AdvaMed
Advanced Medical Technology Association

701 Pennsylvania Avenue, NW
Suite 800
Washington, D.C. 20004–2654
Tel: 202 783 8700
Fax: 202 783 8750
www.AdvaMed.org

March 15, 2019

Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Room 1061
Rockville, MD 20852

Re: Docket No. FDA-2018-D-3443-0001: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff; Availability

To Whom It May Concern:

The Advanced Medical Technology Association ("AdvaMed") appreciates the opportunity to provide input on the Food and Drug Administration's ("FDA" or "Agency") Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff ("Draft Guidance").[1] AdvaMed represents manufacturers of medical devices, digital health technologies, and diagnostic products that transform health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.

Patient safety is the number one priority for the medical technology industry, and medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where technology constantly evolves. Medical device manufacturers make concerted efforts to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data.

AdvaMed's Board of Directors adopted foundational medical device cybersecurity principles[2] that, in addition to being received positively by many government agencies and other stakeholders, serve as a commitment by our industry to ensuring medical device cybersecurity threats are addressed in a meaningful way. Indeed, the first of the five principles—medical device development and security risk management—state that a firm's cybersecurity risk management program should address cybersecurity from medical device conception through disposal.

---

[1] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff (Oct. 18, 2018), *available at* https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm623529.pdf.

[2] AdvaMed Medical Device Cybersecurity Foundational Principles (Nov. 2016), *available at* https://www.advamed.org/sites/default/files/resource/advamed_medical_device_cybersecurity_principles_final.pdf.

We appreciate the Agency's efforts to provide specific, technical guidance for medical device manufacturers to consider as products are developed. However, we believe certain aspects of the Draft Guidance require further consideration, such as the two-tiered risk categorization. Additionally, there are proposed requirements in the Draft Guidance that would benefit from a legislative directive and/or formal rulemaking. Below we more fully address these areas. More detailed, specific feedback can be found in the enclosed chart.[3]

1. FDA Should Eliminate the Proposed Two-Tier Risk Approach

The Draft Guidance proposes an entirely new risk categorization framework based on two "tiers" to determine a product's premarket cybersecurity-related submission requirements. The Draft Guidance proposes that "premarket submissions for Tier 1 devices . . . include documentation demonstrating how . . . device design and risk assessment incorporate the cybersecurity design controls . . .," whereas for Tier 2 devices, FDA proposes that premarket submissions include such documentation or a risk-based rationale for why specific cybersecurity design controls are not appropriate. Draft Guidance at pp. 10–11.

This proposed framework is not rooted in statute or rule and the Draft Guidance acknowledges that the tiers "may not track to FDA's existing statutory device classifications." Draft Guidance at p. 10. We find this proposed two-tier framework confusing and unnecessary given its superficial similarity to FDA's risk classification scheme for medical devices. Moreover, there are significant differences between device types that could fit within the proposed tiers. We believe in such cases the recommended cybersecurity controls should differ accordingly. For example, small implanted medical devices, such as ICDs and pacemakers, have significantly more engineering constraints limiting their hardware and software capabilities when compared to larger medical devices used, for example, in a hospital setting.

We believe FDA should remove the two-tiered approach in favor of a single risk-based approach that addresses the Agency's cybersecurity expectations based on the exploitability of a device vulnerability and the severity of patient harm (if exploited), as outlined in the Agency's postmarket cybersecurity guidance. Doing so would be consistent with FDA's benefit-risk approach to device regulation and align with its "least burdensome" practices.

2. Cybersecurity Bill of Materials (CBOM)

The Draft Guidance "recommends" a number of new design control, labeling, and documentation criteria, inclusion of which "may make it more likely that FDA will find [a] device meets its applicable statutory standard for premarket review." Draft Guidance at pp. 8–9. This includes the proposed CBOM, which FDA states "can be a critical element in identifying assets, threats, and liabilities," and that "[l]everaging a CBOM may also support compliance with purchasing controls (21 CFR 820.50), by facilitating the establishment of requirements regarding cybersecurity for all purchased or otherwise received products."

[3] We note that in some instances the detailed comments in the enclosed chart assume the Draft Guidance's existing structure (*e.g.*, two-tier risk approach) is maintained.

Draft Guidance at p. 10. In its 2018 Medical Device Safety Action Plan,[4] FDA stated that it may seek new statutory authority to require device manufacturers to provide a "Software Bill of Materials . . . to FDA as part of a premarket submission and made available to medical device customers and users." Although FDA has not received new statutory authorities, the Agency nevertheless proposes that device manufacturers submit a CBOM as part of a product's premarket submission in the Draft Guidance.

The medical device industry believes that such documentation—in the form of a software bill of material ("SBOM")—can be a useful tool. Should FDA discuss within the final guidance a bill of material, FDA should reference an SBOM, instead of a CBOM, and define SBOM as:

> "A list of commercial off-the-shelf software or open source software components that are included in the medical device software, limited to version and build."

Providing and maintaining a BOM that includes hardware presents unique challenges compared to software-only BOMs, some of which are outside the immediate control of the manufacturer. For example, if components are sourced from a supplier, it may not be possible to obtain a list of all hardware subcomponents as suppliers may be unwilling or unable to provide such information. If the BOM were to include all software and all hardware down to the lowest component level, the sheer amount of data provided will very likely work against the shared goal to prioritize, prevent and react to cybersecurity risks to protect patient health.

