Final Guidance: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions
November 2, 2023

Moderator: CDR Kim Piermatteo

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

Our topic today is the final guidance titled, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, which was issued on September 27, 2023. This guidance provides recommendations on medical device cybersecurity considerations and what information to include in premarket submissions. And it replaces the FDA's guidance titled, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, previously issued on October 2, 2014.

Before we begin, I'd like to provide two quick reminders for the webinar. First, please make sure you've joined us through the Zoom app and not through a web browser to avoid any technical issues. And second, the intended audience for this webinar is industry. Trade press reporters are encouraged to consult with the CDRH Trade Press team at CDRHTradePress@fda.hhs.gov. And members of national media may consult with FDA's Office of Media Affairs at FDAOMA@fda.hhs.gov.

I now have the pleasure of introducing our presenter for today's webinar, Matthew Hazelett, Cybersecurity Policy Analyst on the Clinical and Scientific Policy staff within the Office of Product Evaluation and Quality, or OPEQ, in CDRH. We'll begin with a presentation from Matt and then field your questions about our topic. Thank you all again for joining us. I'll now turn it over to Matt to start today's presentation.

Matthew Hazelett: Thanks, Kim. Today's webinar will cover the Final Guidance Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.

The learning objectives for today's webinar are to describe the scope of the guidance, describe the general principles in the guidance, describe the design and documentation recommendations, describe the transparency recommendations, and to describe the changes and updates from the 2022 draft guidance.

For the scope of the guidance, this guidance document is applicable to devices that contain software, including firmware, or programmable logic, as well as devices that have device software functions. This includes devices within the meaning of Section 201(h) of the Federal Food, Drug, and Cosmetic Act, or FD&C Act, whether or not they require premarket submission. So, this means that devices that don't require premarket submissions, but meet the definition of a medical device and include software, firmware, or programmable logic, are all included within the scope.

The guidance is not limited to devices that are network-enabled or contain other connected capabilities. This is because devices that have software, firmware, or programmable logic have the potential to have cybersecurity risks; and therefore, the recommendations apply.

For devices that do require premarket submission, this slide outlines the applicable submission types to either CDRH or CBER where the premarket submission documentations would apply. This includes premarket notification, or 510(k) submissions, De Novo classification requests, Premarket Approval Applications or PMAs, and PMA supplements, Product Development Protocols, Investigational Device Exemption submissions, Humanitarian Device Exemption submissions, Biologics License Application submissions, and Investigational New Drug submissions. The last two are new compared to the 2022 draft.

The guidance document scope, including devices and relevant premarket submission documentation deliverables, are also consistent with the requirements under Section 524B of the Federal Food, Drug, and Cosmetic Act, which we'll discuss in more detail in the following slides.

The Consolidated Appropriations Act for 2023 was signed into law on December 29, 2022, and includes the Food and Drug Omnibus Reform Act, or FDORA, which adds Section 524B to the Food, Drug, and Cosmetic Act. These requirements went into effect on March 29, 2023. These requirements apply to prospective submissions for what are identified as cyber devices under the 510(k), De Novo, Humanitarian Device Exemption, Product Development Protocol, and PMA pathways. As these pertain to the submission pathways, these requirements also apply to special and abbreviated 510(k) applications, as well as PMA and HDE supplements. The guidance documentation recommendations are intended to help manufacturers comply with the requirements under Section 524B.

Section 524B, subsection c, defines a cyber device as a device that includes software that a sponsor has validated, installed, or authorized as a device or in a device; has the ability to connect to the internet; and contains any such technological characteristics a sponsor has validated, installed, or authorized that could be vulnerable to cybersecurity threats.

Section 524B, subsection b, requires sponsors of a cyber device application to provide documentation for the following-- submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, post-market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures. It also requires manufacturers to provide documentation on how they design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure. And to make available post-market updates and patches to the device and related systems to address on a reasonably justified regular cycle known unacceptable vulnerabilities and, as soon as possible, out of cycle critical vulnerabilities that could cause uncontrolled risks.

It also requires that in premarket submissions for a cyber device, that you provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components. And to comply with such other requirements as the Secretary may require through regulation to demonstrate a reasonable assurance that the device and related systems are cybersecure.

We will now cover the general principles of the guidance, which are detailed in Section 4 of the document.

The first general principle is that cybersecurity is part of device safety and the quality system regulation. Cybersecurity is a part of safety and effectiveness. Without appropriate cybersecurity controls, you can't have appropriate safety and effectiveness for the medical device. Cybersecurity also aligns with the Quality System Regulation. And throughout the document, we outline specific Quality System Regulation requirements where cybersecurity fits in. A secure product development framework, or SPDF, can be used to fulfill aspects of the Quality System Regulation.

The second general principle is around designing for security. In the document, we outline how designing in, rather than bolting on, cybersecurity controls results in a more effective design of the device to ensure appropriate cybersecurity measures. We also outline key security objectives medical devices should achieve in order to ensure the appropriate cybersecurity measures have been implemented and these are the objectives that we will review devices against during the premarket submission.

The next general principle is on transparency. We outline the importance of end users having cybersecurity information to ensure the continued safe use of the device. This covers the total product lifecycle, from being able to appropriately install and use the device as well as maintaining the device and delivering updates to the device throughout its lifecycle.

The final general principle is on submission documentation. The recommendations in this guidance complement and are in addition to the software premarket guidance. The cybersecurity documentation is expected to scale with cybersecurity risks of the device.

I'll now cover the design and documentation recommendations provided throughout the guidance.

The design recommendations in the guidance for ensuring appropriate cybersecurity controls focus on the security objectives for the design, which are outlined in the general principles. These security objectives include authenticity, which includes integrity controls, authorization, availability, confidentiality, and the secure and timely updateability and patch ability of the device.

In the guidance, we outline eight security control categories that manufacturers should consider and implement to help in meeting the security objectives outlined in the guidance. Appendix 1 provides specific control recommendations and implementation guidance for consideration to avoid common pitfalls in designing medical devices to achieve cybersecurity. It's important to note that the appendices in this guidance are part of the document recommendations. This is different than some other documents, where the appendices may be informative, but for this guidance, the appendices are part of the document recommendations.

The documentation recommendations are covered in Sections 5 and 6 of the guidance. Section 5, Using an SPDF to Manage Cybersecurity Risks, covers different aspects, including security risk management, security architecture, and cybersecurity testing. Section 6, Cybersecurity Transparency, covers labeling recommendations and cybersecurity management plans.

For security risk management, the guidance recommends that this be a system-level assessment. This is important, as if you only consider the device in isolation of the context of the larger system or the environment of use, you're likely to potentially miss the identification of potential risks and potential controls that can be implemented on the device to protect against some of the risks of the larger system

and the environment of use. It's also important to note that security risk management is distinct from safety risk management, but that the two processes should feed into and out of one another to ensure appropriate coverage of the safety and security risks, and that they account for potential risks introduced by other mechanisms or controls implemented in the other assessment.

