Draft Guidance: Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act
April 30, 2024

Moderator: CDR Kim Piermatteo

CDR Kim Piermatteo: Hello, everyone, and welcome to today's CDRH webinar. Thanks for joining us. 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Our topic today is the draft guidance titled, Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act, which was issued on March 13th, 2024. During today's webinar, we will discuss this draft guidance, which proposes updated recommendations to industry on cybersecurity considerations for cyber devices and for documentation and device premarket submissions. Today, we will also take time to answer your questions about this draft guidance.

Before we begin, I'd like to provide a few reminders for the webinar. First, please make sure you've joined us through the Zoom app and not through a web browser to avoid technical issues. Second, the intended audience for this webinar is industry. Trade press reporters are encouraged to consult with a CDRH Trade Press Team at cdrhtradepress@fda.hhs.gov and members of national media may consult with the FDA's Office of Media Affairs at fdaoma@fda.hhs.gov. Third, for those of you who might want to follow along, you may access printable slides of today's presentation from CDRH Learn at www.fda.gov/training/cdrhlearn under the section titled Specialty Technical Topics and the subsection titled Digital Health. And lastly, we look forward to interacting with you during the live question and answer segment today. If you have a question, please wait, and raise your hand at the end of today's presentation to get into the queue.

I now have the pleasure of introducing our presenter for today's webinar, Matthew Hazelett, Senior Cybersecurity Policy Analyst on the Digital Health Staff within CDRH's Office of Product Evaluation and Quality. 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. Matt?

Matt Hazelett: Thanks, Kim. As Kim mentioned, I'm Matt Hazelett, and I'm the Senior Cybersecurity Policy Analyst in the Office of Product Evaluation and Quality's Digital Health Staff as part of the Center for Devices and Radiological Health. I'll be leading today's presentation for the webinar.

Today's webinar will focus on the draft guidance on Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the Food, Drug & Cosmetic Act.

This presentation will cover the main learning objectives outlined on this slide. We will describe the proposed interpretations of key terms from Section 524B of the Food, Drug & Cosmetic Act.
We will describe proposed recommendations of what to provide in premarket submissions for each 524B requirement. We will describe the proposed recommendations of what to provide in premarket submissions for modifications to existing devices. And finally, we'll describe FDA's proposed thoughts on how 524B fits into the existing regulatory submission pathways.

We will begin with some background information on the draft Select Update. Given timing considerations from Section 524B of the Food, Drug & Cosmetic Act was passed and went into effect compared with the finalization process for the Premarket Cybersecurity Guidance, this Select Update provides interpretation of elements from Section 524B that couldn't be included in the final guidance, Cybersecurity in Medical Devices, Quality System Considerations and Content of Premarket Submissions, which was finalized in September of 2023. When this Select Update is finalized, the content from Section 2 of this Select Update will be added as Section 7 to the Premarket Cybersecurity Guidance.

We will now discuss the proposed interpretations of key terms from Section 524B.

For the proposed definition of cyber device, FDA considers a cyber device to include devices that are or contain software, including firmware or programmable logic. For the ability to connect to the internet criterion, FDA considers a larger system view in order to make this determination, and that it includes devices that are able to connect to the internet, whether intentionally or unintentionally, through any means, including at any point identified in the evaluation of the threat surface of the device and the environment of use.

This approach is due to it being well demonstrated that if a device has the ability to connect to the internet, it is possible that it can be connected to the internet, regardless of whether such connectivity was intended by the device sponsor. Accordingly, FDA considers that devices that include the following features to have the ability to connect to the internet. The list below is illustrative and not exhaustive, and includes Wi-Fi or cellular connections, network, server, or cloud service provider connections, the use of Bluetooth or Bluetooth Low Energy, radiofrequency communications, inductive communications, and hardware connectors capable of connecting to the internet like USB, ethernet, or serial ports on the device.

For the proposed definition of related system, FDA considers related systems to include, among other things, the manufacturer-controlled elements such as other medical devices, software that performs other functions as described in FDA's guidance, Multiple Function Device Products, Policy, and Considerations, software and firmware updates servers, and the manufacturer-controlled aspects of connections to health care facility networks.

For the proposed definition of coordinated vulnerability disclosure and related procedures, FDA considers that coordinated vulnerability disclosure and related procedures could include coordinated disclosure of vulnerabilities and exploits identified by external entities, including third-party software suppliers and researchers, the disclosure of vulnerabilities and exploits identified by the manufacturer of the cyber devices, and manufacturer procedures to carry out disclosures of the vulnerabilities and exploits, as identified above.

