FDA CYBERSECURITY GUIDANCE FOR MEDICAL DEVICES A BRIEF ON THE LAW, SPDF, JSP, AND NIST SSDF

GERALD T. RIGDON

Fellow, Software Engineering
Boston Scientific, Inc., United States of America
gerald.rigdon@bsci.com
https://rigdonhouse.com
cell: 651-328-1763

Abstract*—This paper reviews the final U.S. Food and Drug Administration (FDA) Cybersecurity Guidance (CSG) issued September 27, 2023, and explores the use of both the Medical Device and Health IT Joint Security Plan (JSP) version 1.0 and the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF) version 1.1 as a Secure Product Development Framework (SPDF) coined in the FDA CSG. It also offers a legal brief on the changes in U.S. law during 2022-2023 that provide the authority behind these substantial regulatory shifts and the expectations incumbent upon medical device manufacturers.*

***Keywords*—** NIST, SSDF, Cybersecurity, SPDF, Medical Devices

Note: At the time of writing this paper it is understood that JSP 1.0 is undergoing revision. Due to the timing of the paper and lack of access to a public draft of JSP 2.0, the analysis proceeded with the current revision. Moreover, JSP 1.0 was also the official revision when the CSG was finalized.

Acronym Resolver

CFR – Code of Federal Regulations

CSF – Cybersecurity Framework (NIST)

CSG – Cybersecurity Guidance (FDA)

FDA – Food and Drug Administration

JSP – Medical Device and Health IT Joint Security Plan

NIST - National Institute of Standards and Technology

SPDF – Secure Product Development Framework (FDA)

SSDF – Secure Software Development Framework (NIST)

QSR – Quality System Regulations

INTRODUCTION – A LEGAL BRIEF

In December of 2022, Congress passed the Consolidated Appropriations Act [1], which in Section 3305, described the amendments to the Federal Food, Drug, and Cosmetic (FD&C) Act by the addition of section 524B entitled "Ensuring Cybersecurity of Medical Devices." After identifying this applies to anyone who submits a 510(k), PMA, De Novo, IDE, etc., the Act proceeds to lay out both the requirements and the definition of language used. In no uncertain terms the new FD&C Act update expressly requires that manufacturers of cyber devices, defined in subsection (c) as any device with software that can connect to the internet and contains any technology that could be vulnerable to cybersecurity threats, shall, in essence:

1) Have a plan to monitor, identify, and address post-market exploits and vulnerabilities, and disclose findings.

2) Design, develop, and maintain processes and procedures that provide reasonable cybersecurity assurance while making updates to devices and related systems available.

3) Provide a SBOM or Software Bill of Materials which includes commercial, off-the-shelf, and open-source components.