The guidance also recommends that known vulnerabilities should be assessed as reasonably foreseeable risks to the system. Further, it notes that risk transfer should only occur if all relevant information is known, assessed, and communicated to users to ensure that appropriate and responsible risk transfer occurs. The guidance recommends that in premarket submissions, you provide your security risk management report, such as that described in the Association for the Advancement of Medical Instrumentation, or AAMI, Technical Information Report, TIR57. Additional details and recommendations are also included in the guidance for what to include in the security risk management report.

The Security Risk Management section continues into six subsections to detail documentation and design considerations for the device. For the threat modeling documentation, we recommend that you include the full system and the lifecycle of the device in order to ensure that all risks and controls are appropriately considered for the device design. The threat modeling documentation may also include the architecture views, which are discussed later in the guidance. For the cybersecurity risk assessment, we have added this section in order to more clearly identify the documentation deliverable. We recommend that you use exploitability instead of probability to assess cybersecurity risks, as these risks depend on a human actor or a cybersecurity threat that can't be modeled using traditional deterministic methods, such as probabilities.

Interoperability considerations were also added in order to underscore the considerations for cybersecurity controls when having an interoperable device. The cybersecurity controls should not be intended to prohibit users from accessing device data but should be used in order to ensure that interoperability can be done safely and securely.

For third-party software components, this is where we outline our recommendations for the Software Bill of Materials, support and end-of-support information, and the vulnerability assessment for those third-party software components. We also recommend that you provide a security assessment of unresolved anomalies. And this is because anomalies can present a different vector to safety risks through cybersecurity causes.

Finally, we make recommendations around Total Product Lifecycle Security Risk Management, where we recommend that you maintain resources and documentation throughout the lifecycle of the device and that you track and monitor cybersecurity measures and metrics in order to track how your system and processes are performing.

Submission of a Software Bill of Materials is required for cyber device submissions under Section 524B of the Food, Drug, and Cosmetic Act. For these SBOMs, manufacturers should provide machine-readable SBOMs, and that they should be consistent with the minimum elements, also referred to as baseline attributes, identified in the October 2021 National Telecommunications and Information Administration, or NTIA, Multistakeholder Process on Software Component Transparency. These SBOMs are also recommended when provided to users and labeling to conform with industry-accepted formats.

In addition to the SBOM itself, manufacturers should also provide the software level of support provided through monitoring and maintenance from the software component manufacturer. It should also provide the software components end-of-support date, as well as the safety and security risk assessment for each known vulnerability, including the device and system impacts from those vulnerabilities. You should also provide details of applicable safety and security risk controls to address the vulnerabilities that are identified. It's important to note that this information does not have to be included in the SBOM itself but can be provided separately to support tool ingestion and machine readability of the SBOM.

For the vulnerability information that accompanies the SBOM, some sources of that information can include, but may not be limited to, information from the software component suppliers, vulnerability databases, like the National Institute of Standards and Technology, or NIST, National Vulnerability Database, and the Cybersecurity and Infrastructure Security Agency's, or CISA's, Known Exploited Vulnerability Catalog.

As I mentioned before, the architecture views that are recommended in the guidance can be provided as part of the threat modeling documentation. In the guidance, we recommend four different view categories. These are the global system view, the multi-patient harm view, the updateability and patch ability view, and the security use case views. The security use case views should identify all of the use cases for the operational states and different clinical use cases for the device in order to better understand the cybersecurity threats and controls that have been implemented to address those different use cases.

The guidance recommends that these security architecture views should identify the security-relevant system elements in 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 characteristics; and also 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 and includes diagrams and information details for an architecture view. All four of the views for the device should include this level of detail.

The guidance also makes recommendations on the cybersecurity testing that should be performed in order to demonstrate the effectiveness of the cybersecurity controls that have been implemented for the device. There are four types of testing that have been recommended; security requirement testing, threat mitigation, vulnerability testing, and penetration testing. This section also makes recommendations on the independence and technical expertise of testers, the scope of the testing and that the testing should be system-level and include all of the elements of the system and considerations for the use environment, recommendations for when third-party testing is performed for some of the security testing elements as well as the submission documentation that should be provided.

We will now cover the recommendations from the Transparency section of the guidance, including labeling and cybersecurity management recommendations.

The labeling recommendations in the guidance are largely similar to the recommendations proposed in the 2022 draft guidance, with some changes in reordering in order to ensure greater clarity of the recommendations and what should be provided in the labeling. The cybersecurity labeling can be provided in different locations, depending on the appropriate users for the information. For instance,

there may be differences between what's provided in the instructions for use manual as opposed to what may be included in a security implementation guide for devices that are used in a hospital environment.

The labeling mitigations and risk transfer items may need to be included as part of human factors testing tasks in order to ensure that users can appropriately follow the instructions to implement the necessary cybersecurity measures to ensure the continued safe and effective use of the medical device. The labeling should also have a focus on ensuring users have sufficient information on the device to integrate it as well as to have sufficient information to manage the cybersecurity risks and updates to the device throughout the device lifecycle.

The guidance also makes recommendations for what to include in cybersecurity management plans. These plans are required for cyber device submissions under Section 524B of the Food, Drug, and Cosmetic Act. These plans include how the manufacturer will approach managing cybersecurity throughout the lifecycle of the device, inclusive of responses to vulnerabilities and incidents that are identified throughout the lifecycle. These plans should include coordinated vulnerability disclosure processes, such as those described in the 2016 Postmarket Cybersecurity guidance, and also include items like periodic security testing, in order to test identified vulnerability impact and look for new potential risks, the timeline to develop and release patches to the device, as well as the patching capability, or the rate at which updates can be delivered to devices if there is a need identified.

We will now summarize the key changes from the 2022 draft guidance.

Compared to the 2022 draft guidance, the 2023 final guidance has an expanded scope. We included CBER submission types as well as considerations for combination products. We also added elements associated with the requirements under Section 524B of the Food, Drug, and Cosmetic Act. Additionally, we made some structural changes to the guidance. We added new subsections in the Security Risk Management section to clarify premarket submission documentation deliverables, including those associated with Cybersecurity Risk Assessments as well as interoperability considerations for the device. We also added Appendix 4 to the guidance in order to further clarify the premarket submission documentation recommendations. Finally, we updated the recommendations for the Software Bill of Materials. We aligned our recommendations around the 2021 NTIA SBOM framing document and we further clarified that the supporting materials can be provided separate from the SBOM documentation itself.

We will now cover our plans to make a future guidance update.