We'll now discuss the proposed premarket submission documentation recommendations for the 524B requirements.

For the post market plans and procedures required under Section 524B, subsection (b)(1), these plans should include the information recommended for the cybersecurity management plan described in Section 6B of the Premarket Cybersecurity Guidance. They should also include details on coordinated vulnerability disclosure and related procedures, as discussed in the proposed recommendations earlier. They should also describe the timelines with associated justifications to develop and release patches

and updates as required under Section 524B, subsection (b)(2), A and B. This should also include a plan for maintaining documentation as new information becomes available, as well as maintaining documentation to account for any differences in risk management for fielded devices, such as differences between marketed devices and devices no longer marketed, but still in use.

For the documentation to provide a reasonable assurance that the device and related systems are cyber secure as required under Section 524B, subsection (b)(2), the documentation recommendations identified in the Premarket Cybersecurity Guidance and summarized in Appendix 4 of the Premarket Cybersecurity Guidance, should be considered, and used to demonstrate the reasonable assurance that the device and related systems are cyber secure.

The Software Bill of Materials, or SBOM, required under Section 524B, subsection (b)(3), the draft guidance recommends that manufacturers provide SBOMs that contain the information recommended in Section V.A.4(b) of the Premarket Cybersecurity Guidance.

We'll now discuss the proposed premarket submission documentation recommendations for modifications to existing devices.

For modifications to existing devices which rise to the level of requiring a new premarket submission, the draft Select Update outlines two types of changes, changes that may impact cybersecurity and changes unlikely to impact cybersecurity. In general, changes that may impact cybersecurity could include changes to authentication or encryption algorithms, new connectivity features, or changing software update processes or mechanisms. In general, changes unlikely to impact cybersecurity could include material changes, sterilization method changes, or a change to an algorithm without a change to the architecture or software structure or connectivity.

For submissions for changes that may impact cybersecurity, for these types of changes you should see Section II.C of the Select Update, which includes all the documentation identified in the prior slides for new submissions for the required and recommended documentation to be included with each premarket submission.

For submissions for changes unlikely to impact cybersecurity, in order to be least burdensome for these types of changes, FDA has proposed recommended documentation for each of the 524B requirements. For the plans and procedures under Section 524B, subsection (b)(1), if the plan was not previously provided, manufacturers would provide the plan as described in Section 524B, subsection (b)(1). And we recommend that it contain the information as described in Section II.C.1 of the Select Update Guidance. If the plan was previously provided, the manufacturer should provide a reference to the prior submission, a summary of any changes to the plan since that submission, and summaries of any updates or patches made to address vulnerabilities or exploits on the device.

For providing a reasonable assurance that the device and related systems are cyber secure under 524B, subsection (b)(2), instead of the full documentation described previously, manufacturers may provide summary information to provide that there's a reasonable assurance that the device and related systems are cyber secure, and no uncontrolled vulnerabilities as identified in the post market cybersecurity guidance exist. FDA recommends that this information include a summary assessment of any cybersecurity impact from the changes made since the last authorization, such as letter to file or

annually reportable changes, and that the summary assessment include any vulnerabilities identified for the last authorization that were made in the device.

Also, as a part of meeting the requirement under Section 524B, subsection (b)(2) for providing a reasonable assurance that the device and related systems are cyber secure, if there are any limitations to updating the cybersecurity, the manufacturer should provide a description of the limitations of the system, which prevent further cybersecurity controls, an assessment of the residual cybersecurity risk, and an assessment of the benefits and risks of the system.

Finally, for the SBOM requirement under Section 524B, subsection (b)(3), the Food, Drug & Cosmetic Act requires that manufacturers of cyber devices provide an SBOM. To assist with complying with this requirement, we recommend that a cyber device provide SBOMs that contain the information recommended in Section V.A.4(b) of the Premarket Cybersecurity Guidance in each of these submissions for changes unlikely to impact cybersecurity so that the agency has an updated understanding of the current software.

We'll now discuss our proposed thinking on Section 524B and how it relates to the regulatory submission pathways.

Section 3305(c) of the Food and Drug Omnibus Reform Act, or FDORA, provides that nothing in Section 524B of the Food, Drug & Cosmetic Act shall be construed to affect the secretary's authority related to ensuring that there is a reasonable assurance of the safety and effectiveness of devices, which may include ensuring that there is a reasonable assurance of the cybersecurity of certain cyber devices. FDA interprets this provision to mean that a reasonable assurance of cybersecurity can be part of FDA's determination of a device's safety and effectiveness.