Moreover, as FDA is aware, a number of industry groups and stakeholders are actively working to develop a standard form of an SBOM, working with NTIA and the U.S. Department of Commerce, and a Manufacturer Disclosure Statement for Medical Device Security (MDS2) is being piloted by the Medical Imaging & Technology Alliance. These efforts are looking at issues such as the type of information and level of detail that should be included in an SBOM; effective mechanisms for sharing SBOM information; and formats the SBOM should take, including available formats that can be leveraged and whether multiple formats would be able to co-exist. None of these efforts have contemplated the inclusion of hardware, and they also assume that cloud-based platforms, SaaS and other virtual environments are out of scope for the BOM. While in the long-term including hardware in the BOM may be a useful item, its utility, and ability to be properly managed, at this time is unclear.

Should FDA retain the requirement that device manufacturers provide a BOM, the Agency should clarify implementation expectations. For example, because FDA has not previously required documentation of a BOM, under the statutory "substantial equivalence" standard for Class II medical devices we do not believe FDA can impose these requirements on new

[4] *Available at* https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf

devices that have demonstrated substantial equivalence to a predicate device. FDA should explain its authority for such a requirement.

FDA must also explain the frequency by which it would expect a manufacturer to update the BOM. There are many potential triggers that could require an update. Some of these triggers are within the manufacturers control, such as a general software update. But some are not, such as when third party software used in a medical device is updated and/or patched. As a community, we must consider the impact BOM updates will have on the end user (*e.g.*, health delivery organizations). Health delivery organizations and other users of these BOMs will need to have mechanisms to monitor their updates and implement any needed changes to their own systems, which will require significant time and resources. It is therefore in the interest of all parties to work together to agree to an orderly process for updating these BOMs. Again, this is why it is important for FDA to allow the ongoing industry efforts to complete their work.

3. The Proposed Labeling Recommendations Should Focus on Product Communications

We recommend that FDA change existing recommendations relating to device labeling to recommendations about the types of information to be communicated to customers and/or end users, as appropriate, to foster transparency of the right information to the right user of that information. FDA's currently in force, final Premarket Cybersecurity guidance recommends that device manufacturers provide device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the device's intended use environment (such as the use of firewalls and deployment of anti-virus software). The Draft Guidance lists fourteen categories of information to be included in labeling to communicate security information to end users of medical devices, citing 21 C.F.R. § 801.5 (requiring labeling to include adequate directions for use) and 21 C.F.R. § 801.109(c) (requiring labeling for devices that are restricted to prescription use to include relevant hazards, contraindications, side effects, and precautions so the device can be used safely and as intended).

FDA appears to be stretching beyond the intent of the Agency's labeling regulations in that the detailed security information is outside what is necessary for adequate directions related to the intended uses to treat, prevent, mitigate, or diagnose a disease or condition (*i.e.*, uses that are shown to be customary or usual). In fact, FDA may need new statutory authority to define new device labeling requirements, particularly for devices that require premarket notification under section 510(k) of the FDCA. FDA must clear a premarket notification under section 510(k) if the submission demonstrates that the device is substantially equivalent to the predicate device. In order to demonstrate substantial equivalence, if a device has different technological characteristics from the predicate device, FDA can require "information, including appropriate clinical or scientific data . . ., that demonstrates that the device is as safe and effective as a legally marketed device." This does not mean that FDA has authority to require that a device employ different design or labeling elements that are not included in the predicate device.

Central to enhancing the shared responsibilities of cybersecurity is transparency of the right information to the right audience. While we recognize the merits of providing health care delivery organizations with appropriate information to address cybersecurity risks, we question characterizing this type of information as labeling in the traditional sense. Chief Information Officers, for example, are unlikely to review product labeling. Again, we recommend that FDA change existing recommendations relating to device labeling to recommendations about the types of information to be communicated to customers and/or end users, as appropriate, to foster transparency of the right information to the right user of that information. Additionally, to conform with this change, FDA should also remove item number 12 ("A CBOM"), lines 629-635, from the list of labeling recommendations.

4. Implementation of the Draft Guidance

FDA does not explain how and when the principles of the Draft Guidance will begin applying to device submissions, or how the Draft Guidance (when final) would apply to currently marketed products. Consistent with the Agency's Good Guidance Practices, 21 C.F.R. § 10.115, the device industry expects that the Draft Guidance would not be applied until it is issued in final form and FDA has thoroughly considered the public input it receives. However, we understand FDA already has required that 510(k) premarket notification submissions comply with the Draft Guidance and that recent Additional Information Request letters to device manufacturers have cited as deficiencies that insufficient information on cybersecurity was submitted to the Agency even though that information met the requirements of the currently in effect Premarket Cybersecurity Guidance.

For devices currently under development, many undergo years of development and testing prior to submission. It is not in the public interest to hold these currently in development or currently under review devices until FDA finalizes the Draft Guidance. Accordingly, we recommend that FDA adopt a phase-in period for the Draft Guidance for new (non-marketed) medical devices of one to two years.

Similarly, FDA does not explain whether and how the Draft Guidance will apply to currently marketed devices when a modification requires a new regulatory submission. Delaying or forgoing important product enhancements because an already marketed product does not address all elements of the Draft Guidance is not in the best interest of patients.