The agency plans to issue a draft select update to this final guidance in order to provide details on interpretation aspects of Section 524B of the Food, Drug, and Cosmetic Act that we were not able to include in this final guidance release. Select updates are a mechanism for us to release targeted proposed changes to an existing final guidance without putting the entire guidance back into draft status. When finalized, this select update would be incorporated into this final guidance. The select update is on CDRH's A-list of priorities for fiscal year 2024.

This slide provides the resources that were referenced during this webinar and includes the premarket software guidance, the NTIA framing document, and the 2016 Postmarket Cybersecurity guidance. And they can all be accessed at the associated URLs provided on this slide.

To summarize today's webinar, the general principles in Section 4 of the guidance outline core concepts that appear throughout the guidance document. The design recommendations focus on security objectives. And the associated documentation is expected to scale with the cybersecurity risk of the device. Transparency of device cybersecurity recommendations include proactive labeling and plans to respond to emerging issues throughout the total product lifecycle. And finally, the final guidance reflects updates made due to the comments provided on the 2022 draft and new requirements under Section 524B of the Food, Drug, and Cosmetic Act. I'll now turn it back to Kim.

CDR Kim Piermatteo: Thank you, Matt. Thank you for that presentation. We will now transition to our interactive question and answer segment.

We have gathered a panel of subject matter experts in addition to Matt to answer your questions and to help you better understand and get clarity on what we intend in this final guidance. Joining Matt today on our panel is Aftin Ross, Acting Deputy Division Director for the Division of All Hazards Response, Science and Strategic Partnerships, in the Office of Strategic Partnerships and Technology Innovation, or OST in CDRH; Jessica Wilkerson, Senior Cyber Policy Advisor and Medical Device Cybersecurity Team Lead within the Division of All Hazards Response, Science and Strategic Partnerships, in OST as well; and Erin Quencer, Regulatory Policy Analyst in CDRH's Office of Policy. Thank you all for joining us and participating on today's panel.

So before we begin, I'd like to go over how we will manage this segment and a few reminders. To ask a question, please select the Raise Hand icon, 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.

When asking your question, please remember to limit yourself to asking one question only and try to keep it as short as possible. Also, we appreciate that you may have a very specific question involving your device or scenario; however, we might not be able to answer such specific questions; therefore, we'll try to frame a broader response based on what's proposed in this final guidance.

After you ask your question, please lower your hand. And if you have another question, please raise your hand again to get back into the queue. And I'll call on you as time permits.

Now, as we wait to receive some of your questions, I'd like to welcome our newest panelists with a few questions we have gotten over the past few weeks about this guidance. So for our first question, I'll be directing that to Aftin. Aftin, the question is, generally, what kind of transition period is the FDA going to provide for the final guidance?

Aftin Ross: Thank you, Kim. There is no official transition period for the guidance. For any submissions made since the guidance issued, FDA may request the documentation identified in the guidance as we transition our internal review processes to align with the 2023 final guidance.

CDR Kim Piermatteo: Thanks, Aftin. Now, for our next question, I'll be directing that to Jessica. Jessica, the question is, there are multiple documents from the Department of Commerce and the National Telecommunications and Information Administration, or NTIA, that discuss SBOM minimum elements. Which resource does FDA recommend stakeholders use?

Jessica Wilkerson: Thank you. So, we recommend that stakeholders refer to the second edition of the NTIA document, Framing Software Component Transparency: Establishing a Common Software Bill of Materials, as the correct document. Both the guidance and the FAQ that we currently have available point to this document, which helps understand some of FDA's SBOM recommendations, including minimum elements and depth. Thank you.

CDR Kim Piermatteo: Thanks, Jessica. Now, for our next question, I'll be directing that to Erin. Erin, the question is, how does this final guidance impact the March 2023 Cybersecurity and Medical Devices Refuse to Accept Policy for Cyber Devices and Related Systems guidance?

Erin Quencer: Thanks for the question, Kim. This final guidance that is the subject of today's webinar does not supersede the previously issued Cybersecurity RTA guidance that issued on March 29, 2023. The policy in the Cybersecurity RTA Policy guidance, however, expired on October 1 of 2023; therefore, beginning on October 1, 2023, the FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by Section 524B of the FD&C Act. The Cybersecurity RTA guidance that issued in March of 2023 is considered an expired guidance. This final guidance that is the subject of today's webinar, however, does supersede the October 2014 final guidance by the title, Content of Premarket Submissions for Management of Cybersecurity and Medical Devices, as described in the background of this final guidance.

CDR Kim Piermatteo: Great. Thank you so much, Erin. And thank you, everyone, our additional panelists, for joining us and for answering those questions. We will now take our first live question. This question is coming from Gergely. Gergely, I've unmuted your line. Please unmute yourself and ask your question.

Gergely Antalfi: Hi. I'm Gergely Antalfi from Boston Scientific and thank you for taking my question. And it would be about, this guidance provides expected content for new devices, but how would you recommend to handle resubmissions for legacy devices?

CDR Kim Piermatteo: Thank you Gergely for that question. I am going to turn that over to Matt to provide you a response.

Matthew Hazelett: Sure. Happy to. Thank you for the question. I'd say that for submissions for changes to devices that have already been authorized, you should follow the recommendations in the 2023 final guidance, as this also includes the elements for documentation associated with Section 524B of the Food, Drug, and Cosmetic Act. So, we would recommend that you provide all of the documentation elements that are identified in the guidance for submissions of modifications to existing devices. Thank you.

Gergely Antalfi: Thank you. So, you would suggest for all the new information to be provided, not just information related to the changes?

Matthew Hazelett: Correct. Based off of the statutory language in Section 524B where it requires manufacturers to submit the documentation in order to provide a reasonable assurance that the device is cybersecure, as well as the postmarket management plan and the Software Bill of Materials, the documentation in the guidance should be provided as a part of that submission for those changes.

Gergely Antalfi: Thank you very much.

CDR Kim Piermatteo: Thank you, Gergely. And thank you, Matt, for that response. Our next question is coming from Cyrina Swanston. I've unmuted your line. Please unmute yourself and ask your question.

Cyrina Swanston: Hi. This is Cyrina. I have a question regarding the labeling. So, based on the updates made to the FD&C Act, will FDA be making any changes to 21 CFR 809.10, the medical device labeling for IVDs, just to describe what will be required for the cybersecurity-specific labeling?

CDR Kim Piermatteo: Thank you, Cyrina. I think Matt or Erin, would you like to provide a response?

Matthew Hazelett: Sure. Based off of the labeling recommendations, these are the recommendations that we believe apply to all device types under the definition of medical devices outlined in Section 201(h). So these recommendations do apply. Right now, I don't believe there are plans to change any specific regulations to any particular device types. But we do recommend that for all devices reviewed by CDRH that you would provide the elements identified in the labeling section of the guidance for those devices.

Cyrina Swanston: Okay. Thank you.