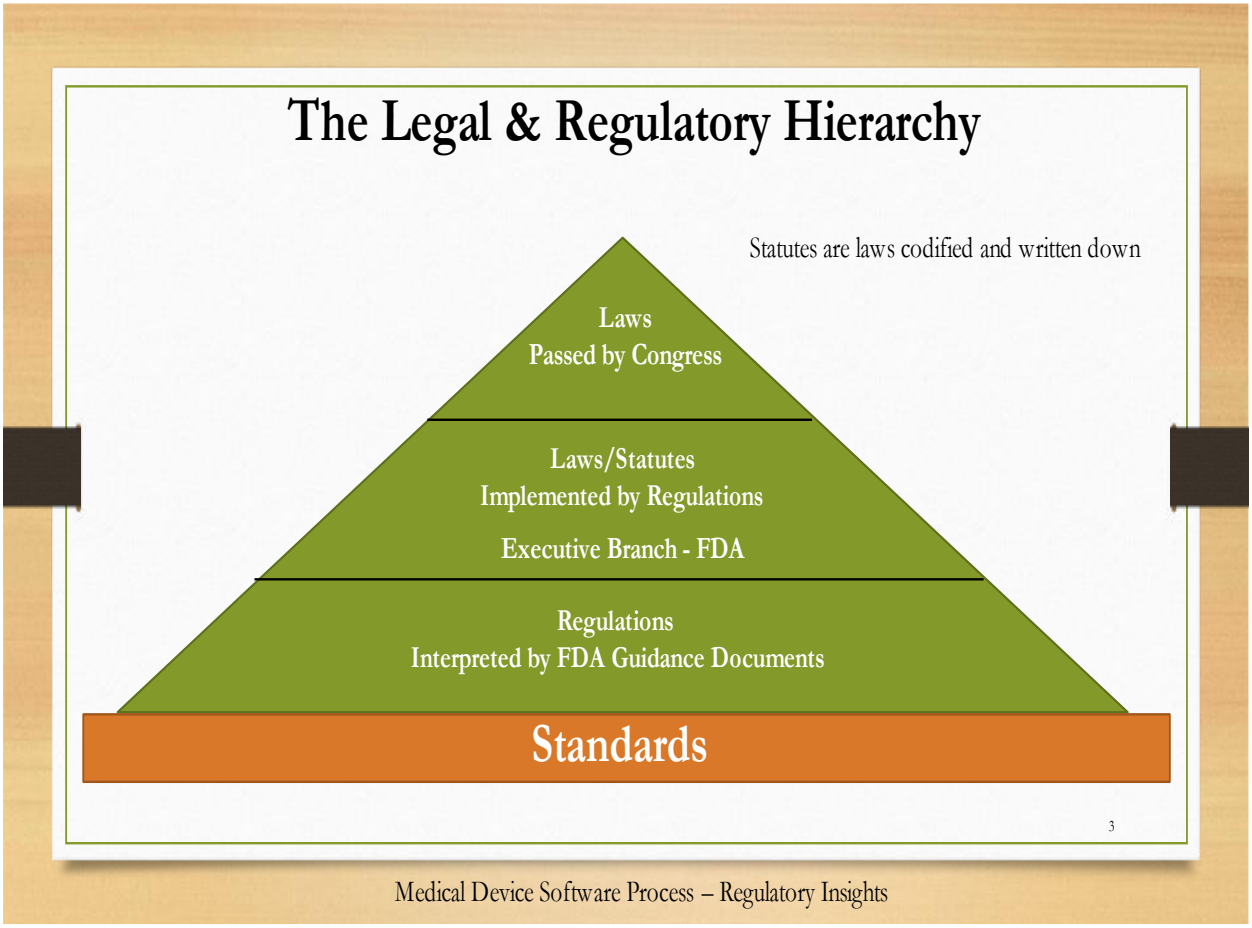
4) Comply with other requirements considered necessary to regulatory authorities that demonstrate devices and related systems are reasonably cybersecure.

Given the last requirement, the Food and Drug Administration (FDA) published its final Cybersecurity Guidance (CSG) [2] and therein references the new section 524B of the FD&C Act. This response did not come unexpectedly given events like the hospital WannaCry ransomware attacks and SweynTooth, the collection of Bluetooth related vulnerabilities that became well known in 2020 and mentioned in the CSG. Although the definition of a cyber device in 524B further raises a more specific question about connectivity, the messaging from the CSG seems to make it clear that this includes both direct and indirect internet connectivity. For example, an implanted medical device may not have direct internet connectivity yet may connect to other devices using wireless communication protocols, such as Bluetooth, opening pathways to indirect internet connectivity.

Historically, FDA guidance documents are considered recommendations without any legal binding, and so true to form the CSG [2] states: "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." A helpful visual aid is presented in Figure 1 where FDA guidance documents form the base of the hierarchy, which itself may relate to international standards that are independent of the laws of any country.

