Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions - Draft Guidance
June 14, 2022

Moderator: CDR Kimberly Piermatteo

CDR Kimberly Piermatteo: Hello and welcome to today's CDRH webinar. Thank you for joining us today. This is Commander Kim Piermatteo of the United States Public Health Service, and I serve as the Education Program Administrator and the Division of Industry and Consumer Education in CDRH's Office of Communication and Education. I'll be your moderator for today's program.

Our topic today is a draft guidance titled, “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.”

As medical devices have become more interconnected, cybersecurity threats have become more numerous, more frequent, more severe, and more clinically impactful. As you'll learn more today, FDA recognizes adequate medical device cybersecurity is essential to ensuring medical device safety and effectiveness and FDA recommends certain content be included in premarket submissions to address cybersecurity concerns.

We're holding this webinar to provide you with an opportunity to learn more and to answer any questions you may have about this draft guidance.

It's my pleasure now to introduce you to our presenter for today's program, Matthew Hazelett, Cybersecurity Policy Analyst within the Clinical and Scientific Policy Staff in CDRH's Office of Product Evaluation and Quality or OPEQ. We'll begin with a presentation from Matt and then field your questions about this topic.

Thank you all again for joining us today. I'd now like to turn it over to Matt.

Matthew Hazelett: Thanks, Kim. As she mentioned, I'm Matt Hazelett. And I'm the Cybersecurity Policy Analyst in the Office of Product Evaluation and Quality at the Center for Devices and Radiological Health. And I'll be leading today's presentation on the draft guidance.

Today's webinar will go over the draft guidance of “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.” The URL for the guidance is provided on the slide and will be available following today's webinar.

As a few general reminders, you may comment on any guidance at any time. For draft guidances, please submit your comments on draft guidance before the closure date of the public comment period. This will help ensure the FDA considers your comment on the draft guidance before we work on the final guidance. For today's presentation, this is a draft guidance. The recommendations discussed today are proposals and may change based on public comment.

There are four primary learning objectives for today's webinar-- to describe the updates from the 2018 draft guidance, to describe the general principles proposed in the draft guidance, to describe the proposed design and documentation recommendations, and to describe the proposed transparency recommendations.

We will begin by discussing the major updates from the 2018 draft guidance.

We'll begin with the guidance title change. The 2014 final Premarket Guidance and the 2018 draft revision to the Premarket Guidance had the title of "Content of Premarket Submissions for Management of Cybersecurity and Medical Devices." We changed the title for this draft to reflect the expanded scope of the guidance and the increased focus on how cybersecurity fits into the Quality System Regulations.

The guidance also provides greater detail from that which was included in the 2014 final Premarket Guidance on how FDA recommends cybersecurity be incorporated into device design and total product life-cycle maintenance. It also outlines how Quality System Regulation aligns with the Secure Product Development Framework, which we'll discuss in greater detail later. It also highlights the importance of Quality System Regulation integration as some medical device manufacturers have not fully incorporated cybersecurity into their quality systems.

I want to highlight some of the major content differences that are included in this update from the 2018 draft. The expanded scope of this draft guidance provides more detail on how cybersecurity aligns with the Quality System Regulations. It also recommends for the assessment of the system and not just the end device in isolation to ensure all the relevant cybersecurity risks are appropriately addressed by the end device design. This assessment of the system considers factors of the environment of use, like the software update Infrastructure, network connectivity, and things like cloud-based services that are used in conjunction with the end device.

The document has also been aligned with a Secure Product Development Framework structure. Secure Product Development Frameworks exist as best practices within the medical device sector and other sectors and is potentially one way to meet the alignment recommendations with the Quality System Regulations. We also have removed the risk tiers for devices that were originally proposed in the 2018 draft. We removed these risk tiers based off of the public comments and to encourage all manufacturers to appropriately consider cybersecurity risks and noting that cybersecurity documentation will naturally scale with cybersecurity risks.

Additionally, we have changed the cybersecurity bill of materials from the 2018 draft to now using a Software Bill of Materials or SBOM. This is in alignment with larger industry and sector efforts on the creation and use of SBOMs. It's also in alignment with Presidential Executive Order on improving the Nation's cybersecurity. We have also included more detailed recommendations for premarket submission documentation.

This is intended to increase the clarity on documentation and labeling recommendations to help improve the review process and review consistency. We've also added Investigational Device Exemptions, or IDEs, to scope with a subset of documentation recommendations. This was done to both ensure cybersecurity is designed into the device and also to ensure patients are informed of cybersecurity risks for the devices that they're using in clinical investigations.

In terms of proposed scope, this guidance document is applicable to devices that contain software, including firmware or programmable logic, as well as Software as a Medical Device, or SaMD products. This would mean that devices within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act, would it be applicable whether or not they require a premarket submission.

This is to say, the device is exempt from premarket submission requirements but still be recommended to follow this guidance. Also, as we've based the scope of the guidance to devices that contain or are software-based products or have programmable logic, we're not limiting this guidance to devices that are network-enabled or contain other connected capabilities, as the software and firmware level are aware cybersecurity risks are introduced.

For devices that do require a premarket submission, this slide provides the applicable submission types, including Premarket Notification or 510(k) submissions, De Novo requests, Premarket Approval Applications, or PMAs, and PMA supplements, Product Development Protocols, Investigational Device Exemption submissions, and Humanitarian Device Exemption submissions.

We will now go over the proposed general principles outlined in the draft guidance.

The proposed general principles included in the draft guidance outlines the things that are recurring topics throughout the guidance document. The first general principle is that cybersecurity is a part of device safety and the Quality System Regulation.