CDR Kim Piermatteo: Thank you, Cyrina. Thank you, Matt. Alright, our next question is coming from Abdo. Abdo, I've unmuted your line. Please unmute yourself and ask your question.

Abdo: Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Abdo: Hi. So this is to do with the SBOM and the vulnerability disclosure. How do we go about disclosing all the SBOM findings? Do we not want to go through the disclosure process, or how do you suggest that we actually disclose that to the FDA?

CDR Kim Piermatteo: Thanks, Abdo. I'm going to turn it over to Matt.

Matthew Hazelett: Thank you. For the vulnerabilities that are identified as part of your premarket development process, so vulnerabilities associated with third-party software components, those can be a part of your device submission as part of the cybersecurity risk management documentation that accompanies the other elements provided, like the SBOM and the component support information. We recommend that you provide a assessment of the vulnerabilities for third-party software components as a part of that documentation. For vulnerabilities that are identified postmarket, there is the requirement under Section 524B to have plans for coordinated vulnerability disclosure and related processes.

So, if vulnerabilities are identified throughout the lifecycle, we do expect that those would be disclosed in a coordinated fashion with the appropriate stakeholders, like the Cybersecurity and Infrastructure Security Agency, and any coordination that may be necessary for FDA if it's a uncontrolled vulnerability

as identified in the postmarket guidance. So that would be the recommendations on how to handle vulnerabilities premarket or postmarket in terms of what the FDA's recommendations are at this time.

Abdo: Thank you. That makes sense.

CDR Kim Piermatteo: Thank you, Abdo, for the question. Thank you, Matt, for your response. Our next question is coming from Brad. Brad, I have unmuted your line. Please unmute yourself and ask your question.

Brad J: Thank you very much for this interesting presentation. Slides 5 and 9 seem to contradict one another. Slide 9 talks about the fact that the device connects to the internet. And slide 5 says we're not only considering devices that connect to networks. Can you please clarify that?

CDR Kim Piermatteo: Thank you, Brad, for that question. Jessica, would you like to provide a response? And again, anybody from the team can chime in if you want to add on, too.

Jessica Wilkerson: Great. Thank you so much. Yes. To clarify, not, without looking at the slides again, the difference in the scope is likely related to the fact that one of the slides was discussing the language in 524B specifically, the statute, which has a statutory definition of what a cyber device is, which includes the requirement that the device have the ability to connect to the internet. This guidance has a broader scope than simply cyber devices or the language within the statute to apply to all medical devices that fall within the scope rather than being solely limited to cyber devices. So that is why there is a difference in the scope there. Thank you.

CDR Kim Piermatteo: Thank you, Jessica. Thank you, Brad, for your question. Our next question is coming from Robert. Robert, I have unmuted your line. Please unmute yourself and ask your question.

Robert Smigielski: Thank you very much, Robert Smigielski from B. Braun Medical. Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Robert Smigielski: Okay, very good. So, in the section on cybersecurity management plans, there is a discussion that the plan itself should include the elements that are, the bullet item I'm curious about is personnel responsible. So in what sense and in what way do we document personnel responsible for the lifecycle of the product? Are you looking for organizational charts? Are you looking for ratios of premarket development team size? That's what I'm getting at.

CDR Kim Piermatteo: Thank you, Robert, for that question. I'm going to turn it over to Matt.

Matthew Hazelett: Sure. Thank you for the question. For the personnel responsible, we're looking for the personnel with particular roles and responsibilities around the postmarket management lifecycle. So that can include the identification of different roles within the product team or your postmarket management team that have responsibilities that would include the items that are identified later in the list to make sure that there's the appropriate management and accountability for performing those activities and that you have resources identified who will be carrying out the activities in the postmarket lifecycle. So, it's more focused on the personnel roles, not necessarily the individual staff names or

particular ratios, but the identification that you have people in the organization that will be carrying out the other items in the cybersecurity management plan.

CDR Kim Piermatteo: Thank you, Matt, for that response. Our next question is coming from Phil. Phil, I've unmuted your line. Please unmute yourself and ask your question.

Phil Englert: Hi. This is Phil Englert with Health ISAC. My question is about labeling, and specifically around sharing SBOMs with users. The language seems to, says that labels should be inclusive and then, but they only may include SBOMs. So, is the expectation that SBOMs are to be shared with customers if they have been through this submission review process?

CDR Kim Piermatteo: Thank you, Phil, for that question. I'm going to turn it over to Jessica.

Jessica Wilkerson: Thank you. Yes, the guidance recommends that SBOMs be included as part of the labeling. I would like to make that distinct from the requirements within 524B that requires that the SBOM be provided as part of the premarket submission. So those are two distinct things, providing the SBOM to FDA and providing the SBOM to end users. We do stress within the labeling that we recommend that SBOMs be made available to end users to assist them in understanding potential cybersecurity risk and other factors relating to cybersecurity risk management. Thank you.

Phil Englert: Thank you.

CDR Kim Piermatteo: Thank you, Jessica. And thanks again, Phil. Alright, our next question is coming from Sarai. Sari, I've unmuted your line. Please unmute yourself and ask your question.

Sarai Meyer: Hello. Thank you. This is Sarai Meyer. I had a question with regards to SBOMs, including off-the-shelf software components where the developer of the device might not know all the libraries or software sub-components of that particular off-the-shelf software item. And we were wondering how to address that in our SBOM, simply have the high-level inclusion of the OTS software component and state why we can't provide the additional sub-dependencies?

CDR Kim Piermatteo: Thank you, Sarai, for that question. I'm going to turn it over to Jessica again. Jessica?

Jessica Wilkerson: Thank you so much. Yes. If you look at the NTIA framing document that FDA points to within our guidance, it does include a discussion of depth. So, our recommendation is that SBOMs be complete, in other words, that they have all transitive dependencies included within them, as stated in the guidance, where manufacturers may not know what all of the transitive dependencies are, we do recommend providing the justification for why the information is not present. Thank you.

Sarai Meyer: Thank you.

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

Tim Lawton: Yes, Tim, Tim Lorton. Thank you for the presentation. I have a short question related to a feedback on deficiencies I received a few days ago. Without going into detail, it's asked me to justify the

choice of, for example, the STRIDE method, the cybersecurity threat analysis we use. In another example, it's asking me to justify the use of, for example, the NIST 800-30. So, my question is, to what level do we need to justify?

CDR Kim Piermatteo: Thank you, Tim, for that question. Matt, would you like to provide a response?