5. Forensic Design Elements

Device design is a benefit-risk process focused on intended use and patient safety. Devices are very diverse, having different purposes, use environments, and size. The Draft Guidance appears to set forth uniform cybersecurity design expectations (*e.g.*, Section V, B) without regard to this diversity and other considerations, such as computational resources, the absence of operating systems with file management systems, the fact that multiple data sources may be necessary to detect cybersecurity breaches, and how these cybersecurity design expectations relate to other key design elements that enable a device to perform its essential services. For example, battery life for certain devices is a higher priority to perform essential services than log files. Other mitigating measures may be better suited to address

cybersecurity while maintaining device essential services. The Draft Guidance is silent on how FDA reviewers will evaluate these design choices during submission reviews. Recognition of this aspect of the benefit-risk process within the Draft Guidance would be helpful, and additional guidance on this balance, for industry and FDA staff, is recommended.

* * *

AdvaMed would like to thank the FDA for its consideration of these comments and looks forward to continuing to work with the Agency on this important issue. Please do not hesitate to contact me at 202-434-7224 or zrothstein@advamed.org should you have any questions.

Respectfully submitted,

/s/

Zachary A. Rothstein, Esq.
Vice President
Technology and Regulatory Affairs

Attachment

AdvaMed Comments

**Content of Premarket Submissions for Management of Cybersecurity in Medical Devices;
Draft Guidance for Industry and Food and Drug Administration Staff
(Docket No. FDA-2018-D-3443)**

#	Line Number	Comment/Proposed Change	Rationale
	89-90	FDA should include a footnote about the WannaCry ransomware attack.	The guidance should reference factually nefarious examples affecting medical care.
	128	Prepend the following text to footnote 6: "As stated in section 201(h) of the FDCA, the term 'device' does not include software functions excluded pursuant to section 520(o) of the FD&C Act, as amended by the 21st Century Cures Act."	The guidance should reflect recent changes resulting from the 21st Century Cures Act. The proposed change is copied from footnote 1, Development a Software Precertification Program: *A Working Model*, version 1.0. Note, the draft FDA guidance, "Clinical and Patient Decision Support Software," also highlights software functions now excluded from the FDCA.
	128	We recommend FDA develop a new definition for "programmable logic" and include this definition in Section III.	Adding this definition will aid industry's understanding of the guidance.
	136	FDA should update Section III to include definitions provided in the FDA's postmarket cybersecurity guidance for the following terms: exploit, threat, and vulnerability.	The identified terms are fundamental in nature and will serve to educate readers who are new to the cybersecurity field. This change also aligns the guidance with the Agency's postmarket cybersecurity guidance.
	136	The term "cybersecurity incident" is used throughout the guidance and should be defined.	Adding a definition will aid industry's understanding of the guidance.
	136	We recommend FDA clarify whether "device" and "product" are used interchangeably in the guidance, or if the terms have different meanings.	The use of both terms in the Tier 1 definition in Lines 286-292 gives the appearance that the two terms may not be interchangeable.
	136	We suggest FDA review all uses of the term "user" and determine when the statement only applies to a human user, or if the machine-to-machine interaction requires the addition of "process," "system" or "device" (*e.g.*, definition of "privileged user").	The definition of "authentication" references "user, process, or device" as actors that can be authenticated. But elsewhere (*e.g.*, the definition of Confidentiality) it only references users.
	151	We recommend the phrase, "property of data" be modified to, "characteristic of data".	The term "property" has dual meanings. For example, property may refer to ownership or a property that helps characterize and classify. It would therefore be helpful to clarify the current language to indicate the interest is in the characteristic of data.

#	Line Number	Comment/Proposed Change	Rationale
	151-153	FDA should clarify that loss of essential services of a device may be more important to patient safety than loss of the information.	The definition of availability focuses on data and information availability, and not the essential services provided by the device. The term "information" encompasses not just data but also software instructions. *See, e.g.*, https://csrc.nist.gov/glossary/term/information. However, defining "availability" in cyber-physical systems as "the assurance that information will be available when needed" does not directly address the physical services provided by the systems (*e.g.*, therapeutic radiation provided by a medical device).
	151-153 155-159 185-186	We recommend including sources for the definitions for Confidentiality, Integrity, and Availability.	The definitions for Confidentiality, Integrity and Availability are fundamental. We recognize that the definitions are the same as those in the original premarket cybersecurity guidance issued on October 2, 2014.
	164-165	We recommend clarifying the meaning of "authoritative sources" and "sufficiently secure," and providing examples of these terms.	Clarification will aid industry's understanding of the guidance.
	179-180	We recommend revising the phrase, "being known or used," to: "being known or used by unauthorized agents."	As written, the text implies that encryption prevents data from being known to anyone. The definition from NIST SP 800-101 Rev. 1 conveys the concept more precisely ("Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data").
	182	Revise the definition of "end of support" as follows: "a point beyond which the product manufacturer ceases to provide ~~support, which may include~~ cybersecurity support~~,~~ for a product or service."	Adding a definition will aid industry's understanding of the guidance. Note, the first sentence of Section III limits applicability: "The definitions listed here are for the purposes of this guidance and are intended for use in the context of assessing medical device cybersecurity."
	196-197	We recommend removing the term and definition, "Patchability/Updatability."	The defined term "Patchability/Updatability" is not used within the body of the document.
	199-201	We recommend changing the second sentence that begins with, "Cybersecurity exploits . . ." to: "Note, cybersecurity exploits . . . ."	Clear definitions are essential to a predictable and consistent regulatory process. The second sentence is appropriately qualified to avoid misunderstanding.
	200, 240, 356, others	We recommend FDA remove "authenticity" from the list of potential losses that could result in risk or harm.	We do not believe it is helpful to have "authenticity" in the list of potential losses that could result in risk or harm. In general security