Moreover, a determination that there is a reasonable assurance of cybersecurity is relevant to the various premarket pathways and authorization under them. Specifically, FDA's review of a Premarket Approval, or PMA application; Product Development Protocol; De Novo; Humanitarian Device Exemption; and Premarket Notification under 510(k)s.

For cybersecurity and 510(k) submissions, when evaluating a 510(k) submission, FDA considers things like changes to the environment of use, such as changes in technology the subject device will interact with or operate with; and any new risks or vulnerabilities the device will be exposed to; new risks or vulnerabilities in the technological characteristics compared to the predicate device submission, such as changes to the level of support for component software, vulnerabilities in communication protocols for technology used by the subject device, and how the subject device, design, and/or performance testing addresses these new risks or vulnerabilities. This all also couples with our overall benefit-risk framework for evaluating devices and making our final determination of whether the device is substantially equivalent.

The Select Update also outlines an example of how the cybersecurity authorities fit into the 510(k) process. It outlines that, for example, if in reviewing the 510(k) for an alarm for a central nursing station software, FDA identifies that the device has increased risk compared to its predicate because it does not have the necessary encryption to protect against a recently identified cybersecurity threat, the FDA may ask for additional performance data. If the data provided in response is inadequate, FDA would likely make a determination that the new device is not substantially equivalent to the predicate device

because this threat, if exploited, could negatively impact the safety and effectiveness of the device because alarm accuracy is essential for health care providers to effectively monitor the health of patients in the hospital.

This slide provides the resources that were discussed in today's presentation and their associated URLs.

As the Select Update is a draft guidance, we wanted to provide a note about draft guidances. You may comment on any guidance at any time. Please submit comments on draft guidances before the closure date to ensure that FDA considers your comment on a draft guidance before we work on finalizing the guidance.

To summarize today's presentation, the draft Select Update includes proposed interpretations of key terms used in Section 524B of the Food, Drug & Cosmetic Act. Each 524B requirement has required and/or recommended documentation associated with it. Submission documentation for modifications to existing devices will generally differ based off of the type of change to the existing device. Finally, providing a reasonable assurance that the device and related systems are cyber secure will be assessed as part of FDA's existing regulatory submission evaluation process.

Thank you for joining today's webinar presentation. I'll now turn it back to Kim to open our question and answer session.

CDR Kim Piermatteo: Thanks, Matt, for that presentation. We will now transition to our interactive question and answer segment for today. I'd first like to introduce our additional panelist, Jessica Wilkerson, Senior Cyber Policy Advisor and Medical Device Cybersecurity Team Lead within the Division of Medical Device Cybersecurity in the Office of Readiness and Response in CDRH's Office of Strategic Partnerships and Technology Innovation, or OST. So, thanks for joining us today, Jessica.

Before we take our first question, I'd like to go over how we will manage this segment and a few reminders. First, to ask a question, please select the Raise Hand icon, which should appear on the bottom of your Zoom screen. I will announce your name and give you permission to talk. When prompted in Zoom, 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. We also appreciate that you may have a very specific question involving your device or a specific scenario; however, we might not be able to answer such specific questions. Therefore, we will try to frame a broader response based on what's described in the draft guidance.

Also, when asking a question, remember the scope of today's webinar is the Select Update, including who is required to comply with 524B, FDA's interpretation of cyber device, documentation recommendations related to each 524B provision, how modifications to previously authorized devices and 524B may interact, and FDA's interpretation of reasonable assurance of cybersecurity. Questions related to the final guidance should be directed to either cybermed@fda.hhs.gov for general questions, or OPEQ_cybersecurity@fda.hhs.gov for implementation or submission-specific questions.

So then after you ask your question, please remember to lower your hand in Zoom. And then if you have another question, please raise your hand again in Zoom to get back into the queue, and I will call on you as time permits.

Before we take our first live question, I'd like to ask Jessica one question we've previously been asked about this draft guidance. Jessica, the question is in regards to the Select Update finalization. The question is, how will this Select Update affect the final guidance titled Cybersecurity and Medical Devices, Quality System Considerations and Content of Premarket Submissions?