Within this section, we go into details of how we believe that cybersecurity is a part of safety and effectiveness. We also outline how cybersecurity aligns with the Quality System Regulations. And we further describe how we believe that a secure product development framework can be used to fulfill aspects of the Quality System Regulations.

The second general principle is around designing for security. In this section, we discuss in detail how we believe the designing in rather than bolting on cybersecurity controls leads to more effective device security. We also outline the key security objectives medical devices should achieve and that FDA would plan to assess devices for during their premarket submissions.

The third proposed general principle is around transparency. In this section, we discussed the importance of the end user having cybersecurity information to ensure the continued safe use of the device. This information includes both labeling provided with the device to the users as well as vulnerability information being provided to users throughout the lifecycle of the device.

The fourth proposed general principle is around submission documentation. In this section, we detail how recommendations give this guidance complement and are in addition to those included in the premarket software guidance. We also discuss how documentation is expected to scale with the cybersecurity risk of the device. So with the elimination of the risk tiers proposed in the 2018 draft, we believe the documentation is going to naturally scale with the cybersecurity risk of the device.

I'll now go into an overview of the proposed design and documentation recommendations included in the draft guidance.

The proposed design recommendations in the draft guidance focus around the security objectives for design, which are introduced in the General Principle section of the guidance. The security objectives are intended to be those items which FDA will assess devices against by how the device design provides for meeting these security objectives. The objectives outlined are authenticity, which includes the integrity of information, authorization, availability, confidentiality, and the secure and timely updateability and patchability of the medical device.

In section V of the draft guidance, we recommend eight security control categories to help in meeting the security objectives mentioned on the prior slide. The eight security control categories are intended to provide additional details in how design considerations can be made to ultimately meet the design security objectives.

Appendix 1 of the draft guidance provides specific control recommendations and implementation guidance for consideration to avoid common pitfalls associated with each of the eight control categories. I want to highlight that the appendices are part of the document recommendations and that when compared to other documentation types where appendices may be only informative or only provide examples, these appendices are part of the document recommendations and, therefore, are part of the guidance document overall and not only informative.

The proposed documentation recommendations for the guidance are spread across sections V and VI. Within section V, which is using an SPDF to manage cybersecurity risks, we provide recommendations around security risk management documentation, security architecture documentation, and cybersecurity testing documentation. Section VI on cybersecurity transparency provides recommendations on labeling and vulnerability management plans. The transparency section will be discussed in greater detail in the next section of this guidance, but the next slides will go into detail of the documentation recommendations outlined in section V.

In Section V of the draft guidance, we've outlined proposed security risk management documentation recommendations. These include the system-level of assessment accounting for factors of the environment of use, as we discussed earlier. It also outlines how security risk management is recommended to be distinct from safety risk management but that the two processes should feed into and out of one another to ensure the completeness of the assessment.

Based off of differences between cybersecurity risks and other potential risks of the system, we also recommend the use of exploitability assessments for security risks. And we also highlight how premarket exploitability assessments may differ from postmarket assessments. Further, we make recommendations how known vulnerabilities should be assessed as reasonably foreseeable risks to the system. And we also recommend that risk transfer should only occur if all relevant information is known, assessed, and communicated to users.

The security risk management section also makes documentation recommendations around the five items shown on the slide. In the Threat Modeling section, we recommend the documentation includes the full system and lifecycle of the device. In the Third-Party Software Components section, we make documentation recommendations around the Software Bill Of Materials and its associated vulnerability assessment.

In the Security Assessment of Unresolved Anomalies, section we make recommendations how anomalies can present a different vector to safety risks through cybersecurity and, therefore, security assessments needed for unresolved anomalies. For Security Risk Management Documentation, we outline aspects that we recommend to include in a security risk management plan and report. Finally, in the Total Product Life Cycle Security Risk Management section, we discuss recommendations around maintaining resources and documentation throughout the lifecycle of the device as well as the tracking and monitoring of cybersecurity measures and metrics.

While all of the security risk management recommendations are important, there has been a lot of focus on the Software Bill of Materials section of the guidance, so we want to spend some additional time discussing these recommendations.

On this slide, we include the recommended elements included in the draft guidance, which include the assets where the software components resides, the software component name, the software component version, the software component manufacturer, the software level of support provided through monitoring and maintenance from the software component manufacturer, the software component's end-of-support date, and any known vulnerabilities.

We acknowledge that some of the recommended elements included in the draft guidance and as listed on the prior slide extend beyond some of the minimum elements for SBOM that have been developed as a part of some of the industry and sector efforts for SBOM development. While we understand that these recommended elements extend beyond those, we wanted to try to address any concerns with these items by highlighting some of the language we included in the draft guidance.

We've indicated that industry-accepted formats of SBOMs can be used to provide this information to FDA. However, if any of the elements are not captured in such an SBOM, we recommend that those elements be provided typically as an addendum to FDA for the purposes of supporting premarket submission review. This is to say that industry-accepted formats can be provided, and any of the elements which are not captured in those can be provided separately from the industry-accepted format to FDA for the purposes of premarket review. I also wanted to highlight that SBOMs provided to users in labeling, we recommend, can conform with industry-accepted formats.

In addition to security risk management, we also want to discuss the documentation recommendations for the proposed architecture views. As we identify in the draft guidance, these views can be part of the threat modeling documentation. In the guidance, we outline four different view categories to be provided in submissions.

We recommend that manufacturers provide a Global System View of the overall system in all of its various elements so that we can get the appropriate system context. We also recommend the inclusion of a Multi-Patient Harm View to be able to understand the potential risks that can lead to multi-patient harms.