Matthew Hazelett: Sure. In terms of justifications for the threat modeling methodology or the risk assessment methodology, we're looking for you to describe what methodology was used and the reasons why you believe that that is applicable or appropriate based off of the elements of your system. For threat modeling and cybersecurity risk assessment, there's pros and cons with any selected methodology for threat modeling or the cybersecurity risk assessment. So, we're looking for you to describe why you selected the methodology that you did and why you believe that that is sufficient based off of the design considerations of your device in order to ensure that you've appropriately captured the threats that the system will be exposed to and that you've applied an appropriate scoring methodology to determine whether your risk mitigations are acceptable and have reduced the risk to an acceptable level.

Tim Lawton: So basically, it will be sufficient to give a fairly brief explanation because, for example, the NIST 800-30 is already recognized and listed in the FDA guidance. So, do we need to actually push the reflection to say this is justified because, because, because, or can we consider that it's sufficient to say that it is in the guidance?

Matthew Hazelett: You should be providing a description of why you believe that that methodology is appropriate for your system, so we don't particularly identify only one methodology. So there's differences between the different methodologies out there. NIST 800-30 is one and they all have pros and cons, or may need adaptation by the manufacturer, as many of them involve qualitative assessments, so making sure that it is fit for purpose for your particular device considerations and describing why you believe that that particular methodology works based off of your device characteristics.

Tim Lawton: Okay. Thank you very much.

CDR Kim Piermatteo: Thank you, Tim, for the question. And thank you, Matt, for your response. Our next question is coming from Denise. Denise, I've unmuted your line. Please unmute yourself and ask your question.

Denise Angwin: Hi there. Thank you. I assume you can hear me.

CDR Kim Piermatteo: Yes, we can.

Denise Angwin: I have a follow-on question to the legacy device question. And that's related to testing. What are the expectations for testing? And I'm thinking of legacy devices that, in particular, don't connect to networks. I know they may still be cyber devices, and they're certainly medical devices, but we're just curious about ongoing testing for products like that.

CDR Kim Piermatteo: Thanks, Denise, for your question. Matt, I'm going to turn it back over to you.

Matthew Hazelett: Sure. So as we outlined in the guidance, we believe that throughout the lifecycle of the device, there should be recurrent testing, especially if you're making changes in coming back into the agency with a new submission for modification. So, we do recommend that all of the testing types are, that are identified in the guidance be completed if you're making another submission. And this is in order to demonstrate that the controls that have been implemented are still effective for the device against the emerging, evolving nature of cybersecurity risks given that the devices are continuing to be used and maintained. We want to make sure that they are still providing that reasonable assurance that they're cybersecure and that the cybersecurity controls are still effective for the particular design and device considerations in the architecture and environment of use of the device.

Denise Angwin: Can I ask just a follow-on question to that related to all the architecture views? Some products have been in the market for 10, 15, or more years, where that was never provided. Would we need to follow up with all that, too, if a new submission goes in?

Matthew Hazelett: Yes. That is our recommendation, is that all of the documentation outlined in the guidance would be provided for any submissions moving forward for work devices, regardless of whether they are new or they're making changes to existing devices, as this is the documentation that the agency believes that we need to see in order to make sufficient determinations of whether the device is sufficiently safe and effective or cybersecure, depending on if it's a cyber device or not. But this is the documentation the agency believes we need in order to make sufficient evaluations of products moving forward.

Denise Angwin: Thank you very much.

CDR Kim Piermatteo: Thanks, Denise, for those questions. And thanks, Matt, for your responses. Alright, our next question is coming from Vanessa. Vanessa, I've unmuted your line. Please unmute yourself and ask your question.

Vanessa Bacey-Arballo: Hi. So some of us may have thousands of third-party software within our devices and software. Is it acceptable to kind of use a risk-based approach to ensure that we, at a minimum, have critical items in our SBOM and other OTS supporting documentation? It just seems almost hard to sustain looking for information as end date for 4,000 OTSs within a given product. So, I guess that's my question, is it acceptable to do a risk-based approach?

CDR Kim Piermatteo: Thank you, Vanessa. I'm going to turn it over to Jessica.

Jessica Wilkerson: Thank you for the question. We do believe and recommend that SBOMs need to include all third-party software and all off-the-shelf software components in order for both the FDA to do the appropriate risk assessment and risk analysis of the different components that may be included within the device. So we do recommend that all software components and all OTS, as well as manufacturer developed components be included within the SBOM. Thank you.

Vanessa Bacey-Arballo: Thanks.

CDR Kim Piermatteo: Thanks, Jessica. And thanks, Vanessa. Our next question is coming from A. Macchi. A. Macchi, I've unmuted your line. Please unmute yourself and ask your question.

Antonio Macchi: Hello, everybody. My name is Antonio Macchi from [INAUDIBLE], based in Switzerland. And I've been working extensively with NIST and the Center for Internet Security Critical Security Controls. And sometimes, we feel that the terminology is not completely harmonized. So, my question is, is there an initiative to harmonize the cybersecurity recommendations from the FDA with the industry best practices, such as NIST and CIS Critical Security Controls? I can give you an example. For instance, what is called a security event, attack, or exploit throughout the FDA documentation in NIST and in CIS, there's a more clean-up way of presenting cybersecurity incidents, or so it would be great to hear just which direction we should think. Thank you very much.

CDR Kim Piermatteo: Thank you, Antonio, for your question. I'm going to turn it over to Matt or Jessica. Jessica, did you want to take a first crack at it?

Jessica Wilkerson: Happy to. Thank you. So for FDA, we see cybersecurity considerations as being somewhat unique than general use cases for cybersecurity events and incidents and risks that may be covered by something like the NIST Cybersecurity Framework. When we look at cybersecurity incidents, they may go beyond simply being about impacts to information systems or the devices that are within those systems and the communication pathways. A cybersecurity incident may have safety considerations, certainly patient safety considerations, that may not be fully covered or anticipated by some of the NIST language. So that is the reason why we use the language that we did and did not necessarily stick only to things like the NIST's definitions, is, again, looking for the fit-for-purpose definitions and recommendations specifically for FDA's and the sector's needs, we did believe that we needed to capture the larger use cases that may be present with some of these incidents in these risks. Thank you.

CDR Kim Piermatteo: Thank you, Jessica. Our next question is coming from Dan. Dan, I've unmuted your line. Please unmute yourself and ask your question.

Dan, I see that you've unmuted. I don't know if you are double-muted.

Dan, are you able to unmute your line?

Alright, if you are able to get back into the queue later, please do so. We're unable to hear you. Our next question is coming from Jurgen. Jurgen, I've unmuted your line. Please unmute yourself and ask your question.

Jurgen Pesara: Yes, thank you. I have a question in the context of testing security requirements. The guidance on page 26 says manufacturers should provide evidence of their boundary analysis and the rationale for the boundary assumptions. So what kind of boundaries does this refer to, exactly? And what kind of evidence is expected?

CDR Kim Piermatteo: Thank you, Jurgen. I'm going to turn it over to Matt.