Jessica Wilkerson: Thank you, Kim, for the question. As stated by Matt during the original presentation, once finalized, this draft Select Update will become Section 7 of the final guidance titled Cybersecurity and Medical Devices, Quality System Considerations and Content of Premarket Submissions. Thank you.

CDR Kim Piermatteo: Thanks, Jessica. I'd now like to call on Gergely. Gergely, I have unmuted your line. Please unmute yourself and ask your question.

Gergely Antalfi: Hi. I'm Gergely Antalfi from Boston Scientific. And first of all, thank you for taking my question. And my question is, could you clarify the guidance on the timely security updates, lines 111 to 119 of the draft versus the risk management of all fielded versions of the software, lines 130 to 136 of the draft? For instance, by providing some examples on how these two may be balanced over the decade of two or medical device in the field.

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

Matt Hazelett: Sure. In terms of the aspect for timely updates, that's going to depend on the device architecture and what technological components are factored in. So, we recommend that those timelines be specific to, and be in alignment commensurate with the risk of the device, as well as the technology involved. So, you should provide justifications for any different elements in the system. So, we're going to expect faster or more routine updates to things like software that exists in the cloud service provider environment, because that's a very dynamic environment where software lives, as opposed to an embedded implant device. So based off of the technology involved, you should be providing a risk-based justification for what the timeline for updates are.

In terms of considering the risks against different versions of the system, so we know that there are sometimes delays between when an update is made available and when those updates are implemented in the field. So as new vulnerabilities are identified or new risks to the system are identified, if you have multiple different versions of software or firmware in use by users, you should be considering the risks against all of the associated versions, as those may differ given what updates have or have not been applied to particular devices. Thank you.

Gergely Antalfi: Thank you.

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

Alex Smith: Hi. This is Alex Smith from Hogan Lovells. A quick question. I receive this question about once a day from clients, and they're very concerned that FDA's going to start scanning the electronic version of the SBOMs. Is there any intent to do this in the future? Thank you.

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

Matt Hazelett: Sure. So definitely, we know that the SBOM landscape is dynamic. So as SBOM capabilities mature and evolve over time, FDA's review of that information will also mature and evolve over time. So, we definitely intend to use SBOMs to help us identify potential vulnerabilities that can impact a device during premarket submissions. So, we're going to be leveraging the SBOMs to make the best informed-based and risk-based considerations for a particular submission. So, it's definitely something that we're going to consider moving forward as it's a very dynamic landscape and we're trying to best utilize SBOMs in a manner to make the best decisions on files based off of the risks involved.

Alex Smith: Thank you. That's helpful. Appreciate it.

CDR Kim Piermatteo: Thanks, Alex, and thanks, Matt. Our next question is coming from Kaitlin. Kaitlin, I have unmuted your line. Please unmute yourself and ask your question.

Kaitlin K: Hi, this is Kaitlin. Our question is for the changes that may impact cybersecurity, one of the items is authentication and encryption algorithms. We just wanted to clarify the phrasing. Is the authentication, are we referring only to authentication algorithms or general authentication changes?

CDR Kim Piermatteo: Thanks, Kaitlin. Again, Matt or Jessica, I will leave it up to you.

Matt Hazelett: Happy to take this one. So, it definitely can apply to both. It depends on the scope and nature of the change. If you're developing changes for a particular submission and you're unsure of what process may be appropriate and whether those changes may require a submission, or whether those changes would be considered to impact the cybersecurity of the device, we definitely encourage manufacturers to leverage the Q-Submission program to get greater clarity given the specifics of a particular change. But definitely changes to general authentication or user authentication as well as authentication of communication protocols or software updates are all things that potentially could have an impact on the cybersecurity and fall under those recommendations for submissions for modifications.

Kaitlin K: Thank you.

CDR Kim Piermatteo: Thank you, Kaitlin, for your question. And thank you, Matt, for your response. Our next question is coming from Phil. Phil, I have unmuted your line. Please unmute yourself and ask your question.

Phil Englert: Hi. Yeah, thank you. This is Phil Englert with Health-ISAC. For many years, the FDA had stated that updates to devices that only, that were only addressed cybersecurity issues didn't have to be through submission. Can you clarify how 524B has changed the guidance relative to that previous position? Thank you.

CDR Kim Piermatteo: Thanks, Bill. Matt, I'll turn it over to you.