Figure 1: The Legal & Regulatory Hierarchy

[3]



Interestingly, the CSG [2] later says: "For cyber devices, failure to comply with any requirement under section 524B(b)(2) (relating to ensuring device cybersecurity) is considered a prohibited act under section 301(q) of the FD&C Act." Considering the brevity of the requirements in the FD&C Act and the somewhat circular nature of the language, one is presented with the following to digest:

- FDA states that the CSG is not legally binding.
- FDA emphasizes that failure to follow the FD&C Act is prohibited, the same Act that says you must comply with "other" (unspecified future) ***requirements*** that can be added through regulations per the Office of the Secretary.

The word "should' is used 161 times in the CSG [2] and the word "shall" only 7 times (the word generally associated with ***requirements***), leaving what appears to be 53 pages of mostly recommendations that also reference the Code of Federal Regulations (CFR) ***requirements*** over 50 times. Ultimately, there is an implied expectation that medical device manufacturers follow the recommendations to avoid potential legal consequences. However, navigating these recommendations should not deter one from challenging the CSG along the way.

SPDF - SECURE PRODUCT DEVELOPMENT FRAMEWORK

One of the central messages of the CSG [2] is the concept of a SPDF or "a set of processes that reduce the number and severity of vulnerabilities in products throughout the device lifecycle." This framework is a generic way to describe how you go about securing medical devices within a product development environment. SPDF is not a legal term and so is presented as "one way" to satisfy the Quality System Regulations (QSR) with respect to cybersecurity risk management as derived from 21 CFR Part 820.30. Moreover, the CSG suggests that a SPDF may possibly be satisfied by other pre-existing more established cybersecurity frameworks and references both the Medical Device and Health IT Joint Security Plan (JSP) [6] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

However, the CSG [2] further distinguishes between medical facilities and device manufacturers and suggests that while NIST CSF can be used for the former, JSP [6] is applicable for the latter. Yet, the NIST Secure Software Development Framework (SSDF) is not mentioned. The FDA's rationale for the use of other frameworks is that they contain device design processes described in the QSR which support device development and maintenance. Among the list of candidates for use as a SPDF are IEC 81001-5-1, ANSI 62443-4-1, and JSP.

But, what about NIST SSDF [10]? A big part of a SPDF framework is the management of cybersecurity risks, and the NIST SSDF is self-described as a document that provides recommendations for a risk-based approach to threat mitigation and the reduction of software vulnerabilities. Revisiting Figure 1, in the center of the hierarchy is where laws, like the FD&C Act are implemented in the form of regulations known as the CFR. Yet, as for the amended section 524B of the FD&C Act, the CSG [2] seems to prefer to reference the Act itself while resting on the unrevised pre-existing language of QSR Design Controls in the CFR. In fact, the risk management element of a SPDF as proposed in the CSG hinges on clause (g) of the QSR 820.30 which states:

"(g) *Design Validation.* Each manufacturer shall establish and maintain procedures for validating the device design…Design validation shall ensure that devices conform to defined user needs and intended uses… Design validation shall include software validation and ***risk analysis*****,** where appropriate. The results of the design validation, including identification of the design, method(s), the date, and the individual(s) performing the validation, shall be documented in the DHF."

Therefore, cybersecurity risk management as described in the proposed SPDF falls under the language **"*risk analysis*"** from the QSR. Interestingly, on February 23, 2022, the FDA [4] proposed to amend the entire medical device QSR part 820 with the 2016 version of ISO 13485 [5], but the CSG [2] stresses that "the concept of risk management as described in 21 CFR 820.30(g) would remain." That is an odd statement considering ISO 13485 per FDA [4] admittedly places greater emphasis on risk management activities than does 820.30 (g) which relies on ***risk analysis*** within design validation to support all the activities of risk management; the process of identifying, analyzing, evaluating, controlling, and monitoring risk.

In order to avoid spending too much time debating legal matters, one can simply embrace the proposition that the "risk analysis" language in 820.30 (g) includes cybersecurity risk management.

The strong-minded can defer to ISO 13485 [5]; the direction where the U.S. QSR appears to be headed. The following sections will consider how JSP [6] can be used as a SPDF and then a case will be made for NIST SSDF [10].