We also recommend for an Updateability and Patchability View. This is to provide information on how the device will be updated and patched through an end-to-end cycle. We also recommend for the inclusion of Security Use Case Views. These views are recommended to cover operational states in different clinical use cases. This is a way of ensuring that the cybersecurity documentation can help ensure that particular clinical harms can be sufficiently mitigated when exposed to security risks.

For the proposed architecture views, the draft guidance recommends that each view should identify security relevant system elements and their interfaces, define the security context, domains, boundaries, and external interfaces of the system, align the architecture with the system security objectives and requirements as well as the security design considerations, and, finally, establish traceability of architecture elements to user and system security requirements.

The level of recommended detail for the architecture views is captured in Appendix 2. This information includes the use of diagrams, like call flow diagrams, as well as the information details for an

Architecture view which outlines the individual elements of each view and the associated detail for them.

Documentation recommendations in section V the draft guidance are around the proposed testing. In this section, FDA makes recommendations around the types of testing to be performed, including security requirement testing, threat mitigation, vulnerability testing, and penetration testing. This section also makes recommendations on the independence and technical expertise to testers, the scope of the testing, the third-party testing recommendations, and submission documentation to ensure that all of these elements are captured and easily understood by the associated FDA reviewer.

[INAUDIBLE] our proposed transparency recommendations, including the labeling and vulnerability management recommendations.

Proposed labeling recommendations in the draft are largely similar to the recommendations provided in the 2018 Draft with some changes in reordering made to the original listing. In this draft guidance, we acknowledge that some of the labeling recommendations can be provided in different locations depending on the appropriate users for the information. For example, some information may be appropriate for the user manual or instructions for use. Whereas for capital equipment, there may be information that's more appropriate to be separated and included in a security implementation guide.

For some of the labeling mitigations and risk transfer items, they may need to be included as part of the Human Factors Testing tasks in order to ensure that they're going to be able to be followed effectively. We also make recommendations to focus on ensuring users have sufficient information on the device to integrate it and have sufficient information to manage risks or updates that occur throughout the lifecycle of the device.

In this draft, the proposed vulnerability management plan recommendations expand on the plan for providing validated software updates and patches originally described in the 2014 Premarket Guidance. In this draft, we also recommend that the plan should include coordinated vulnerability disclosure processes, as described in the 2016 Postmarket Guidance.

Additional recommendations include items like periodic security testing to test identified vulnerability impact, an assessment of the timeline to develop and release patches once the device is on the market, and the patching capability, or the rate at which updates can be delivered to devices, as a part of the vulnerability management plans provided in the premarket submission.

This slide identifies the resources that have been mentioned throughout this webinar and provides their associated URLs which can be accessed following this webinar.

Please submit comments to the Docket by July 7th. The URL for the Docket is located on this slide.

In summary, this draft is more detailed than the 2018 Draft. The general principles proposed in section IV outline the core concepts in the guidance. The proposed design recommendations focus on security objectives and that documentation will scale with cybersecurity risk. Transparency of device cybersecurity recommendations include proposals for proactive labeling and plans to respond to emerging issues throughout the total product lifecycle.

Thank you for attending, and I'll now turn it back to Kim, who will provide instructions for the Q&A portion of this webinar.

CDR Kimberly Piermatteo: Thank you, Matt, for that presentation. I'd now like to introduce our other panelists who are joining Matt for the interactive question-and-answer segment of today's program.

Linda Ricci, Division Director of the Division of All Hazards Response, Science and Strategic Partnerships, or DARSS, and CDRH's Office of Strategic Partnerships and Technology Innovation, or OST. And Aftin Ross, Senior Special Advisor for Emerging Initiatives within OST.

Before we begin our question-and-answer segment, I'd like to go over a few reminders before we take your questions and a few tips.

Foremost, to ask a question, please click the Raise Hand button, which should appear on the bottom of your Zoom screen. I'll announce your name and give you permission to talk. When prompted, please select the blue button to unmute your line, and then ask your question. After you ask your question, please lower your hand. If you have another question, please raise your hand again to get back into the queue. And I'll call on you again as time permits. Please remember to limit yourself to one question only, and try to keep it as short as possible.

And lastly, please refrain from asking about specific submissions. For these questions, we ask that you consider submitting a Q-Submission or consider emailing my division at DICE@fda.hhs.gov.

Now as we wait to receive some of your questions, I'd like to welcome our newest panelists with a few questions that we've gotten over the past few weeks about the draft guidance.

For our first question, I'll be directing that to you, Linda. And Linda, the question is, what is the planned timeline to finalize the guidance?

Linda Ricci: Thanks, Kim. We often get this question about any draft guidance that we publish. Our first step with this guidance is to collect the comments. And again, the Docket closes for this document on July 7. So we appreciate, if you have comments on this guidance, to please submit them to the Docket by July 7.

Once the Docket closes for this, we then carefully review all the comments that we have received and update the guidance as appropriate. Once we have completed that process, we then look to publish the guidance in final.

I know it can be frustrating to wait for a final guidance to be published, but I guarantee that we are doing this as quickly as possible and really want to take the time to evaluate all of the comments that we receive. Thank you.

CDR Kimberly Piermatteo: Thanks, Linda. Alright, our next question that we've previously received, I'll be directing to you, Aftin. Aftin, the question is, how does guidance align with overall international efforts, such as the International Medical Device Regulators Forum, or IMDRF?