Matt Hazelett: Sure. So, the FDA guidance documents in terms of determining whether something is a recall versus an enhancement as well as the guidances on deciding when to submit a 510(k) for software modifications or deciding when to submit a 510(k) for general modifications as well as our PMA

supplements guidances are all still relevant, and those considerations still factor in. So, the 524B requirements do not directly change whether a modification to the device would need to come into the agency for review. The recommendations that we have proposed in the draft Select Update are focused around if you have the need to make a submission based off of those other guidances, what cybersecurity documentation will the Agency be looking for based off of whether some of those changes can impact cybersecurity or whether they'd be unlikely to impact the cybersecurity of the device.

CDR Kim Piermatteo: Great. Thanks, Matt. And thank you, Phil, for the question. Our next question is coming from Duane. Duane, I have unmuted your line. Please unmute yourself and ask your question.

Duane Herberg: Yeah. Thanks for taking my question. My question is on the section regarding changes unlikely to impact cybersecurity. Your slide today says FDA recommends information include a summary assessment, including a summary assessment of any cybersecurity impact from changes made since the last authorization. Are those two different summary assessments, or are they the same thing?

CDR Kim Piermatteo: Thanks, Duane. Matt, I'll turn it over to you first.

Matt Hazelett: Sure. So, what we're recommending is one overall summary assessment and identifying some components around what can be included in that summary assessment. You definitely are welcome to submit any comments if there's a lack of clarity in the wording, but the intent is that it would be one overall summary assessment that includes some of the details that are listed in that section of the guidance.

Duane Herberg: OK. Thank you.

CDR Kim Piermatteo: Thanks, Duane. And thanks, Matt. Our next question is coming from, and I apologize if I mispronounce this, it's Vaishnav Gollapudi. I have unmuted your line. Please unmute yourself and ask your question.

Vaishnav Gollapudi: Hi, there. This is Vaishnav from Nevro. I'm curious if this guidance impacts any nondevice or device, medical device data systems.

CDR Kim Piermatteo: Thank you for that question. I will turn it over to Matt or Jessica. I mean, feel free.

Matt Hazelett: I'm happy to take this one. In terms of the scope of the guidance, so in order to be considered a cyber device, you have to first be a medical device. So, the cyber device definition does not change the medical device definition. Cyber devices are a subset of the overall definition of medical devices. The general premarket guidance is broader than just cyber devices, as it applies to other submission types. But in terms of what would be considered a cyber device and in scope, you'd first have to be a medical device. In terms of the medical device data system aspect, those would be considered related systems, so, you would have to consider the cybersecurity impact of those on a medical device if you're making a medical device submission. And that's consistent with our multiple function device products guidance.

Vaishnav Gollapudi: Thank you. Appreciate it.

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

Gilles Pelletier: Yes, thank you. I think my question maybe a follow-up to the just previous one. So, would this guidance apply to software as a medical device? In a sense, it could be installed on a customer or end user's furnished PC that would have internet connection or Wi-Fi, but it's provided as part of the device. Thank you.

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

Matt Hazelett: Sure. So, most SaMD products and pretty much all that we have considered so far are considered cyber devices based off of the platforms that they operate on. So, whether that's within a cloud service provider environment, a mobile device or tablet, or a computer system, those would all be the operating environment where the SaMD product would be performing its intended use and intended function. So those would be considered cyber devices as the platforms in which they operate on would have the ability to connect.

CDR Kim Piermatteo: Thanks, Matt. And thanks, Gilles, for your question. Our next question is coming from Andrew. Andrew, I have unmuted your line. Please unmute yourself and ask your question.

Andrew Long: Hello. Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Andrew Long: Hi. This is Jaiyen. My question is regarding a software accessory. So, if our submission is for a software accessory which is based in its own right not a cyber device, but the reliance on other medical device systems to integrate and establish indirect connections to internet, for example. Then my question is, what cybersecurity information would the FDA expect the submission provided for this software accessory? Thank you.

CDR Kim Piermatteo: Hi. Andrian, I believe it was. We had a hard time hearing you, your question specifically. Would you mind repeating your question?

Andrew Long: Can you hear me better?

CDR Kim Piermatteo: We can hear you. But please repeat your question. Yes.

Andrew Long: Yeah. So, my question is for a, if a subjective device is a software accessory, and by its own right it is an accessory, it's not a separate device, but it relies on other medical device systems to integrate and establish connections indirectly to internet, and then in such scenarios, what cybersecurity information would the FDA expect for this submission?

CDR Kim Piermatteo: OK, thank you. I believe you're describing, you're talking about accessories, right? Software as accessories?