Matthew Hazelett: Sure. So when we refer to boundary analyses, we're looking for you to assess the overall architecture of the device and look for boundaries where there may be differences in trust levels in communications and how those interfaces handle those different boundaries and the different endpoints or edges of the device ecosystem. So, we're looking for you to make assessments and demonstrate testing of those different boundaries of the device and making sure that those are

appropriately secured and have the appropriate controls being effective to manage those different boundary points between the device and other elements of either the device system or the environment of use for the medical device.

Jurgen Pesara: So, it's more about trust boundaries and not boundaries of performance in the context of denial of service attacks, for example?

Matthew Hazelett: Yeah. So, boundaries of trusts is largely where that's referring to, but to your example, you could look at a boundary for the potential for a denial of service impact. So, it's more focused on the trust boundary aspect, but not limited to the considerations of just the trust aspects, but what that boundary interface may cause in terms of risks and the appropriate controls to mitigate those risks.

Jurgen Pesara: Okay. Thank you.

CDR Kim Piermatteo: Thank you, Jurgen. Thank you, Matt. Our next question is coming from James. James, I've unmuted your line. Please unmute yourself and ask your question.

James Frerichs: Yes, hello. Thank you for the webinar. I think mine is a follow-up to Brad's question about the definition of a cyber device. We have a USB connected on 510(k) required Class II medical device. What is your recommendation for submission of cybersecurity materials? Like a full assessment or, I think as the definition's not a cyber device, per se, under the Cosmetic Act?

CDR Kim Piermatteo: Thank you for your question, James. I'm going to turn it over to Matt. I'm not sure, Matt, if you needed additional clarification?

Matthew Hazelett: I think I'm good.

CDR Kim Piermatteo: Okay.

Matthew Hazelett: So, when we're looking at the determination of whether a particular medical device is a cyber device, we're looking at all of the aspects of the system and looking at the overall threat surface and what could lead to the potential ability to connect. So, while we can't outline currently an exact interpretation of everything that would be considered a cyber device, generally, when we're looking at different interfaces, like USBs, we look for the possibility in terms of connectivity to that USB to a dongle that can enable Bluetooth or Wi-Fi connectivity as a potential vector for the ability to connect.

So, we look more holistically at the overall device, its environment of use, and the overall threat surface in order to make those determinations of whether something is a cyber device or not. If you have a particular question regarding a specific device type, we definitely encourage you to reach out either in a Q-Submission to the agency or reaching out to your particular review team, who may be able to provide more specific guidance based off of the particular device involved.

James Frerichs: Thank you.

CDR Kim Piermatteo: Thank you, James. And thanks, Matt. Our next question is coming from Satya. Satya, I've unmuted your line. Please unmute yourself and ask your question.

Satya, are you able to unmute your line?

Alright, we're going to move down to our next question. Our next question is coming from David. David, I've unmuted your line. Please unmute yourself and ask your question.

David Shanes: Hi. Thank you for the webinar. I had a question, on the cybersecurity management plan. There were a couple of things there, time to develop and release patches and patching capability. What about devices that were not designed with the intent to be patchable?

CDR Kim Piermatteo: Thank you, David. I'm going to turn it over to Matt.

Matthew Hazelett: Sure. So if you have a device that was previously designed without the ability to update it or patch it, that's something that you should provide a description of the limitations of the device as a part of the submission for why that may not be relevant. But we do look more holistically in terms of whether there's updates that can be made by service personnel to a device, that would still be something that we would look at in terms of how long it would take field service personnel in order to reach a particular device if that is the only mechanism for the device to be updated.

So, we look more broadly, so evaluate what's in the realm of possible for the particular device. But if there truly is just no way to patch a device and the only option for if a unacceptable cybersecurity risk were identified is to replace the device, that would also be something that you could discuss as a part of the cybersecurity management plan in terms of what those capabilities and timelines would be in order to do an emergency replacement if a patching capability is not available.

David Shanes: So, is there almost a presumption that all new devices should be patchable?

Matthew Hazelett: If they have software or firmware programmable logic, we expect that there's likely a mechanism for the device to be updated unless it's something where it's a single use device and if there was an unacceptable risk identified that, instead of patching, you would replace the device, instead. But generally, if there is software or firmware, the general expectation is that there would be some mechanism to patch or update the device in order to protect against emerging cybersecurity risks.

David Shanes: Okay, great. Thank you. I appreciate that.

CDR Kim Piermatteo: Thanks, David. And thanks, Matt. Our next question is coming from Stuart. Stuart, I've unmuted your line. Please unmute yourself and ask your question.

Stuart Turner: Yes, can you hear me?

CDR Kim Piermatteo: Yes, we can.

Stuart Turner: Perfect. I just wanted to give you a chance to answer a question. Will the presentation and recording be available later on?

CDR Kim Piermatteo: Thank you, Stuart, for that question. Yes, it will be. We will post a recording and the transcript within a few weeks of today. And the printable l slides are already available on the webinar page and CDRH Learn. So, they will be.

Stuart Turner: Thank you very much.

CDR Kim Piermatteo: You're welcome. Our next question is coming from Ellen. Ellen, I have unmuted your line. Please unmute yourself and ask your question.

Ellen Riebe: Hello. I have a question related to…

CDR Kim Piermatteo: Ellen, you're very, very faint. I'm going to need you to either turn up your volume or speak up loudly.

Ellen Riebe: Sorry. I have a question more related to inspection and enforcement.

CDR Kim Piermatteo: Ellen, we're still having a really hard time hearing you.

Are you still there?

Ellen, did we lose you?

Alright, I'm going to go down to our next caller. Kayra, I have unmuted your line. Please unmute yourself and ask your question.

Kayra Otaner: Hey, can you hear me?

CDR Kim Piermatteo: Yes, we can.

Kayra Otaner: Kayra Otaner with [INAUDIBLE]. My question is about 524, Section B, in regards to the sentence that goes like, make available post-market updates and patches to the device and related systems to address. You might know there are two emerging standards, VEX and CSAF. Did FDA recommend or require use of VEX and/or CSAF in addition to the SBOM in the future?

CDR Kim Piermatteo: Thank you for that question. I'm going to turn it over to Jessica.

Jessica Wilkerson: Thank you so much. At this time, FDA is not asking for or is not necessarily recommending VEX or the other, some of these other vulnerability disclosure standards that are emerging. Manufacturers should feel free to leverage them if they so choose. But they would not necessarily replace elements that are otherwise recommended within the premarket submissions, such as the cybersecurity risk management plan, and otherwise. Thank you.

CDR Kim Piermatteo: Thank you, Jessica, for that response. Our next question is coming from, I apologize, I'm going to say Hornseb. I have unmuted your line. Please unmute yourself and ask your question.