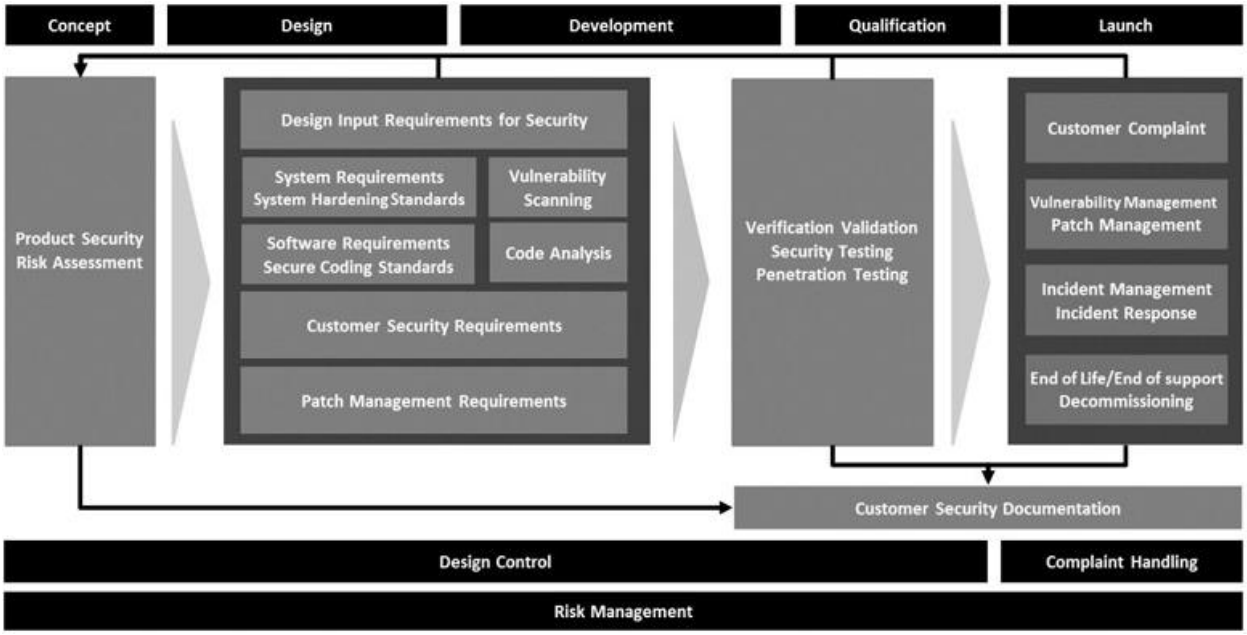
JSP 1.0 – MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN

As stated in the front matter, this analysis uses the 2019 version of JSP. According to [6], "JSP is a consensus-based total product lifecycle reference guide for developing, deploying, and supporting cyber secure technology solutions in the health care environment." It was produced by the Health Sector Coordinating Council or HSCC Joint Cybersecurity Working Group and so it is not a regulatory document nor an international standard. It claims to be a guide but provides a framework and is applicable to organizations of all sizes and maturity to address cybersecurity challenges. See Figure 2.

However, as a framework, it employs terminology familiar to those working in the regulated medical device industry. In fact, JSP [6] was created specifically for medical device development so the linkages to FDA requirements are explicit. As stated in the CSG [2], device manufacturers are steered toward frameworks like JSP because of the "use of device design processes such as those described in the QS regulation to support secure product development and maintenance."

Figure 2: JSP 1.0 Framework

[6]



Although JSP [6] does not reference the QSR, when a person doing development in a regulated environment sees a reference to "Design Control," QSR part 820.30 automatically comes to mind. This mental model is further reinforced with the use of concepts like Risk Management, and Complaint Handling, which are not particularly prominent in the QSR but become more familiar

in the language of international quality system standards such as ISO 13485 [5]. As mentioned previously, the CSG [2] rationale for the use of other frameworks like JSP [6] is that they contain device design processes described in the QSR. Thus, the focus will now turn to "Design Control" as described in JSP to identify and better understand these design processes.