Aftin Ross: Thanks, Kim. The guidance is well-aligned with international best practices and efforts, such as IMDRF. For example, IMDRF released guidance in 2020 that highlighted best practices in both premarket and postmarket medical device cybersecurity. And similar to FDA's Premarket Guidance draft, the IMDRF guidance champions the need to really emphasize taking a total product lifecycle approach to medical device cybersecurity risk management, security by design, threat modeling, and software transparency via documentation, and Software Bill of Materials, or SBOM.

The guidance from IMDRF also emphasizes providing relevant communication about the security and security risks of the device across the total product lifecycle because it's important to enable sufficient understanding by end users to aid in risk management across TPLC. I think we heard a lot about that in Matt's presentation earlier today. Thanks, Kim.

CDR Kimberly Piermatteo: Great. Thank you, Aftin. Alright. So now, we will go ahead. I see a bunch of raised hands, so we'll go ahead and take your live questions.

The first question is coming from Emmanuel. Emmanuel, I've unmuted your line. Please unmute yourself and ask your question.

Emmanuel: Yes, can you hear me?

CDR Kimberly Piermatteo: Yes, we can.

Emmanuel: Yes, so on the SBOM, there was one element that has been mentioned that you have to provide the end of life for the component that you list. And most of the components mostly do not have end of life as part of the component that get listed. So what is the FDA's recommendation as handling those? Do you say not applicable? Or what is the recommendation?

CDR Kimberly Piermatteo: Thanks for that question. I think Matt is going to go ahead and take the first response.

Matthew Hazelett: Sure, thank you for that question. We definitely understand that not all components may have a defined end of life or end of service date that may be incorporated in the medical device. But when known, we would appreciate that information in the premarket submission if that remains a part of the guidance when finalized.

Largely, what we're looking to try to do is understand what the supported lifecycle of the device is expected to be throughout the lifecycle of the product and how the product maintains. So while there may be unknowns, we'd like to get a understanding of either how long service agreements were in your purchasing agreements with that supplier for the software component to continue to maintain it. But we do understand that not all of those dates are going to be defined for every system component. But for many, they may be already defined at the time that you're acquiring them.

Emmanuel: Thank you.

CDR Kimberly Piermatteo: Great. Thank you, Matt. Our next question is coming from C-Y-S-H-E. I have unmuted your line. Please unmute yourself, and ask your question.

Cyshe: Yes, hi. Yes, hi. I have a straightforward question. So right now, we have this new draft guidance, and we also have 2018 guidance, and the 2014 final guidance. They have different requirements in the details of the information we need to submit. So for example, if we need to make a submission tomorrow, which guidance do we need to follow?

CDR Kimberly Piermatteo: Thank you for that question. Linda, did you want to take that?

Linda Ricci: Yes, I'd be happy to. So this guidance that we just published, the 2022 draft guidance, is just that-- it is draft guidance. So it is not final yet. So we will not be implementing this guidance until it is final. This guidance supersedes the 2018 draft guidance, which was also a draft guidance.

So right now, the 2014 Premarket Guidance is final [INAUDIBLE]. This guidance builds on the principles that were in the 2014 guidance. So hopefully, you will see the similarities between what's in this draft guidance and what's in the final 2014 guidance. But to directly answer your question, we would expect you to follow the 2014 final guidance.

Cyshe: Yes, OK. Thank you.

CDR Kimberly Piermatteo: Thank you, Linda. Alright, our next question is coming from Majojkumar. I have unmuted your line. Please unmute yourself, and ask your question.

Majojkumar Parmar: Thank you. I hope you can hear me.

CDR Kimberly Piermatteo: Yes, we can.

Majojkumar Parmar: Thanks. My question is very pointed. The cybersecurity risk of AI is emerging as a critical threats, like hackers abusing or exploiting the AI system. What is the suggestion on the cybersecurity aspects for AI-based SaMD?

CDR Kimberly Piermatteo: Thank you for that question. Matt, would you like to take this question?

Matthew Hazelett: Sure. We definitely understand that AI and machine learning-based devices have some specific considerations. The way how we approach in this draft guidance document was by aligning around the security objectives which would be still relevant to those AI/ML solutions, such that those considerations would just have different applicability and different additional considerations when applied to AI and ML technologies.

So the integrity of those algorithms then becomes a additional consideration, as with authenticity of the data and the access to those algorithms. So while they have some specific implementation considerations, largely the overall security objectives are fully aligned with those that we presented in this guidance.

So when considering AI and ML solutions and how to apply security to those, they are still reliant on those same security objectives but may have some different implementation considerations based off of the different technologies used and where that AI and ML algorithm resides.

So if that's something that resides in a cloud-based solution or whether that's inherent to the end device product, you're going to have the same security objectives apply, but you're going to approach them slightly differently. So we believe that those solutions are encompassed in these, and we may consider further detailed specific recommendations for cybersecurity of these technologies in other guidance documents. But we do believe the same security objectives apply.

Majojkumar Parmar: Thank you.

CDR Kimberly Piermatteo: Thank you, Matt. Thank you for that question. Alright, our next question is coming from Tom. Tom, I have unmuted your line. Hold on one second. Tom, I have unmuted your line. Please unmute yourself, and ask your question.

Tom Hirte: Alright. Thank you, Matt-- a very helpful presentation. Linda and Aftin, my question is regarding SBOMs. We have some challenges looking at specifically how you would like us to include the level of SOUP documentation-- in other words, to know the SOUP inside of SOUP inside of SOUP, et cetera. How many levels down is expected?

CDR Kimberly Piermatteo: Thank you, Tom, for that question. I think we are going to go ahead and give Aftin-- would you like to take the first response?