#	Line Number	Comment/Proposed Change	Rationale
		If authenticity needs to remain a consideration (*e.g.* as a pre-requisite for non-repudiation), FDA should update the definition in Line 145 to clarify that authenticity is a special case of integrity and that authenticity enables the principle of accountability.	literature, the "loss of integrity" (which is already listed) covers the concern that information could be maliciously manipulated.
	206-208	Delete lines 207-208 from the definition.	Clear definitions are essential to a predictable and consistent regulatory process. The current definition of "Quality of Service" is overly broad. Not all medical products have "measurable, end-to-end performance properties" that can be "guaranteed in advance by a Service Level Agreement." Moreover, these considerations are better left for commercial business agreements between two parties, rather than being set forth in FDA guidance.
	209	We recommend adding the following definition: "Resilience - the ability of a system or components to ensure maintenance and continuity of device safety and essential performance under degraded operating conditions (such as network outages, excessive bandwidth usage by other products, disrupted quality of service, or excessive jitter) and under exposure to security threats (such as Denial of Service attacks, attempts to install invalid software, or to execute unauthorized commands)."	This term is used in line 271, 544-547 and 548-552, but is not defined. The proposed definition is intended to aid industry's understanding of the guidance.
	210	Change the Risk definition to, "the combination of the exploitability of known or potential vulnerabilities and the severity of associated harm." Remove footnote to 14971. For purposes of clarity, FDA should also add a note below the definition of "risk" that states: "Likelihood assessments for security risks should leverage an analysis of exploitability not probability."	Footnote 23 and lines 343, 663, and 707 state exploitability should be used instead of probability, so defining risk-based on the probability-centric ANSI/AAMI/ISO 14971 text is contradictory. Consistent use of terminology benefits industry and FDA avoiding confusion between safety risk and cybersecurity risk. Further, this definition aligns with Health Canada and TGA cybersecurity definitions.
	242	We recommend replacing, "patient illness, injury, or death," with: "patient harm."	Harm can result in injury to the user of the equipment (*e.g.*, clinician, nurse or other healthcare professional) and to bystanders in the device's environment of use (*e.g.*, members of a surgical team who may not be operating a radiation device but would be subject to radiation effects in case of a critical safety malfunction).
	246	We recommend revising the phrase, "appropriate Cybersecurity Protections," to: "Cybersecurity Controls."	The suggested phrasing is more consistent with currently used terminology.

#	Line Number	Comment/Proposed Change	Rationale
	254	FDA should clarify what is meant by the phrase: "manufacturers of devices containing computer software."	It is not clear what is meant by this phrase. The presence of software does not indicate the device is automated. There may be portions of the device where software controls some aspects of the device, but the user of the device chooses settings that drive the therapy.
	264, footnote 23	We recommend the footnote be modified to state: "Likelihood assessments should include exploitability."	While we agree exploitability is important, in order to take a risk based, least burdensome approach, measures of probability may be appropriate.
	268	We recommend revising the term, "Hard-Wired," to simply, "Wired."	The definition of hard-wired is "permanently connected." There may be wired connected devices that are not intended to be "permanently connected."
	273	We recommend FDA replace the term "liabilities" with "vulnerabilities."	This is the only part of the guidance where the word "liabilities" is used.
	279	We recommend changing "probable risk of patient harm" to "likelihood of patient harm."	The guidance emphasizes that "likelihood assessments should leverage an analysis of exploitability not probability." To be consistent, the reference to "probable risk of patient harm" should be changed to "likelihood of patient harm."
	281	If tiers are retained, we recommend replacing, "FDA's premarket cybersecurity recommendations," with the following underlined text: "For purposes of this guidance, and to help clarify the level of cybersecurity design control documentation to provide in a premarket submission, we are defining two 'tiers' of devices according to their cybersecurity risk:"	For the reasons identified in our cover letter, we recommend FDA eliminate the proposed two-tier risk approach in which Tier 1 devices are to incorporate all the cybersecurity design features identified in the guidance document, regardless of the device's intended use or size. We recommend FDA use a single risk-based approach for the incorporation of cybersecurity design features/design controls. If tiers are retained they could relate to the depth and breadth of documentation provided in a premarket submission, with tier 2 devices containing summary information of the incorporated cybersecurity design features and risk assessment and tier 1 devices containing more detailed information.
	284, 300	Should FDA maintain its tiered approach, we recommend removing "higher cybersecurity risk" and "standard cybersecurity risk" and simply refer to Tier 1 and Tier 2.	This change will simplify terminology used in the document.