Per JSP [6] and referencing Figure 2 once again, these design processes are:

- Design Input Requirements for Security
- System Requirements, System Hardening Standards
- Vulnerability Scanning
- Software Requirements, Secure Coding Standards
- Code Analysis
- Customer Security Requirements
- Patch Management Requirements
- Security Testing

SPDF & JSP ALIGNMENT

One initial observation about JSP [6] is that when providing examples of how to address risk assessments it uses the Confidentiality, Integrity, and Availability, or CIA triad, which is ubiquitous in the cybersecurity industry. In contrast, the CSG [2] prefers something more like CAAAU to capture the security objectives for a design:

C – Confidentiality
A – Authenticity
A – Authorization
A – Availability
U – Updateability

In the CSG [2], "Integrity" is replaced with "Authenticity" given the latter is a broader term that includes integrity. The point FDA makes is that you can maintain integrity of data from an un-authentic source hence the focus on making sure that the valid data is from a trusted source. "Authorization" is an important addition since privileges and permission for access are critical for device security. Finally, "Updateability" emphasizes the need for medical device manufacturers to be able to respond to discovered vulnerabilities with flexible designs that facilitate securely loading newer software versions into their medical devices that mitigate or address those vulnerabilities.

A second observation is that JSP [6] states that the Common Vulnerability Scoring System or CVSS "provides a way to characterize and assess the severity of a cybersecurity vulnerability" and suggests its use in the risk assessment activity. The use of CVSS is also mentioned in ANSI/AAMI SW96 [7], a recently published risk management standard that is now on the FDA recognized list. SW96 presents a balanced view of CVSS and defers to the MITRE rubric [8] on how one might adjust the vulnerability scoring as part of an acceptance criteria. This rubric was qualified by the

FDA as a Medical Device Development Tool or MDDT for post-market vulnerability assessment, and even the CSG [2] itself references the use of CVSS as such per its footnote inclusion [9].

However, the CSG [2] cautions the usefulness of CVSS in the context of premarket submission or the development of unreleased software and development within a SPDF. Hence, the use of CVSS as an assessment for risk acceptance may be at odds with the CSG, which states that "a premarket exploitability assessment could either assume a worst-case assessment and implement controls or provide a justification for a reasonable exploitability assessment of the risk throughout the TPLC and how the risk is controlled." This focus on the TPLC or Total Product Life Cycle steals the spotlight from CVSS, which by its very definition is intended for risk prioritization and not risk acceptance.

Further, to compare the Design Control processes in JSP [6] with the content of a SPDF per the CSG [2], let us start with the big picture view which is an excerpt from the CSG Table of Contents:

Whereas JSP [6] in Figure 2 rests upon quality system processes, namely, Risk Management, Design Control, and Complaint Handling, a SPDF in the CSG [2] rests upon Security Risk Management, Security Architecture, and Cybersecurity Testing pillars. The Security Architecture pillar contains the design processes which are represented in the Implementation of Security Controls. Hence, drilling down into the security controls from a SPDF presents the design processes in comparison to JSP as follows:

JSP	SPDF
Design Input Requirements for Security	Authentication
System Requirements, System Hardening Standards	Authorization
Vulnerability Scanning	Cryptography
Software Requirements, Secure Coding Standards	Code, Data, and Execution Integrity
Code Analysis	Confidentiality
Customer Security Requirements	Event Detection and Logging
Patch Management Requirements	Resiliency and Recovery
Security Testing	Firmware and Software Updates