Aftin Ross: I can certainly start-- and then if others want to chime in. So with regard to how deep do you need to go-- so certainly, it's helpful to have more information additional insight, if possible.

But we recognize, as SBOM is still relatively nascent, that it might be as at least a good first start to be able to go at least to that first level, all those primary components within your system. And as we continue to mature, the ability to ingest in automated ways some of this additional information will continue to evolve, will have additional tools and things that will be helpful here that will better enable, better facilitate the ability to go deeper. So what we would say is, certainly, as deep as is possible based on what's known, recognizing that there might be some technology limitations at the time.

CDR Kimberly Piermatteo: Thank you, Aftin.

Tom Hirte: Thank you.

CDR Kimberly Piermatteo: Yeah. Alright, thank you, Tom. Alright, our next question is coming from Erin. Erin, I have unmuted your line. Please unmute yourself, and ask your question.

Erin Bissonnette: Hi, there. Thanks for this information. This is super helpful. Real quick question on the list of required testing-- what exactly are you looking for the threat mitigation testing item that I saw on there that appears to be separate from the vulnerability and penetration testing?

CDR Kimberly Piermatteo: Thank you, Erin. Matt, I'll turn this question over to you.

Matthew Hazelett: Sure. Thank you for this question. Largely, we're trying to understand that the mitigations applied are effective. So it definitely couples with some of the vulnerability scanning, fuzz testing, and penetration testing recommendations. So largely, it comes into the effectiveness against known threat mitigations that exist in the current system.

So I believe it's a item that can be coupled with some of the other security testing, but making sure that those existing mitigations are blocking against known potential threats to the system are what we're trying to get at with that specific testing item.

Erin Bissonnette: Thanks, Matt. Would the threat model be that? What you just described-- what a threat model? Is that what you're talking about there?

Matthew Hazelett: So the threat model would be the documentation in terms of how you've designed the system to do that. The testing would be how you're demonstrating that the threat modeling is effective-- so demonstrating that those mitigations that you applied are blocking those anticipated threats.

Erin Bissonnette: Alright, thank you so much.

CDR Kimberly Piermatteo: Thank you, Matt. Thank you, Erin. Alright, our next question is coming from Tom. Tom, I have unmuted your line. Please unmute yourself, and ask your question.

Tom Wood: Oh, thank you. Can everybody hear me?

CDR Kimberly Piermatteo: Yes, we can.

Tom Wood: Excellent. So I had a quick question. In terms of a submission, assuming we've done our threat modeling, we've done penetration testing, we've identified all of the potential issues in the system and have remediated them all with the exclusion of potentially an end-of-life operating system, now would that just totally go against the submission itself? Or would there be some credence to the submission seeing as how all the other security controls have been mitigated?

CDR Kimberly Piermatteo: Thank you, Tom, for that question. Matt, I'm going to turn that question over to you again.

Matthew Hazelett: Sure. Thank you for that question. I think that when you get into a new device with an unsupported operating system, that definitely presents a challenge for considering the life cycle of the device and whether the device would be able to be secured.

So while we definitely evaluate devices based off of the totality of information, that would be something that would be of particular challenge since it's so critical to the overall device operations and, typically a important aspect of the defense in depth design of the device to be operating on a supported operating system that's getting those security updates throughout the lifecycle of the device. I do believe that would be a particular challenge. But as always, we evaluate the totality of the information. And there may be instances where a particular operating system may be able to be justified for some sort of shorter time frame. But typically, that would be a significant hurdle during the FDA review process based off of the recommendations in this draft.

Tom Wood: Excellent. Thank you.

CDR Kimberly Piermatteo: Alright, our next question is coming from Michael. Michael, I have unmuted your line. Please unmute yourself, and ask your question.

Michael Nilo: This is actually a-- thank you, everyone, for getting on the call. This is actually a good follow-up to Tom's previous question. Does the FDA-- for operating systems that reach their end of life on supported hardware that may connect to implants, does the FDA have-- for longer-term hardware-type devices, does FDA have a plan for how they expect companies to address this, where the operating system used to maybe program a device is no longer supported by the hardware the companies provided?

CDR Kimberly Piermatteo: Thanks, Matt-- or Michael, for that question. And I'm going to go ahead and turn that over again to Matt.

Matthew Hazelett: Sure. Thank you for this question. I think a lot of the recommendations we've provided in this draft go around having the plans for what happens when a particular component goes end of service or end of life that's incorporated within the medical device. So while there are instances where the hardware may not be supported, it then becomes a question of what other aspects with the device design can you do in order to ensure the continued security of the device design moving forward?

So whether that's the implementation of future compensating controls or other design changes that can be made throughout the lifecycle of the device to further ensure the security, I think it becomes a planning for that lifecycle of the device where you're identifying in the submission when you're known limitations are, when there are hardware limitations to being able to update the operating system that's part of the device design, as well as what plans you have in order to continue to mitigate security threats throughout the lifecycle of the device.

Michael Nilo: Thank you.

CDR Kimberly Piermatteo: OK, thank you, Matt, for that response. Thank you, Michael, for that question. Our next question is coming from Dick. Dick, I have unmuted your line. Please unmute yourself, and ask your question.

Dick Brooks: Oh, thanks very much. And thank you all for putting this together today. So my question goes to an earlier statement about SBOM. And so I'm wondering is, will the FDA be requiring their MDMs to follow NIST requirements for providing Software Bill Of Materials and vulnerability disclosure report attestations when all of your final decisions are made, is that in your plan to require these requirements from the vendors? Thanks.