#	Line Number	Comment/Proposed Change	Rationale
	284-302	The guidance should include additional examples of complex connected systems and each tier-based classification of each system component.	Adding these examples will aid industry's understanding of the guidance.
	288-292	As we stated in our accompanying letter, we believe FDA should remove the two-tiered approach in favor a single risk-based approach that addresses the Agency's cybersecurity expectations based on the exploitability of a device vulnerability and the severity of patient harm (if exploited), as outlined in the Agency's postmarket cybersecurity guidance. However, if tiers are retained to distinguish the level of cybersecurity design documentation in the premarket submission, we recommend Tier 1 criteria be revised to state: "A device is a Tier 1 device if the following criteria are met: 1) The device is ~~capable of~~ intended to connect (*e.g.*, wired, wirelessly) to another medical or non-medical product, or to a network, or to the Internet; AND 2) ~~a cybersecurity incident affecting the device could directly result in patient harm to multiple patients~~ the device is life-supporting or life-sustaining as defined in 21 C.F.R. § 860.3(e)."	We recommend replacing the second prong with "life-supporting" or "life-sustaining" because this is a well-defined list that directly addresses the physical services provided by the systems, as it relates to patient safety. Such an approach aligns with past FDA action where patient safety crosses statutory Classification I, II, and III. For example, this approach was used when implementing UDI.
	329	We recommend changing the term "procedures" to: "principles" or "best practices."	Procedures indicate a specific process. Principles and best practices are referenced in line 471 of the guidance.
	334-342	If tiers are retained to distinguish the level of cybersecurity design documentation in the premarket submission, we recommend Tier 1 criteria be revised to state: ~~"We recommend premarket submissions for Tier 1 devices with higher cybersecurity risk to include documentation demonstrating how the device design and risk assessment incorporate the cybersecurity design controls described below. For Tier 2 devices with standard cybersecurity risk, w~~We recommend that manufacturers include documentation in their premarket submissions that either 1) demonstrates they have incorporated each of the specific design features and cybersecurity design controls described in this section, or 2) provide a risk-based rationale for why specific cybersecurity design controls, described in this section, are not appropriate. Risk-based rationale for Tier 1 devices should describe intended use scenarios, technological	Risk-based rationale, including risk-benefit analysis in accordance with ISO 14971, should be permitted for both tiers of devices. For example, some miniaturized low-power devices may not have the capability to "Employ a layered authorization model by differentiating privileges based on the user role (*e.g.*, caregiver, patient, health care provider, system administrator) or device functions." (lines 390-393) without jeopardizing the intended use and/or longevity of the device. Further, for some devices whose intended use encompasses emergency department scenarios, inclusion of a listed control may lead to new types of hazardous situations (*e.g.*, a clinician not being able to access a medical device in a timely manner).

#	Line Number	Comment/Proposed Change	Rationale
		limitations, or risk-benefit trade-offs that preclude the implementation of specific control(s).	
	343	We recommend FDA define the term, "likelihood," and clarify whether quantification of likelihoods is expected. If quantification is not needed, FDA should explain how likelihoods must be expressed so they can facilitate both exploitability-based rationales in security risk analysis, and the P1 and P2 quantification that is required for hazard analysis pursuant to ISO 14971.	It is unclear if "likelihood" means "likelihood of occurrence" (weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability, per AAMI TIR-57), "likelihood of patient harm due to a successful cybersecurity breach" (Line 279), or something else. If manufacturers refrain from estimating probabilities in the security risk analysis, it is unclear how "likelihood" should be transformed to P1 (Probability of a hazardous situation occurring) and P2 (Probability of hazardous situation leading to harm) when the security risk analysis feeds the hazard analysis for those security risks that are associated with hazards.
	342-344	We recommend revising the sentence to: "Risk-based rationales should leverage an analysis of exploitability that reflects the ease and technical means by which a vulnerability could be exploited."	As currently written, it is not clear that "an analysis of exploitability" includes analysis of foreseeability or probability.
	342-344	The guidance should provide illustrative examples related to the statement, "Risk-based rationales should leverage an analysis of exploitability to describe likelihood instead of probability." In particular, for those vulnerabilities with the potential to cause "harm" as defined in ISO 14971, the document should compare and contrast exploitability with probability.	Adding these examples will aid industry's understanding and implementation of the guidance.
	346, 373	FDA should clarify what is meant by the terms "comparable" and "equivalent" cybersecurity design controls.	This information would assist the reader's understanding of the guidance document.
	349-350	We recommend including guidelines for documenting pre-submission discussions related to product cybersecurity design including the design element discussed, the manufacturer's recommended design, and, if FDA concludes the design is inadequate from a benefit/risk perspective, the Agency must provide a clear articulation of the reason why the manufacturer's design was inadequate. Without clear agreement and understanding, product development and deployment could be hampered.	Use of the pre-submission process to discuss design considerations can be an effective process. Subsequent redesign of products is inefficient and costly to the ecosystem.
	356	We recommend removing, "authenticity."	Authenticity is covered by integrity and confidentiality.