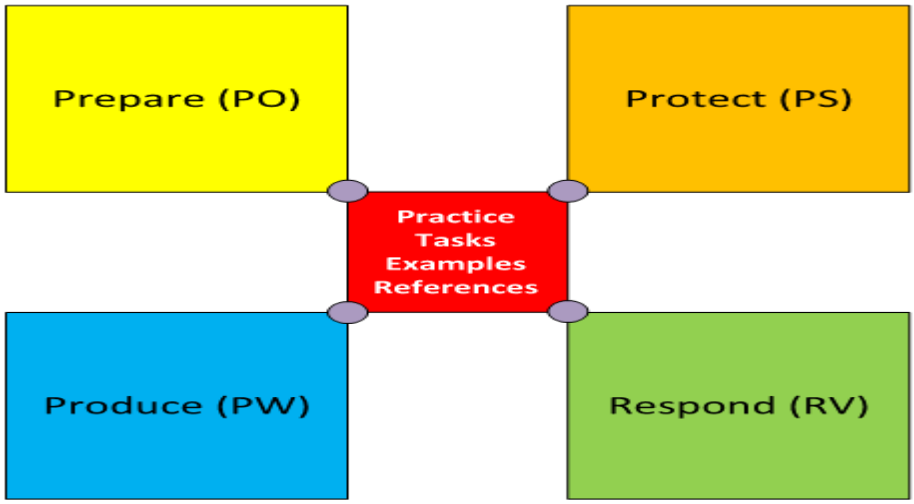
In essence, the CSG [2] focuses on security control categories for a SPDF that are intended to help meet the previously discussed CAAAU security objectives. While the CSG does emphasize that per the QSR in 21 CFR 820.30 that design output must evaluate to design input requirements, the security control categories are more high-level and so unlike JSP [6], the security controls do not focus on specific types of requirements and coding standards and address concerns like security requirements, code analysis, and vulnerability scanning under Cybersecurity Testing.

Without knowing anything about the ongoing JSP [6] revision work, it would not be surprising if some areas of JSP like the CIA triad, CVSS, and Design Control processes are reworked to be more aligned with the language in the CSG [2] even though the CSG seems to embrace JSP as it stands.

NIST SSDF AS A SPDF

As stated earlier, the CSG [2] recommends NIST CSF but only for medical facilities managing medical devices and not device manufacturers while overlooking the usefulness of NIST SSDF [10] for medical devices in any context. As shown in Figure 3, the NIST SSDF secure software development practices are organized into four groups where each practice includes a practice identifier, tasks, implementation examples, and references to practice documents.

Figure 3: NIST SSDF Framework



Revisiting the CSG [2] language once again, affinity for the JSP [6] framework seems to revolve around the inclusion of design processes described in the QSR, which support development and maintenance. Moreover, when comparing JSP with SPDF elements identified in the CSG, only Design Control related processes were considered. However, the Security Risk Management quality system process or pillar per the CSG is equally important and figures prominently in JSP. Likewise, for NIST SSDF [10], a SPDF Security Risk Management process stands tall as threat modeling, risk assessment, and third-party components are discussed within the four practice groups.

But how does NIST SSDF [10] measure up with respect to security controls within the Security Architecture pillar? While device design processes are emphasized in the CSG [2], it amplifies the fact that security must be "built in" and not "bolted on." Therefore, a SPDF addresses device design holistically by means of security controls. Listed below are the eight SPDF security controls [2] and then linkages to the abbreviated practice group example references to these concepts within NIST SSDF as follows:

SPDF Security Controls

1. Authentication
2. Authorization
3. Cryptography
4. Code, Data, and Execution Integrity
5. Confidentiality
6. Event Detection and Logging
7. Resiliency and Recovery
8. Firmware and Software Updates

SPDF Security Controls and NIST SSDF [10] Practice Group mappings where:

PO = Prepare Organization
PS = Protect Software
PW = Produce Well Secured Software
RV = Respond to Vulnerabilities