Andrew Long: Yes.

CDR Kim Piermatteo: OK. Let me turn it over to Matt.

Matt Hazelett: Sure. So, if the accessories performing medical device functionality or supporting the medical device functionality that's considered in terms of the larger cyber device and related systems aspects, so we would still be looking for cybersecurity considerations from the accessory in terms of how it may impact the larger system. So, we would be looking for cybersecurity information consistent with the guidance and also in accordance with the multiple function device, device product guidance in terms of what cybersecurity impacts those accessories could have on the main medical device and the larger medical device system.

Andrew Long: OK, thank you.

CDR Kim Piermatteo: Thanks, Matt. Alright, our next question is coming from Chris. Chris, I have, Chris Gates, I have unmuted your line. Please unmute yourself and ask your question.

Christopher Gates: Thank you. Christopher Gates of Velentium. The current scope of the guidance leads to a lot of confusion between 524B, and the September finalized guidance. Can you add some clarity as to the distinctions between those two, between the 524B and that finalized guidance? As an example, if you had that completely standalone medical device that had no communications of any type, it would not be a cyber device; therefore, 524B would not be applicable, but is the September 2023 finalized guidance still?

CDR Kim Piermatteo: Thank you, Christopher, for your question. Jessica, I will turn it over to you. I did cut, mine cut out at the last bit, so I don't know if Christopher needs to repeat anything. But I'll let you provide a response first.

Jessica Wilkerson: Thanks so much, Kim. And thank you, Chris, for the question. So, it is important to understand that the scope of 524B and the scope of the final September 2023 guidance are distinct. 524B is tied to the definition within the text of the statute itself, including that ability to connect. The guidance scope, the scope of the September 2023 guidance is broader, and the scope of the guidance is software, medical devices that contain software, firmware, or programmable logic. So, one way to think about it is that cyber devices, and specifically those contemplated under 524B, are a subset of the devices that are covered by the guidance in both the cyber devices and devices within the scope of the guidance will need to provide appropriate cybersecurity documentation as detailed within that guidance. Thank you.

CDR Kim Piermatteo: Thank you, Jessica. And thank you, Christopher, for that question. Our next question is coming from Rshah. Rshah, I have unmuted your line. Please unmute yourself and ask your question.

Rshah: Hi, my name is Ronald, and I'm from [INAUDIBLE]. So basically, I have a previously cleared 510(k) device, and I'm making a new change to labeling, which does not impact cybersecurity via eSTAR format. So, my question is, do I need to select the cybersecurity section where it asks, select all the sections affected by modifications in comparison to predicate and provide all the documentation, which is listed in cybersecurity section, including SBOMs and all the other documentation? Or will a summary assessment will be sufficient?

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

Matt Hazelett: Sure. So given the language in the statutory provisions for all submissions moving forward for devices that are considered cyber devices, all of the documentation is currently expected, given the direct language in the statute. The proposal in this draft Select Update is intended to implement our least burdensome principles where feasible to tailor the recommended documentation to be fit for purpose of the submission. However, until this guidance is finalized, and we are able to implement the modifications proposal for submissions using the eSTAR template, the complete documentation would still need to be submitted until the guidance is finalized and changes can be made to eSTAR for enabling the proposal for modifications unlikely to impact the cybersecurity of the device.

For things that aren't leveraging the eSTAR template like certain PMA supplements and 30-day notices, the FDA can consider accepting the proposed summary documentation identified in the draft, but we may request full documentation if needed. But for submissions under the 510(k) submission platform, including traditional, special, and abbreviated 510(k), the full documentation is needed until we finalize our modifications proposal.

CDR Kim Piermatteo: Great. Thank you, Matt, for that response. Alright, so, we have quite a few hands raised. We are going to move through them and get to them as we can today. Our next question is coming from Erin. Erin, I have unmuted your line. Please unmute yourself and ask your question.

Erin Bissonnette: Hi, thank you. Erin Bissonnette from Stryker Instruments. I have a real quick question with regard to the cybersecurity documentation, both for new devices and for the changed submissions. We keep hearing about a six-month freshness for the pen test, but I haven't seen it written expressly. So, is that a real expectation, and is that documented somewhere?

