the Common Vulnerability Scoring System (CVSS) specification document.
[104] Definition is adapted from NISTIR 8183 *Cybersecurity Framework Manufacturing Profile*. https://doi.org/10.6028/NIST.IR.8183
[105] Definition is adapted from NIST Computer Security Resource Center Glossary.
[106] Definition is adapted from AAMI TIR 57 *Principles for Medical Device Security – Risk management*.
[107] Definition is adapted from NIST Computer Security Resource Center Glossary.

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.[108]

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.[109]

Patient harm – injury or damage to the health of patients, including death.[110]

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).

Quality of Service – necessary level of measurable performance in a data communications system or other service which may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.[111]

Reasonably foreseeable misuse – use of a product or system in a way not intended by the manufacturer, but which can result from readily predictable human behavior.[112]

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.[113]

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 Sections IV and V, and throughout the guidance.[114]

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

---

[108] Definition is adapted from NIST Computer Security Resource Center Glossary.
[109] Definition is adapted from NIST SP 800-45 *Guidelines on Electronic Mail Security*. https://doi.org/10.6028/NIST.SP.800-45ver2
[110] Patient harm from cybersecurity risks is discussed at length throughout this guidance and the Postmarket Cybersecurity Guidance.
[111] Definition is adapted from CNSSI 4009 National Information Assurance (IA) Glossary.
[112] Definition is adapted from ISO 14971 *Medical Devices – Application of Risk Management to Medical Devices*.
[113] Definition is cited from NIST Computer Security Resource Center Glossary.
[114] The term "Secure Product Development Framework" was developed for the purposes of this guidance to help reflect and encompass the concepts related to secure development lifecycles and frameworks. While the term SPDF is new, the concepts around secure product development and risk management are not new, and align with expectations in the QMSR and Labeling Regulations. As cybersecurity continues to evolve, FDA continues to align its terminology to reflect best practices.

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.[115]

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).[116] 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 formal inventory of software components and dependencies, information about those components, and their hierarchical relationships.[117] The software components in an SBOM include, but are not limited to, commercial, open source, off-the-shelf, and custom software components. See Section V.A.4 for a more complete description of an SBOM.

System – the combination of interacting elements or assets organized to achieve one or more function.[118]

Threat – 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.[119]

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.[120]

---

[115] Definition is adapted from NIST Computer Security Resource Center Glossary.
[116] Definition is cited from NIST SP 800-108 *Recommendation for Key Derivation Using Pseudorandom Functions*. https://doi.org/10.6028/NIST.SP.800-108
[117] Definition is adapted from NTIA's Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM).
[118] Definition is adapted from ISO/IEC/IEEE 12207 *Systems and Software Engineering – Software Life Cycle Processes*. https://doi.org/10.1109/IEEESTD.2017.8100771
[119] Definition is adapted from NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5
[120] Definition is adapted from CNSSI 4009 *CNSS Glossary*.

Threat surface – the set of points on the boundary of a system, a system element, or an environment where a cyber threat can try to enter, cause an effect on, or extract data from, that system, system element, or environment.[121]

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.[122]

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

Unresolved anomaly – a defect that still resides in the software because a sponsor deemed it appropriate not to correct or fix the anomaly, according to a risk-based rationale about its impact to the device's safety and effectiveness.[123]

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.[124]

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

Vulnerability Chaining – the sequential exploit of multiple vulnerabilities in order to attack to attack a system, where one or more exploits at the end of the chain require the successful completion of prior exploits in order to be exploited.[125]

[121] Definition is adapted from NIST Computer Security Resource Center Glossary.
[122] Definition is adapted from NIST SP 800-32 *Introduction to Public Key Technology and the Federal PKI Infrastructure*. https://doi.org/10.6028/NIST.SP.800-32
[123] Definition is consistent with the Premarket Software Guidance even though we use the terms differently.
[124] Definition is cited from IMDRF Guidance "Principles and Practices for Medical Device Cybersecurity."
[125] Definition is adapted from the Common Vulnerability Scoring System (CVSS) specification document.

Guidance History[*]	Date	Description
Revisions to Final Guidance	February 2026	Revisions issued under Level 2 guidance procedures (21 CFR 10.115(g)(4)), including revisions to align with the amendments to 21 CFR 820 (the Quality Management System Regulation (QMSR)). This guidance supersedes the final guidance titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" and published June 2025.
Level 1 Final Guidance	June 2025	See Notice of Availability for more information.** This guidance supersedes the final guidance titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" and published September 2023.
Reissued as Level 1 Draft Guidance	March 2024	See Notice of Availability for more information.**

*This table was implemented, beginning June 2025, and previous guidance history may not be captured in totality.

**The Notice of Availability is accessible via the Search for FDA Guidance Documents webpage.