1. Authentication
    - PO.5.1, PO.5.2
2. Authorization
    - PO.5.1
3. Cryptography
    - PS.1.1, PS.2.1, PW.4
4. Code, Data, and Execution Integrity
    - PO.1.3, PS.1.1, PS.2.1, PS.3.2, PW.4.4
5. Confidentiality
    - PS.1.1
6. Event Detection and Logging
    - PO.5.1, PW.4.4, PW.5.1
7. Resiliency and Recovery
    - PO.5.1
8. Firmware and Software Updates/Patches
    - RV.2.2

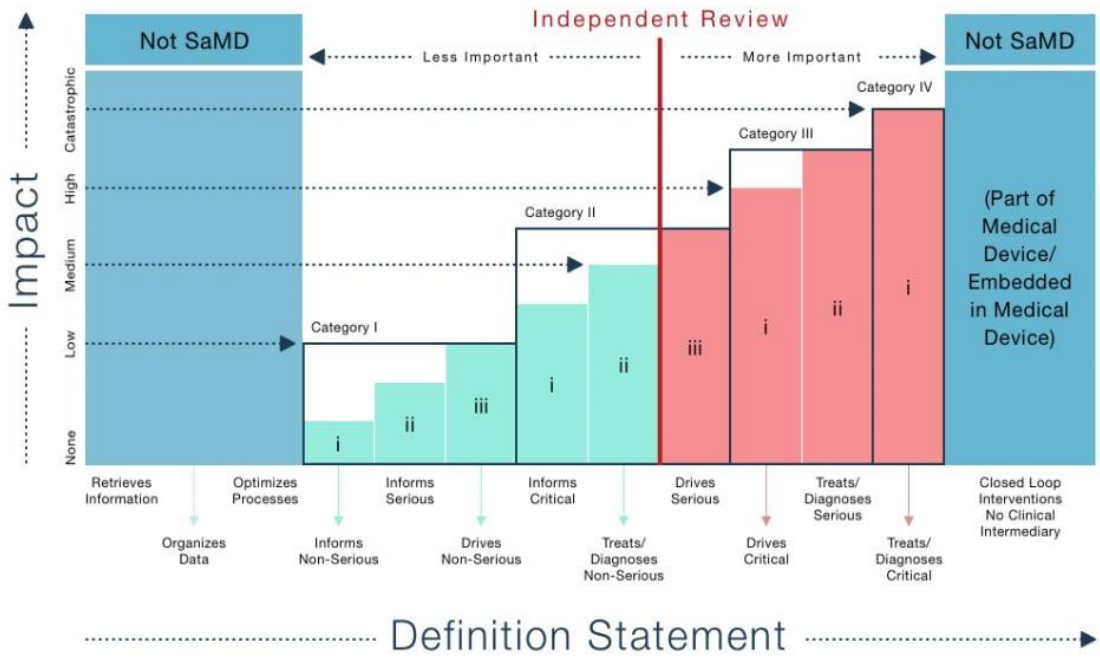
This list of security control references from NIST SSDF [10] is limited, abbreviated, and not exhaustive, yet sufficient to reveal a respectable coverage of the important controls emphasized in

the CSG [2] for a Security Architecture. Next, analyzing the final SPDF quality system pillar, Cybersecurity Testing, reveals that NIST SSDF identifies vulnerability testing, fuzz testing, penetration testing, and code analysis testing, all testing concepts called out in the CSG. Hence, in NIST SSDF, there is broad coverage of all three SPDF pillars, namely, Security Risk Management, Security Architecture Controls, and Cybersecurity Testing.

Perhaps suggesting NIST SSDF [10] is short-changed by the CSG [2] is an overstatement, but it was overlooked whether intentional or not. Thus, in defense of NIST SSDF, it seems plausible for someone to entertain its use for low to medium risk medical device applications. This includes both Software in a Medical Device (SiMD) and Software as a Medical Device (SaMD). For the latter, these low to medium risk Category I and Category II definitions identified by the International Medical Device Regulators Forum (IMDRF) [11] and then further by the FDA [12] are shown in Figure 4 below.