CDR Kimberly Piermatteo: Thank you for that question. I think we're going to go ahead and give that question to Aftin. So Aftin, the floor is yours.

Aftin Ross: Thanks, Kim. So certainly, as FDA has considered development of what we would like to see in an SBOM, we maintain awareness and active engagement and other efforts in industry as it relates to this topic. So what I think you will find in the end is that we'll be fairly well aligned. But certainly, any additional specifics, such as what Matt talked about today with having some of the end-of-support information, that would be something that might be specific to FDA that would be in addition to some of those common SBOM formats that might have some of those other pieces of information that you might find in NTIA or elsewhere.

CDR Kimberly Piermatteo: OK. Thank you, Aftin. Alright, the next question is coming from John. John, I have unmuted your line. Please unmute yourself, and ask your question.

John Hepworth: Hi. Happy Tuesday. As medical device manufacturers update their patching processes to address the draft guidance, what advice can you provide on balancing testing requirements to prove safe and effective use with an acceptable timeline for the removal of vulnerabilities from devices being used by end users?

CDR Kimberly Piermatteo: Alright, thank you for that question, John. I'm going to go ahead and direct that question to Matt as well. John, could you go ahead and repeat that question, though? We had a hard time hearing that.

John Hepworth: Sorry. So as medical device manufacturers update their patching processes to address the draft guidance, what advice can you provide on balancing testing requirements to prove safe and effective use with an acceptable timeline for the removal of vulnerabilities from devices being used by end users?

CDR Kimberly Piermatteo: OK, thanks. Matt are you free? You're going to take that question?

Matthew Hazelett: Sure. Definitely, in terms of updating existing devices, it definitely would refer you to what our recommendations are in terms of the Postmarket Guidance in terms of remediating known vulnerabilities or issues as they're identified throughout the lifecycle of the device. This guidance, while we do include more total product lifecycle considerations in this draft, the Postmarket Guidance will still be in effect as that's been finalized. And we reference that guidance throughout this process.

In terms of other updates to the device and processes, we definitely understand that there are trade-offs in the design considerations when adding in updating capabilities and adding in to security to those update mechanisms. But throughout the premarket process, we'll be evaluating those updateability and patchability capabilities in accordance with our premarket recommendation.

So as this draft guidance moves into finalization, as we're reviewing existing devices for how secure updateability and patchability are implemented, we'll be using those same criteria and considerations that are outlined in this draft. But understand that we evaluate the totality of the information and know that not all existing devices that are currently in use may be able to meet every level of the recommendations based off of hardware limitations. But we do intend to use those same premarket considerations as included in this draft once finalized for the evaluation of those update mechanisms.

CDR Kimberly Piermatteo: Great, thank you, Matt, for that response. Alright, our next question is coming from Lane. Lane, I have unmuted your line. Please I'm yourself, and ask your question.

Lane Desborough: Good day, everyone. So people with chronic disease such as insulin-requiring diabetes rely on medical devices, such as continuous glucose monitors to sense physiologic status and determine appropriate treatment actions. Device manufacturers are increasingly expected to lock down access.

My question, are patients considered malicious actors with respect to the new cybersecurity guidance? Or will they be able to securely programmatically access their own data from their cybersecure medical devices?

CDR Kimberly Piermatteo: Thank you, Lane, for that question. We are going to be directing that question to Matt or Linda, would you like to take a response or provide a response?

Linda Ricci: This is Linda. I can start off with this one. First of all, we definitely understand patients and their needs with regards to the use of medical devices. The discussions in this guidance are our current thoughts on premarket submissions with regards to medical devices and security.

Patients are considered partners with us and not malicious actors. We certainly understand the needs, particularly of devices that are used in the home and the need to access important information. When it gets to looking at specific information or specific devices, we encourage that you work with the specific review branch that will handle those devices.

CDR Kimberly Piermatteo: Thank you, Linda, for that response. Our next question is coming from Christopher. Christopher, I have unmuted your line. Please unmute yourself, and ask your question.

Christopher Gates: Thank you very much. In light of the FDA's current transition from QSRs to QMSRs and, thus, some form of harmonization with ISO 13485, I was sort of disappointed to see that you're not, in this new guidance, trying to align with the MDRs or any of the good ISO/IEC specifications, like ISO 24971, 14971, IEC 81001-5-1-- all about medical device risk and medical device total product lifecycle.

Why did you guys decide to go out and align yourself with consensus standards and thus create a whole new standard that we're going to have to work to?

CDR Kimberly Piermatteo: Thank you, Christopher for that question. I think I'm going to turn this over to Linda. Linda, would you like to provide a response first. And then if anyone else has anything they want to add, please do so.

Linda Ricci: Sure, be happy to start off. Thank you, Kim. First of all, we definitely appreciate the reference to 13485, understanding that that itself is also draft, and this guidance is draft and really would appreciate, if you have comments on specific sections, where you think we could reference additional items, we would appreciate if you would send those to us in the Docket.

When we're looking at security and security risk, we see that as part of patient safety, as Matt had indicated. But the implementation and the characteristics of that tend to be a little bit different with cybersecurity, in that unlike the 14971, where you can determine probabilistically if there is the potential for this risk with these types of vulnerabilities, you really can't do that probabilistic assessment. So we looked at this a little bit differently for those reasons but certainly would welcome any of your specific comments on specific areas where we should or could align with other standards.

Christopher Gates: Thank you. Thank you very much, Linda. And I've already made those comments that I'll be putting back into the comment portal. And yes, the latest version of 14971 and 24971 do address a totally separate, non-probabilistic, non-likelihood-based way of assessing cybersecurity risk. So I suggest you reference the current version. Thank you.