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

Matt Hazelett: Sure. Pen testing is a point-in-time assessment, so it's based off of evaluating the device with the current skills of an attacker. So, there is a sense of timeliness in terms of when that testing is performed as opposed to the submission timeline. So internally, when we're looking at pen testing, we're looking for ideally something within six months to a year. The guidance proposes that pen testing be performed, for example, it's provided as an e.g., of annually, but it should be commensurate with the risk. But we do evaluate the totality of the information and considerations for assessments of any newly identified risks or threats to the device and the technology that the device uses as a course of our review process. So, it's what we view as a potential best practice, but we evaluate the totality and that's based off of the example of annually for the recurrence of penetration testing.

Erin Bissonnette: Thank you.

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

Julian Alpers: Hi. Thank you very much. Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Julian Alpers: Perfect. So, I have a question, which is raised most likely from our clients. When finalizing this new guidance, you stated that for cybersecure, for changes that have less or no impact to cybersecurity, you can state a summary information. Can you maybe clarify a little bit more what the extent of the summary information should be? Is it a reference to the old information? Is it just two or three sentences? Or how much do you expect for the summary information?

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

Matt Hazelett: Sure. So generally, for current submissions for changes unlikely to impact the cybersecurity of the device, we expect the full documentation to be provided, especially for anything coming in under the eSTAR templates. There are a few submission types for PMA supplements, like 30-day notices that do not currently use the eSTAR template. And in those instances, we can consider accepting summary information as proposed in the draft Select Update covering the points that are provided there, but we may still request the full documentation to be provided if the summary information is insufficient as we continue to work to finalize this draft Select Update.

Julian Alpers: OK. Thank you very much.

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

Ramki Pillai: Thank you. You can hear me?

CDR Kim Piermatteo: Yes, we can.

Ramki Pillai: Thank you. So, this Ramki Pillai from LivaNova. I have a question on the CVD procedure. It was mentioned that the CVD should also include other third-party disclosures and internal findings as well. So, does it need to be explicitly included in the CVD, or it can be part of the post market cybersecurity procedure itself? Because that covers pretty much all these things anyway most of the time. Yeah. Thank you.

CDR Kim Piermatteo: Thank you, Ramki. I'd like to turn it over to Jessica. Jessica, would you like to provide a response?

Jessica Wilkerson: I'd love to. Thank you so much. Yes, so the expectation is that coordinated vulnerability disclosure programs will cover any components relevant to the medical device itself. Obviously, coordinated disclosure programs are meant to help manufacturers, the FDA, and the sector, including patients, have confidence that vulnerabilities within a given medical device may be addressed.

And so, the scope of a coordinated vulnerability disclosure program should include any vulnerabilities that may arise within that medical device, regardless of whether the vulnerabilities are considered third party or not. Thank you.

Ramki Pillai: Thank you.

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

Chris K: Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Chris Ki: Thank you. My question is with regards to Section D modification under changes unlikely to impact cybersecurity. One of the points discussed is if there are any limitations to updating the cybersecurity of the device and provides recommendations for information to include. My question specifically is, does this apply to devices that fall into both categories? Let's say some changes were made that do not impact cybersecurity, but some changes do impact cybersecurity. But in that process, there may be limitations that cannot fully address all of the cybersecurity concerns. Let's say an operating system is out of date, for instance. Would we in that case submit all the required documentation, and in addition, the assessment of cybersecurity controls, residual risk, and the benefits and risks of the system?

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

Matt Hazelett: Sure. So, in the scenario you described, if you're making changes that can both impact cybersecurity as well as changes that are unlikely to impact cybersecurity, the documentation we would be looking for would be what's recommended for changes that are likely to impact the cybersecurity of the device. In that documentation, if there are limitations to your system that preclude further updates to any areas, you should be providing that as a part of your risk management documentation and identifying those generally.

So, if there are aspects to an established system that have limitations, definitely identify what those limitations are. And the FDA will consider that in our total benefit-risk framework for evaluating individual submissions based off of the benefits and risks. But there may be circumstances where the FDA does not agree with your assessment or justification provided for some of those limitations. So just be aware that we are still fully evaluating, but if there are specific limitations, definitely identify those and provide the documentation as recommended in the draft Select Update if that's encountered.

Ramki Pillai: Thank you.

CDR Kim Piermatteo: Thank you, Chris. And thank you, Matt. Our next question is coming from Chris Reed. Chris Reed, I have unmuted your line. Please unmute yourself and ask your question.

Chris Reed: Yeah. Hi, Matt and Jessica and Kim. Thanks so much. There's been a little bit of confusion, and it was in your slides too. It referenced providing additional performance data. And there was an earlier statement around performance testing. This is around the nonsubstantial equivalence for 510(k)s. Can you elaborate a little bit more of what's considered performance data in this context, just to help us understand what FDA may be looking for?