Ben Hornseb: Hi. My name is Ben. I have two, hopefully very quick, questions. The first is related to section 524B, subsection b2, the requirement to design, develop, and maintain processes and procedures around cybersecurity. I'd like to clarify if, in premarket submissions, the expectation is to provide those processes and procedures or simply the output of those procedures, like a cybersecurity risk analysis, as an example.

CDR Kim Piermatteo: Thank you, Ben, for that question. I'm going to turn it over to Matt.

Matthew Hazelett: Sure, happy to take this question. So for the elements of the requirements in b2 of Section 524B for the submission documentation, we're looking for the outputs of those processes and procedures. So, the things identified in the guidance document, like the risk management report, threat modeling, cybersecurity risk assessment, SBOM, all of those contribute to the demonstration or providing the reasonable assurance that the device is cybersecure. So, we're focused from the premarket submission standpoint on more of the output documentation from those processes.

Ben Hornseb: Got it. Thank you for clarifying. My next very quick question is around medical device data systems, specifically, a non-device MDDS and whether if there are components of an overall regulated medical device system that meets the non-device MDDS designation. Is the expectation that 524B documentation would be provided for those components, an SBOM, as an example, or because those components are technically not regulated per FDA policy, we are not required to submit for those components?

Matthew Hazelett: So, for the particular components themselves, you wouldn't have to provide an SBOM for the MDDS itself. What you would need to provide is the cybersecurity considerations on the submitted medical device from those components. So, this is consistent with our multi-function device products guidance, where we consider those to be what are identified as other functions, where the cybersecurity considerations from those different non-medical device functions need to be considered for how they interact with and interface with the subject medical device submission.

Ben Hornseb: Perfect. Thank you. That makes sense. Those are all the questions I had. Appreciate it.

CDR Kim Piermatteo: Thanks, Ben. And thank you, Matt. Our next question is coming from Sasha. Sasha, I've unmuted your line. Please unmute yourself and ask your question.

Sasha, I see that you've unmuted, but I don't know if you are double-muted.

We still cannot…

Sasha Perebikovsky: Can you hear me now?

CDR Kim Piermatteo: Yes, we can.

Sasha Perebikovsky: So, I wanted to ask, I know that in the latest guidance, you discussed a little bit about devices connected to the cloud. I wanted to know if there's any specific recommendations, additional resources you can give for medical devices that are cloud-connected that we might be able to leverage or templates that we might be able to leverage when preparing this guidance? Thank you.

CDR Kim Piermatteo: Thank you, Sasha. I'm going to turn it back over to Matt.

Matthew Hazelett: Sure. So, as we outlined in the guidance, the security objectives and considerations and recommendations that are made throughout the guidance do apply to devices that either exist solely in the cloud if they're a SaMD product or devices that interface with the cloud environment. We know that these are complex architectures, so, it's really important to describe what the architecture and the particular services that are being provided by the cloud service provider are as a part of your architecture descriptions consistent with the guidance recommendations.

We don't have any specific materials on cloud-based environments currently available at this time. Those are very dynamic environments, as you well know, and change very rapidly, but it is important for, as a part of your cybersecurity documentation to describe the environment that you are leveraging, the services that you're leveraging, and how that overall fits together to achieve the security objectives that are outlined in the premarket guidance.

So everything still is relevant. And we understand that cloud environments have shared responsibility where there's elements that the manufacturer is responsible for and there are elements in the back end that the cloud service providers are typically responsible for. But it's important to convey that architecture information as well as describing how you're going to maintain your elements of the architecture as a part of the overall design and maintenance of the device.

So, to put it simply in summary, there's nothing specific in terms of cloud-specific resources currently available that we're directly pointing to, but the considerations outlined in the guidance still apply for devices that leverage cloud-based environments.

Sasha Perebikovsky: Thank you.

CDR Kim Piermatteo: Thank you, Matt. Our next question is coming from Jim. Jim, I've unmuted your line. Please unmute yourself and ask your question.

Jim Jacobson: Okay. Thank you. This is Jim Jacobson from Siemens Healthineers. The metrics recommended in this section on TPLC security risk management cover postmarket activities. So how is it possible to provide this information for a new device or one with limited history, even given the suggestion of providing averages that, which might not make sense for a complex product portfolio that has very different characteristics?

CDR Kim Piermatteo: Thank you, Jim, for that question. I'm going to turn it over to Matt.

Matthew Hazelett: Sure. So, the metrics that we outline, we do indicate to provide those if they're available. So, if it's a brand new device and a new model that doesn't have a similar device that has been maintained, we understand that there might not be metric documentation available. So, you'd provide a justification for why that information is not possible to be provided based off of not having that history in order to provide those metrics. But it is possible for, if you're submitting an iterative change, to provide the measures and metrics from the prior model that demonstrates how your cybersecurity management program operates, as it can give us the potential confidence on how you're going to manage the device throughout its lifecycle as a part of the submission in order to give greater context for how your post-market lifecycle plans continue to function or work. But definitely, we acknowledge

that not every new device coming to market will have those metrics available. And you can provide a justification to that effect.

Jim Jacobson: Okay. Thank you.

CDR Kim Piermatteo: Thank you, Jim. And thank you, Matt. Our next question is coming from Sophia. Sophia, I've unmuted your line. Please unmute yourself and ask your question.

Sophia Lauwers: Hi. Thank you. So, I know you mentioned using exploitability instead of likelihood. I was wondering if you could give us some insight on what tools we could use to determine that. And if the CVSS score is a good way to start, should we be looking at the newly released 4.0 instead of the current 3.1?

CDR Kim Piermatteo: Thank you, Sophia. Matt, would you like to provide a response?

Matthew Hazelett: Sure. So, one thing I wanted to clarify just from the question, so we recommend using exploitability instead of using probability. Both of these assessment techniques are a way of measuring the likelihood of occurrence. So, we understand from the larger risk management perspective and traditional paradigms it's, exploitability is one mechanism for assessing likelihood. But we recommend that you use exploitability instead of probabilities because of the difficulty in assessing cybersecurity risks in a probabilistic manner, as you can with some other risk types for a particular device.

In terms of the different methodologies for security risk assessments that are out there, we definitely do see manufacturers try to leverage CVSS. There're difficulties in doing so in the premarket context because CVSS is intended as a risk prioritization methodology and not a risk acceptance methodology. So, in that, in idea in terms of is a particular methodology fit for purpose, that does create challenges. And sometimes, we see manufacturers make adaptations to the CVSS scoring methodology to make it more applicable to premarket cybersecurity risk assessment methodologies. So, we do point to some different resources, and we do have some recognized standards that go into some of the different risk assessment methodology approaches. But they all, similarly, have some pros and cons or may require adaptation in order to work in a premarket context. So, that's part of why it's important to provide the description of your methodology and your justification for where the methodology is a part of your premarket submission.