CDR Kimberly Piermatteo: OK. Thank you, Christopher. And thank you, Linda. Our next question is coming from Craig. Craig, I have unmuted your line. Please unmute yourself, and ask your question.

Craig Strang: Yes. Thank you very much. Yeah, great presentation, very informative. Have a quick question about penetration testing. What is the agency's definition of end-to-end testing for penetration testing? And is there a desired state of the software when we do that penetration? For instance, do we do it as a premarket? Or is it a more of a postmarket activity or both?

Christopher Gates: Thank you, Craig. Matt, I'm going to turn that question over to you.

Matthew Hazelett: Sure. Thank you. In terms of end-to-end for penetration testing, we're looking at the totality of the system. So when we've discussed in the draft guidance around the overall architecture, including things that are directly part of the device as well as the additional supporting systems that the device may interact with, we're definitely considering the end-to-end relationship.

So from the software update standpoint, from where the update is generated at the medical device manufacturer, from that end point all the way until it reaches the end device. For complex device systems that incorporate a number of different elements, including web portals, cloud services, hospital network infrastructure, we're looking at the totality of those end-to-end connections to ensure that the device functions, and the safety and effectiveness of the device are going to be reasonably expected to be able to maintain that security throughout those different pathways.

In terms of the question of whether penetration testing is a premarket versus postmarket activity, we definitely believe that penetration testing should be part of the documentation that's provided as part of the premarket submission, as that's one of the means to demonstrate that the cybersecurity controls that have been designed into the device ecosystem are effective against current cybersecurity threats.

We understand that these are point-in-time assessments. So while they demonstrate the capabilities of a current attacker looking at the system, they definitely evolve over time. So while it is part of the premarket submission documentation, we've also identified in the vulnerability management plans a section of the draft guidance to also consider the needs for re-testing and re-evaluation, potentially including penetration testing, throughout the lifecycle of the device.

So hopefully, that's helpful because we definitely view penetration testing as one element of the overall premarket submission but also is an activity that should be carried out throughout the lifecycle of the device, as it is a point-in-time assessment of the security effectiveness of the controls against the current attacker. So those capabilities are going to evolve over time, especially as additional vulnerabilities are identified and attacker capabilities mature throughout the lifecycle of the device.

Craig Strang: Thank you very much.

CDR Kimberly Piermatteo: Yes, thank you Matt, for that response. Our next question is coming from Steve. Steve, I've unmuted your line. Please unmute yourself, and ask your question.

Steve Beighley: Thanks very much. So this draft guidance recommends human factors testing beyond the standard safety and effectiveness, now adding management of cybersecurity risks, which appear to fall beyond safety and effectiveness. So in terms of determining which tasks require HF testing for safety and effectiveness, we would refer to define severity cutoff of severe harm or worse to a person. It's less clear for cybersecurity risk. So I'm wondering, do you have any recommendations on how to pick and choose which cybersecurity risks rise to the level of the required HF testing?

CDR Kimberly Piermatteo: Thank you, Steve, for that question. Matt, I'm going to turn that question to you.

Matthew Hazelett: Sure. Definitely, in terms of the human factors testing recommendations that we identified in the draft, I believe that those largely pertain to when there are security controls or security steps in terms of the integration of the device that the user is going to be expected to need to interact with. So are there configuration settings that the user is going to have to set in order to have the expected security that the medical device manufacturer has designed the device to have?

So if those instructions aren't able to be followed by the user, you can end up having a less secure system than what the device was designed to be and therefore, potentially have those increased risks. So I think in terms of the identification of which tasks for cybersecurity may need to be considered, I think that would come from looking at the overall security architecture cases that we've outlined in the architecture views, where you are identifying that there's a potential risk with a control that a user is supposed to interact with that would therefore rise to that threshold of being included as part of the human factors testing.

We definitely don't think that every single one of the security controls requires human factors testing. But the ones that have that user interaction piece and rises to that level of risk, that's going to depend on the system at hand and the associated risks with what happens if that control is not applied correctly by the user.

Steve Beighley: OK, is there a particular severity of risk that would then qualify severity of pre-mitigation risk?

Matthew Hazelett: I don't think there's a preset risk from the security standpoint. I would use the same methodology used for your existing human factors testing to determine which tasks are appropriate for inclusion. What we wanted to ensure we highlighted in this draft document is that there are going to be, for some systems, user-based controls and actions to ensure the continued security of the device, which may need to be considered as a part of those human factor task identifications.

CDR Kimberly Piermatteo: Alright. Thank you, Matt. And thank you, Steve, for that question. Our next question is coming from KH. KH, I have unmuted your line. Please unmute yourself, and ask your question.

Karen Hughes: Hi, everybody. Thank you this. Is Karen Hughes calling from Beaufort. I actually have a question about third-party software components and at a really high level, thinking specifically about computers that would be associated with general lab equipment, where that piece of equipment might be used, for example, to read the results of a device, like a plate reader.

Can you talk a little bit more about what the expectations for that third-party software components are in the guidance under that third-party software components-- those expectations?

CDR Kimberly Piermatteo: Sure. Thanks, Karen. Thanks for that question. Matt, I'm going to go ahead and turn that question over to you.

Matthew Hazelett: Sure. I think, in terms of specific recommendations, I think that depends on the overall architecture of the system. So I think that this question gets a little specific into a particular device design. So I don't want to go into too far of detail without knowing the system if that would be better addressed through a Pre-Submission or Q-Submission to the Agency.

But ultimately, you want to look at the overall architecture of the system to make sure you're identifying where those sources of risk to the medical device that you're submitting to the Agency can come from.