#	Line Number	Comment/Proposed Change	Rationale
	370-371	We recommend that FDA clarify what is meant by the phrase, "safety-critical."	Providing this information will aid industry's understanding of the guidance.
	386	We recommend the following revisions: "Limit access to devices through the authentication of users (*e.g.*, user ID and password, smartcard, biometric) or other system components (*e.g.*, unique implantable device characteristics, a security certificate or similar.)"	Limiting access to only authenticated users will dramatically impede home monitoring of pacemaker and defibrillator patients. These systems are designed to monitor patient and implanted device status (after device-to-device authentication) without user authentication, with well-demonstrated clinical benefits.
	394	We recommend FDA change this section to: "use authentication appropriate to the role of the user, process or device," and make the list of examples in parenthesis part of the description of the control.	"appropriate authentication" is ambiguous.
	398-403	We recommend revising the language to: "Strengthen password protection as appropriate for the intended use environment. For example, do not use credentials . . . ."	We appreciate the desire to mitigate risk that arises based on access controls and credentials, but from a practical perspective customer needs will vary based on the intended use of the device and clinical setting. For example, hospital emergency departments are typically physically controlled, with numerous and rotating staff working under stressful conditions. Access controls on devices used in these settings are often bypassed in these circumstances, such as by attaching user credentials to the product exterior. FDA may wish to consider: (a) recommending that manufacturers distribute the product in a secure configuration by default; (b) recognizing that health care providers may be allowed to alter that configuration within a predefined, risk-based based range of options; and (c) expecting that manufacturers communicate to customers the potential risk(s) associated with each configuration option.
	402-403	We recommend revising this sentence to: "Shared passwords should be avoided, but when they are required access to shared passwords used for privileged device access must be controlled including regular reviews of authorized access and updating passwords routinely to reduce the risk of exposure from previously authorized individuals."	As written, the guidance implies that shared passwords are acceptable. We believe the guidance should first state that shared passwords should be avoided, but if they are required, they must be controlled.
	404-405	We recommend removing this bullet (vi).	Physically locking a medical device and its communication ports is the responsibility of customers.
	406	We recommend deleting the phrase: "of Safety-Critical Commands."	This change is a clarification to section (b) which focuses on authentication and authorization.

#	Line Number	Comment/Proposed Change	Rationale
	411-413	We recommend the following revision: "Require authentication before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware."	Pacemakers, defibrillators and associated monitoring products are generally not capable of user authentication but can authenticate connected systems to some degree. In addition, for medical apps running on third-party mobile platforms (*e.g.*, smartphones), software updates are typically managed by the operating system and are not the under app's or medical product manufacturer's control.
	417	We recommend deleting the word, "all."	It may be technologically prohibitive to authenticate certain connections.
	417-420	The intent and scope of this requirement is not clear. We recommend FDA provide examples including those in the context of a hospital and laboratory network.	Mutual authentication generally applies to communicating through TCP/IP internet.
	421-427	We recommend FDA add, "For example," to the second sentence.	As currently written, this clause is problematic for medical apps that run on third-party mobile devices (*e.g.*, smartphones). Although the operating system typically verifies app authenticity using methods along these lines, mobile platform companies typically do not provide design or verification evidence in accordance with FDA guidelines.
	421-426	We recommend separating this section of the guidance into two different items: "v) 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/have MACs. vi) Devices should be electronically identifiable (*e.g.*, model number, serial number) to authorized users." Furthermore, we recommend FDA not request MACs for software because it is outdated. Precise security requirements should not be prescribed because of the evolving nature of technology.	These statements are two separate requirements.
	429-430	We recommend changing the second sentence to: "For example, authenticate external systems."	This clarification would be helpful to understand the application the guidance.

#	Line Number	Comment/Proposed Change	Rationale
	432	The term, "signal of intent," for authentication/authorization is not a security best practice and we recommend FDA elaborate on the use of this term.	The term is vague and subjective as currently used.
	435-439	We recommend the following revisions: "Devices should be designed to 'ignore by default,' *i.e.*, that which is not expressly permitted by a device is ignored by default. For example, the device should generally ignore all unauthorized connections (*e.g.*, incoming TCP, USB, Bluetooth, serial connections)."	Systems that send a response to unauthorized commands or connections can unintentionally equip an attacker with information about authorized commands, or about the software that issued the response (which may have known vulnerabilities). To prevent this issue from occurring, it is better to avoid returning any such information.
	440-441	We recommend moving section viii to the paragraph describing expectations for authorization starting at line 376.	This provision is not a specific requirement. Roles should be grouped into appropriate grants of authorization to manage the complexity and risk of the system.
	464-466	We recommend revising the sentence so it begins with: "Where feasible." The guidance should provide variability of strength based on the intended protection interval the cryptography being used because the strength needed is dependent on the application of the cryptography. This can become an issue for battery powered devices such as implants.	Current NIST standards may not be feasible for all medical devices (particularly older designs), which lack sufficient computational power to implement cryptography on all communication channels.
	467-469	We recommend deleting the phrase, "per device."	The phrase, "per device," could be interpreted to indicate that the same device version sold to different customers should have their unique communication key pairs, which may be difficult to achieve.
	471-473	We recommend FDA explain how a manufacturer should determine what is an "industry-accepted best practices to maintain/verify integrity of code."	Elaborating on this statement will aid the reader.
	476	We recommend revising this sentence to: "whose disclosure could likely lead to patient harm."	Product design should be driven by more than theoretical risk.
	476	We recommend FDA provide additional examples that illustrate best practices applied to ensure data confidentiality.	Adding these examples will aid industry's understanding and implementation of the guidance.
	491-491	We recommend adding the following phrase: "Where appropriate to the device class and function."	Many of the controls in this section are appropriate for medical devices that are standalone. For Class III devices, due to the small