CDR Kim Piermatteo: Thank you, Chris, for that question. Matt, I'm going to come to you first.

Matt Hazelett: Sure. So, in terms of the performance data that's identified that's consistent with the 510(k) flowchart in terms of the decision steps around evaluating the performance data, so that can include the design documentation. So, some of the threat modeling risk assessment architecture review documentation can factor into that, as well as the cybersecurity testing that's recommended in the guidance in terms of the actual testing outcomes, including the penetration testing and the assessment of those findings. So, performance data can be pretty general in terms of what can be considered in order to assess what the differences in technological characteristics exist between the subject device and the predicate.

CDR Kim Piermatteo: Thank you, Matt. And thank you, Chris, for that question. We have time for maybe one or two more questions for today. So, the next person I'm calling on is Monica. Monica, I have unmuted your line. Please unmute yourself and ask your question.

Monica Stalin: Hi. Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Monica Stalin: Thank you. My question is, could you please clarify how much of related device should be considered in scope of a medical device security? Is the goal limited to ensuring medical device is safe and effective, or should it expand to data security in connected nonmedical software system?

CDR Kim Piermatteo: Thank you, Monica. Matt, would you like to start? And then Jessica, feel free to chime in if you need.

Matt Hazelett: Sure. So largely, it's device-dependent and we look at the overall medical device system in terms of evaluating what the particular risks are and potential impacts of the overall device. We know that devices don't operate in isolation once they're connected in terms of considerations of impacts to potential hospital networks or home networks. So, we do look at the overall medical device system, but it is dependent on the device in terms of what specific risks and considerations are applied.

CDR Kim Piermatteo: Great. Thanks, Matt. And thank you, Monica, for that question. We have time for another question, our last one for today. And that is coming from Mohamad. I have unmuted your line. Please unmute yourself and ask your question.

Mohamad Foustok: Hi, this is Mohamad Foustok from Bold Type. With regards to this update and the phrase reasonable assurance of cybersecurity, can you elaborate as to the approach by which this will be determined? Particularly, what is reasonable? Thank you for taking my question.

CDR Kim Piermatteo: Thank you, Mohamad. Matt, I'll turn it over to you.

Matt Hazelett: Sure. So much like the considerations around reasonable assurance of safety and effectiveness, there's a lot of factors that go into that consideration. So, the reasonable assurance that the device and related systems are cyber secure, as is pointed out in the draft Select Update, is really dependent on the totality of the cybersecurity documentation submitted. So, we're making that as a full evaluation of the overall medical device system, the threats the device will be exposed to, the controls that have been implemented, and the effectiveness of those controls. So, it's looking at the overall cybersecurity documentation in its totality, similar to how FDA evaluates the reasonable assurance of

safety and effectiveness or impacts the safety and effectiveness from our established regulatory authorities in those areas.

CDR Kim Piermatteo: Thanks, Matt. And again, thank you, Mohammed, for that question.

So, thank you again. This wraps up our question and answer segment for today. We greatly appreciate your engagement and all of your questions. At this time, I'd like to turn it back over to Matt to provide his final thoughts for today. Matt?

Matt Hazelett: Sure. Thanks, Kim. We very much appreciate your attendance and participation in the great discussion. We really hope that you take away from this how FDA is proposing to address the cybersecurity authorities under Section 524B and how we're trying to integrate this into our review processes and try to build towards a least burdensome approach where feasible for the modifications to existing devices. Thank you. I'll turn it back to Kim.

CDR Kim Piermatteo: Thanks Matt for those final thoughts. And again, thank you so much for your presentation. As I mentioned earlier, printable slides of 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 also be posted to CDRH Learn under this same section and subsection in the next few weeks, and a screenshot of where you can find these webinar materials is provided on this slide as well.

If you have additional questions about today's topic, you may email the CDRH Digital Health Center of Excellence at digitalhealth@fda.hhs.gov. And if you have additional general questions about today's webinar, feel free to reach out to us in DICE at dice@fda.hhs.gov.

And lastly, we hope you're able to join us for a future CDRH webinar. You can find a listing of all of our upcoming CDRH events, including upcoming webinars, via the link provided on the bottom of this slide at www.fda.gov/cdrhevents.

Thank you all again for joining us. This concludes today's CDRH webinar. Have a great day.

****

END