So definitely, those third-party software components that are part of generating the device function are interacting with the device function are sources of those potential risks and should be included in the overall system-based assessment to identify those potential risks and sources for potential cybersecurity risks.

So overall, I think it depends on the overall architecture of the system. But definitely would encourage for any specific application to consider coming into the Agency with a Q-Submission to discuss things at a greater detail if additional clarification is needed.

Karen Hughes: Thanks. And I think it's not so much establishing the vulnerabilities because I think that piece hasn't really changed. I think it's more when you don't have the control over that instrument, the expectations for what would be used for controls and mitigations.

CDR Kimberly Piermatteo: Alright. Matt, I don't think there's an additional response. So thank you, Karen, for that question. Our next question is coming from Cameron. Cameron, I have unmuted your line. Please unmute yourself, and ask your question.

Cameron Burke: Hello. Thank you for taking the time today. Quick question regarding the definition of legacy devices-- my question is surrounding what recommendations do you guys have for new medical products that need to still interface with devices that are currently on the market and, specifically, if they use deprecated cryptographic algorithms, such as, for example, SHA-1. And can you provide maybe a little bit more clarity as to what you guys consider a legacy medical device?

CDR Kimberly Piermatteo: Thank you, Cameron, for that question. I think at this time, I'm going to turn it over to Linda. Linda, would you like to provide a response?

Linda Ricci: Sure. I definitely understand that whether you are trying to connect to another medical device that, perhaps, is considered legacy with-- and may or may not have adequate security controls, or whether you are connecting to a third-party instrument or some other product that may not be considered a medical device, that also you either don't know what the security is of that device, or you know that it's not adequate to, which you would like to have. It's important that you consider that those items, perhaps, cannot be trusted.

So if you think about a zero-trust architecture and across the lifecycle of your device, which is what we talk about in this guidance, it's really about protecting your current device. So in terms of how do you connect with those devices that might have the deprecated cryptography, as you described?

You think about what do you need to put in place to protect your device? What are the assets that you are trying to protect? And knowing that you have that type of system on the other side, what is it that you can do to protect your device to understand it? And those would be the type of mitigations that would be necessary in those types of situations. I don't know if Matt or Aftin would like to add to that.

Aftin Ross: Thanks, Linda. So one of the things I just like to point out about legacy devices is that, currently, there is a draft guidance out by IMDRF that talks about legacy devices and the definition that's used there that other industry efforts here in the U.S. have been leveraging, is that a legacy device is one that cannot be reasonably protected from current cybersecurity threats and what's nice about this broader definition is that it really is focused on the capability of the device and not just age as a sole determinant of legacy. Thank you, Linda.

CDR Kimberly Piermatteo: Alright. Thank you, Linda. Thank you, Aftin. And thank you, Cameron, for that question. We have time for one more quick question and, hopefully, quick response. I'm going to call on Phill F. I've unmuted your line. Please unmute yourself, and ask your quick question.

Phill F: Hi, good afternoon. I just have a quick question about the distinction of the use of call flow diagrams in the guidance versus, say, a more standard UML sequence diagram expectation as part of the submission filing. I'm just curious if you can speak a little bit to the specifics you're looking for in a call flow diagram versus, say, a UML sequence diagram.

CDR Kimberly Piermatteo: Great. Thank you, Phill. Matt, would you like to provide a response?

Matthew Hazelett: Sure. In the guidance, we've provided the recommendation around call flow diagrams as one example. There's definitely other diagramming methods that can effectively convey the security controls and the processes implemented. So it's definitely not saying that call flow diagrams are the only means in which you can provide visual representation of how your security design and security controls are integrated but was more provided as an example of one potential format system.

So definitely, as long as the documentation's clear in terms of how the processes work and how the controls play, other diagramming methods would be something that would be accepted by all means. But definitely, we acknowledge that there are additional diagram formats that are also effective in conveying the information and could also be used in lieu of call flow diagrams.

CDR Kimberly Piermatteo: Great. Thank you very much, Matt, for providing that response.

So with that, I wanted to conclude our Q&A segment. Thank you all for a very engaging segment. I hope that you found it informative. At this time, I'd like to turn it back over to Matt for his final thoughts today. Matt?

Matthew Hazelett: Thanks, Kim. I wanted to definitely take a moment to thank you all for your attendance and participation in today's webinar. Adequate medical device cybersecurity is essential to ensuring medical device safety and effectiveness, and we hope that you found today's discussion helpful in understanding this draft guidance better.

And I'd also like to remind you to please remember to submit your comments to the Docket by July 7. And the link to the docket is provided in the webinar slides, and is also available on the webpage to today's webinar.

Back to you, Kim.

CDR Kimberly Piermatteo: Thank you, Matt, for those final thoughts and for your presentation today on this draft guidance. I'd also like to, again, thank our other panelists, Linda Ricci and Aftin Ross, for their participation today.

Printable slides for today's presentation are currently available on CDRH Learn at the link provided on this slide under the section titled, Specialty Technical Topics and the subsection titled Digital Health. A recording of today's webinar and a transcript will be posted to CDRH Learn under this same section and subsection in a few weeks. A screenshot of where you can find the presentation materials has also been provided on the slide.

If you have additional questions about today's presentation, please email us at DICE@fda.hhs.gov.

And we also encourage you to attend a future CDRH webinar. The link on the bottom of this slide is provided a listing of all of our other scheduled upcoming webinars.

And with that, this concludes today's CDRH webinar. Again, thank you for joining us, and have a nice day.

****

END