#	Line Number	Comment/Proposed Change	Rationale
			size constraints, many of these controls may interfere with the device's essential performance. Scanning the device as "normal performance" should not be allowed. The device should be designed to only respond to authorized commands.
	497	We recommend FDA delete the phrase: "in a timely fashion."	This is a subjective term.
	499-501	We recommend the following revisions: "When appropriate and feasible, i~~I~~mplement design features that allow for security compromises to be detected, recognized, timed, and acted upon by users and operators during normal use."	Manufacturers should log relevant events required to determine if a system has been compromised, rather than simply logging security compromises.
	505-510	We recommend the following additions to this text and to lines 618-622: "Where feasible, the design should include mechanisms to create and store a security event log. Documentation should include how and where the log is located, stored, recycled, archived, and how it could be used by forensic investigators." FDA should also clearly indicate that manufacturers can provide the capability, but the customer needs to allow implementation.	Log files are more applicable to operating systems with file management capability. Not all devices will have such operating systems, although logs can be generated in other ways. This change (*i.e.*, from "log files" to "log") makes these requirements more broadly applicable.
	507	Regarding the sentence starting with "Documentation," we believe it should be moved to the customer documentation section of the guidance.	Ensuring a control is documented properly is not appropriate for this section, but it is appropriate within section VI (labeling and customer documentation).
	514 – 518	We believe this item should be moved to the customer documentation section of the guidance.	Ensuring a control is documented properly is not appropriate for this section, but it is appropriate within section VI (labeling and customer documentation).
	519-522	We believe FDA should add to the beginning of clause (e): "When feasible,".	As written, this provision is overly broad. For example, it may not be feasible for implanted pacemakers and defibrillators (particularly older designs), which lack sufficient computational resources, to implement this control measure. This is also not feasible for medical apps running on third-party platforms (*e.g.*, smartphones), because software changes are managed at the platform level using designs that are not under control of the medical app manufacturer.
	523-525	We recommend revising the sentence to:	The terms "horizontally" and "vertically" have been used in FDA's guidance concerning postmarket management of cybersecurity.

#	Line Number	Comment/Proposed Change	Rationale
		"The product life-cycle, including its design, should facilitate ~~a variant analysis~~ an impact analysis horizontally and vertically of a vulnerability across device models and product lines."	
	526-527	We believe this item should be deleted.	This design element is not practical or necessary. The BOM is a physical document still under development. To expect production by devices is not practical at this time.
	530-531	We recommend removing this sentence.	The forensic information and alerts that support customer security monitoring and incident response are already captured in lines 499-511. Detecting potential cybersecurity breaches usually requires correlating data from multiple sources; this is not a medical device functionality.
	532-533	We recommend FDA change the phrase, "anticipate the need for," to, "accommodate."	The proposed change clarifies that a software device, as currently defined in the guidance, should be designed to accommodate patches and updates as an accepted design practice.
	534-537	We recommend the sentence be revised to state: "The maintenance plan for a device should be designed to facilitate the ~~rapid~~ verification, validation, and testing of patches and updates, consistent with the Agency's postmarket cybersecurity guidance."	Not all patches and updates demand the same level of urgency. For example, verification, validation and testing of an improvement feature would not require the same timing as a critical patch to address or prevent a significant cybersecurity risk.
	542-543	We recommend the following addition: "The design should provide methods for retention and recovery of device configuration by an authenticated privileged user or system."	Individual user authentication is not feasible for a pacemaker or ICD; patients move and travel and so are seen in different clinics, so the implantable device can't maintain an accurate list of authorized users (for example, a particular healthcare delivery organization or provider). These devices can authenticate the system that is providing the update, but not the user.
	544	We recommend replacing the word "autonomous" with "independent" or "modular."	The phrase "autonomous" does not fit well into the definition of resilience.
	577	We recommend that FDA clarify how to determine the appropriate "end-user" and who would be expected to be notified and the type of information included in the notification.	Even though a device may have good cybersecurity controls that lower the cybersecurity risk to an acceptable level, there can be unforeseen changes (*e.g.*, a crypto cipher is deprecated due to a discovered design flaw). The end user may not be the appropriate party, it may be the IT or biomedical engineers that approve access to the hospital's networks.