Figure 4: Medical Device Software Categorization

[12]



Unlike SiMD which operates on special-purpose computing platforms, SaMD targets are most often smart phones, tablets, and personal computers where an operating system is always involved as are libraries and APIs provided to make application development easier. In these environments there are many layers of software between the SaMD application and the actual hardware. For SaMD the software runs on a general-purpose computer, which by the nature of the software running, acts as a medical device. Given these types of general-purpose computing platforms are the host for IT and Enterprise applications that may make use of NIST SSDF [10] already, is it really a stretch to suggest the use of this framework as a viable option for use in medical device

software development, specifically lower risk applications that do not involve the more serious patient consequences or security concerns? Even the CSG [2] itself in the context of a SPDF states "Device cybersecurity design and documentation are expected to scale with the cybersecurity risk of that device." Unfortunately, the CSG does a poor job of providing further explanation. If the device design and submission documentation should scale, then why not a SPDF that governs this process? The recommendation of NIST SSDF in this paper is an attempt at suggesting such a scaling solution.

CONCLUSION

The recent changes to the FD&C Act in United States law regarding the management of cybersecure medical devices has in turn led to a change in thinking in the FDA resulting in a comprehensive CSG [2] that emphasizes the following:

- Cybersecurity is Part of Device Safety and the QSR
- Design for Security
- Transparency
- Submission Documentation

Emerging from this is a proposed SPDF which the CSG [2] describes in terms of security objectives, where the pillars to support this framework are identified as:

- Security Risk Management
- Security Architecture
- Cybersecurity Testing

Further, given a Security Architecture is achieved by certain design processes that align with the QSR, the FDA recommends specific frameworks like JSP [6] that can possibly be used to help satisfy criteria for a SPDF. This paper considered the use of JSP and went further in exploration of NIST SSDF [10], which is unreferenced in the CSG [2]. While not making the claim that NIST SSDF is as effective as JSP, this paper highlights what is offered in the framework in the context of the expectations laid out in the CSG for a SPDF in hope that it:

1. ***At least*** initiates some novel consideration of the use of NIST SSDF in broader contexts.
2. ***At most*** provides some input for another future revision of NIST SSDF that becomes even more accommodating for use in medical device development.

REFERENCES

[1] *Public Law 117–328 117th Congress* (2022, December). congress.gov. https://www.congress.gov/117/plaws/publ328/PLAW-117publ328.pdf

[2] *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (2023, September). fda.gov. https://www.fda.gov/media/119933/download

[3] *Medical Device Software Process Blackbelt* (2023, April). udemy.com. https://www.udemy.com/course/medical-device-software-process-blackbelt

[4] *Medical Devices; Quality System Regulation Amendments.* (2022, February). federalregister.gov. https://www.federalregister.gov/documents/2022/02/23/2022-03227/medical-devices-quality-system-regulation-amendments

[5] *Medical Devices-Quality management systems-Requirements for Regulatory Purposes* (2016). ISO 134585:2016/(R) 2019. iso.org. https://www.iso.org/standard/59752.html

[6] *Medical Device and Health IT Joint Security Plan* (2019, January). healthsectorcouncil.org. https://healthsectorcouncil.org/wp-content/uploads/2021/11/HSCC-MEDTECH-JSP-v1.pdf

[7] *Standard for medical device security-Security risk management for device manufacturers* (2023). ANSI/AAMI SW96:2023. ansi.org.

[8] *Rubric for Applying CVSS to Medical Devices* (2020, October). mitre.org. https://www.mitre.org/news-insights/publication/rubric-applying-cvss-medical-devices

[9] *Postmarket Management of Cybersecurity in Medical Devices* (2016, December). fda.gov. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

[10] *Secure Software Development Framework (SSDF) Version 1.1* (2022, February). nvlpubs.nist.gov. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

[11] *Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations* (2014, September). imdrf.org. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf

[12] *Software as a Medical Device (SAMD) Clinical Evaluation.* (2017, December). fda.gov. https://www.fda.gov/media/100714/download