We are aware that the CVSS 4.0 just finalized yesterday. As this is a new update to the CVSS scoring, I know that it's going to take time for other entities, like NIST, and other organizations, like CISA, to move forward adopting the new version. But it may be something that people can consider moving forward, especially in the postmarket context, for risk, cybersecurity risk assessments moving forward. But likely, as the CVSS methodology is that risk prioritization measure, it likely still would not be appropriate as is out of the box for a premarket risk assessment scoring methodology.

CDR Kim Piermatteo: Thank you, Sophia, for your question. And thank you, Matt, for that response. Our next question is coming from Don. Don, I've unmuted your line. Please unmute yourself and ask your question.

Don, are you able to unmute your line?

Don Peters: Hi, can you hear me?

CDR Kim Piermatteo: Yes, we can.

Don Peters: Thank you. Yes, I also had a comment with regards to the use of exploitability on the slide. I think that others will find that confusing. However, I find that there is a very good annotation in the IEC/ISO SW96 document with regards to using it as a proxy for either using proxies such as exploitability or likelihood. I'm wondering, and my question is, can someone comment as far as any status or plan for SW96 being entered into the FDA consensus standard list?

CDR Kim Piermatteo: Thank you, Don, for your question. I'm going to turn this over to Matt.

Matthew Hazelett: Sure. I'm actually able to state that we have recognized SW96. We just recently recognized it. So, it is currently in the standards database of FDA-recognized standards.

Don Peters: Excellent.

CDR Kim Piermatteo: Thanks, Matt. Our next question is coming from Canwen. Canwen, I've unmuted your line. Please unmute yourself and ask your question.

Canwen Liu: Yes. My question is about the security risk management, the security architecture document and threat modeling document and the presentation of the slides today emphasize on the threat modeling document. But from what I can see, the FDA guidance is more emphasized on the security architecture. So, my question is that can we have the threat modeling part included in a split architecture, or should be the other way around?

CDR Kim Piermatteo: Canwen, I had a hard time, a little bit, hearing you. But I'm going to see, Matt, do you understand what she's asking, or should I ask her to repeat the question?

Matthew Hazelett: I believe I got it. I can repeat it just to confirm my understanding. So you were asking around the differences between threat modeling and architecture view documentation and whether these can be included in one another or vice versa as a part of the premarket submission documentation? Is that correct?

Canwen Liu: Yes, correct. Yes. And for me, security architecture is not just about security architecture views. So, this would be a security architecture document for the entire device or system.

Matthew Hazelett: Sure. So, for the different documentation deliverables, so threat modeling is really that systematic process for evaluating the entire system for potential threats and appropriate controls. What we go into detail in terms of the architecture view is really getting into specific documentation in terms of what's included in Appendix 2. So that may go beyond what would traditionally be included in standard threat modeling documentation because of how detailed we're looking for those architecture views to be.

So, we acknowledge that the architecture views may be included as a part of the threat modeling documentation, but we recommend that you include the level of detail outlined in Appendix 2 of the

guidance if you're going to include the views as part of the threat modeling documentation. But that the architecture view should still be a distinctive element within the threat modeling documentation if it is being included there.

Canwen Liu: I see. And you don't require a separate security architecture document for the medical device?

Matthew Hazelett: Yeah. So it goes more than just one specific architecture. So there's the four different architecture views, including the security use case views, which extend to the different operational and states and clinical use cases. So, you want to make sure that you're including all of the relevant architecture views and not just a kind of global system view. That's one of the views we're looking for, but you would want to make sure you're addressing all four of the architecture view types identified in the guidance.

Canwen Liu: Thank you.

CDR Kim Piermatteo: Thank you, Matt, for that response. We have time for one more quick question and, hopefully, a quick response. The next stakeholder I'm going to call on is Chandramohan. Chandramohan, I have unmuted your line. Please unmute yourself and ask your question.

If you are double-muted, we are unable.

Chandramohan Thiruvamkulam: Can you hear me now?

CDR Kim Piermatteo: Yes, we can.

Chandramohan Thiruvamkulam: Sure. So, a quick question, I just want to, want your advice. Rather, can you compare and contrast the requirements of the guidance here with respect to EU Cybersecurity Act for medical devices? How are they similar? Are they different? If so, what are the differences?

CDR Kim Piermatteo: Jessica, I can turn it over to you. And you can provide a response. I don't know if that's a quick answer.

Jessica Wilkerson: I can definitely take it to say that that is not something that we would be able to answer today, but if there would be interest in following up, it could be sent to an appropriate FDA email address for a follow-up. Thank you.

Chandramohan Thiruvamkulam: Thank you. And then one quick, another question is, since this is part of the submission, how aligned is the eSTAR with regards to the changes that are going to come with this guidance? Do we need to make, is the eSTAR updated to accommodate the changes required?

CDR Kim Piermatteo: Thank you for that question. I'm going to turn it over to Matt for a quick response regarding eSTAR.

Matthew Hazelett: Sure. The current eSTAR template identifies that a update to the eSTAR template to align with the guidance in the 524B submission elements is forthcoming. So that update will be made

here shortly in order to update it to align with all of the submission documentation elements in the new final guidance.

Chandramohan Thiruvamkulam: Thank you so much.

CDR Kim Piermatteo: Great. Thank you, Matt. Alright, at this time, this wraps up our question and answer segment for today. We want to thank you for all of your questions. They were very, you were very engaged. So we thank you very much. And I'd like to turn it back over to Matt for his final thoughts. Matt?

Matthew Hazelett: Sure. Thank you. I wanted to thank everyone for attending and for all the questions. We definitely appreciate all of the engagement that we've received on the guidance. We know that there's a going, moving evolution of cybersecurity in the medical device space and we know that this is a change to how FDA has been evaluating documentation, but we really believe that this is the important documentation in order to provide continued safety and effectiveness for patients that are using these medical devices and being treated and cared for with these devices. So we believe that this is a continued important evolution to the medical device space.

CDR Kim Piermatteo: Thank you, Matt, for those final thoughts. And thanks again for your presentation today. I'd also like to thank Aftin, Jessica, and Erin for participating on our panel. And for your information, printable slides of today's presentation, like I mentioned earlier, are currently available on CDRH Learn at the link provided on the slide under the section titled, Specialty Technical Topics, and the subsection, Digital Health.

A recording of today's webinar and a transcript will be posted to CDRH Learn under the same section and subsection in the next few weeks. A screenshot of where you can find these webinar materials has been provided on the slide as well.

If you have additional questions about today's webinar, please feel free to reach out to us in DICE at DICE@fda.hhs.gov.

And lastly, we hope you are able to join us for a future CDRH webinar. A listing of upcoming webinars can be found via the link provided on the bottom of this slide at www.fda.gov/CDRHWebinar. Thank you all again for joining us. This concludes today's webinar. Take care.

****

END