#	Line Number	Comment/Proposed Change	Rationale
	584-585	We recommend the sentence be revised to state: "Specifically, we recommend the following be ~~included in labeling~~ provided to end users through nonpublic channels".	We recommend manufacturers be permitted to provide sensitive cybersecurity information in methods other than traditional labeling. It is understood that providing cybersecurity vulnerabilities will help end users prioritize and prevent cybersecurity risks. However, labeling information is typically available to the public. Allowing manufactures to facilitate the methodology for how sensitive cybersecurity information is transmitted will ensure end users receive the information while helping to prevent unauthorized access to such sensitive information.
	591-592	We recommend FDA remove item 2: "A description of the device features that protect critical functionality, even when the device's cybersecurity has been compromised."	The description recommended in item 2, if publicly disclosed, could provide malicious actors with sensitive information that could enable the development of new – and potentially catastrophic – attacks. For many devices, public disclosure of features "that protect critical functionality" would significantly reduce effectiveness of defense-in-depth strategies.
	605	We recommend FDA describe how the port configuration information in the labeling should be distributed so only legitimate and trusted customers can access the information.	It is unclear on how sharing the port configuration provides security. Attackers would benefit from knowing this information.
	618-622	We recommend FDA remove item 9: "A description of how forensic evidence is captured, including but not limited to any log files kept for a security event. Log files descriptions should include how and where the log file is located, stored, recycled, archived, and how it could be consumed by automated analysis software (e.g., Intrusion Detection System, IDS)."	The description recommended in item 9, if publicly disclosed, could provide malicious actors with sensitive information that could enable the development of new – and potentially catastrophic – attacks. If a malicious actor is provided details about "what is being monitored" then they will pursue specific types of attacks to maintain their anonymity. Manufacturers should be encouraged to work with health care providers to securely provide this information.
	647	Industry would benefit from being able to review cybersecurity process and design exhibits as part of the presubmission process without having to include all the information in the premarket submission in order to prevent overburdening the PMA review process.	N/A
	647-745	FDA should clarify whether the documentation listed in Section VII needs to be maintained within the manufacturer's Quality System or	Additional information from FDA is needed to understand the application of this guidance.

#	Line Number	Comment/Proposed Change	Rationale
		if it would be acceptable for some of the documentation to be maintained as regulatory submission records.	
	649	Additional detail on how to present information in a substantial equivalence discussion would be helpful. For example, if a 510(k) is submitted for changes to a Tier 1 device but the change itself does not have cybersecurity implications, should a manufacturer "catch up" the device's file to include all the cybersecurity reports/risk assessment performed to date to be compliant with the guidance? If the predicate is a legacy device that did not include cybersecurity information in its submission, how should a manufacturer demonstrate Substantial Equivalence?	Additional information from FDA is needed to understand the application of this guidance.
	658-663	We recommend FDA combine item 1 (line 658) and item 2 (line 660) to a single item, and add the following language to be consistent with our proposed change to lines 334-342: "~~2~~1. ~~For Tier 2 devices, d~~Documentation that addresses each recommendation in Section V or include a risk-based rationale for why a cybersecurity design control was not necessary. Risk-based rationale for Tier 1 devices should describe intended use scenarios, technological limitations, or risk-benefit trade-offs that preclude the implementation of specific control(s). Risk-based rationales should leverage an analysis of exploitability to describe likelihood instead of probability."	A risk-based rationale, including risk-benefit analysis in accordance with ISO 14971, should be permitted for both tiers of devices. For example, some miniaturized low-power devices may not have the capability to "Employ a layered authorization model by differentiating privileges based on the user role (*e.g.*, caregiver, patient, health care provider, system administrator) or device functions." (lines 390-393) without jeopardizing the intended use and/or longevity of the device. Further, for some devices whose intended use encompasses emergency department scenarios, inclusion of a listed control may lead to new types of hazardous situations (*e.g.*, a clinician not being able to access a medical device in a timely manner.).
	664-684	We recommend FDA further elaborate on what is meant by "system" and "system-level."	It is unclear how this would apply in practice. For example, for an infusion pump, would the system scope only include the components of the pump itself or also include the gateway?
	671	We recommend FDA clarify what is meant by "state diagram."	It is unclear what security states or behaviors are expected to be represented.
	677-678	We recommend FDA remove item (d): "Users' roles and level of responsibility if they interact with these assets or communication channels."	Typically, a manufacturer does not have complete visibility to "roles and level of responsibility" established by health care delivery organizations.
	719-722	FDA should provide additional information concerning when penetration testing and similar testing is expected.	It is unclear when penetration testing and similar tests would need to be performed and on what types of products.

#	Line Number	Comment/Proposed Change	Rationale
	722, 733	We recommend FDA change the phrase, "Test reports should," on line 722 to: "Test reports, including those provided by third parties, should include." We also recommend FDA append to line 733 to the end of item (h): ", if available."	The inclusion of this item in the list of test report content appears to recommend third-party testing for all product submissions.
	723	We recommend FDA clarify what is meant by the phrase, "testing of device performance."	Clarification will aid industry's understanding and implementation of the guidance. This item appears to be redundant; sub-points (c)-(h) are types of testing that provide evidence for (a) and (b).
	724-725	We recommend providing further clarification and/or examples for "evidence of security effectiveness of third-party OTS software in the system."	It is not clear whether the evidence of security effectiveness of third-party OTS software in the system means the effectiveness of the security risk controls implemented in the OTS software, or the security controls implemented in the medical device software addressing the security risks from third-party OTS software. If it references the former, it is not within the responsibility of the medical device manufacturer. If it references to the latter, the work is already included in bullet 5 (line 735-737) of the same section.
	733	We recommend deleting item 4(h).	This item is not necessary; any of the recommended types of testing can be performed by MDMs or third parties, but third party test reports should not be required for every medical device.
	745	For tests that are not deemed necessary or appropriate to establish the cybersecurity risk control, regardless of tier/other classification mechanism, justification/rationale for not performing testing should be acceptable, with documentation of the rationale in the Risk Management Report.	This information would benefit FDA and assist the manufacturer in documenting their internal deliberations.