Postmarket Management of Cybersecurity in Medical Devices Final Guidance
Moderator: Irene Aihie
January 12, 2017
1:00 pm ET

Coordinator: Welcome and thank you for standing by. At this time all participants are on listen-only mode. During the question and answer session press Star followed by the number 1. Today's conference is being recorded if you have any objections you may disconnect at this time. I'd now like to introduce Irene Aihie. Ma'am you may begin.

Irene Aihie: Hello and welcome to today's FDA Webinar. I am Irene Aihie at CDRH's Office of Communication and Education. On December 28, 2016 the FDA issued the final guidance document on post-market management of cyber security in medical devices. This guidance document is intended to inform industry of agencies recommendation for managing post-market cyber security vulnerability for marketed and distributed medical devices. The focus of today's Webinar is to share information and answer questions about the final guidance document.

Today's presenters are Dr. Suzanne Schwartz, Associate Director for Science and Strategic Partnership and Dr. Seth Carmody, Cyber Security Project Manager in the Office of the Senate Director here in CDRH. Following the presentation we will open the line for your questions related to topics in the final guidance. Additionally members of the cyber security team will be made available to assist with the Q&A portion of our Webinar. Now I give you Suzanne.

Dr. Suzanne Schwartz: Good afternoon and happy New Year everyone. Welcome to FDA's Webinar on the post-market management of cyber security in medical devices. My name is Suzanne Schwartz, I'm the Associate Director for Science and Strategic Partnerships at FDA's Center for Devices and Radiological Health. With me today is Dr. Seth Carmody our Center's Senior Program Manager for Medical Device Cyber Security. We are also joined by Dr. Dale Nordenberg of MDISS and Denise Anderson of the NH-ISAC who will contribute to this Webinar presentation by providing a high level overview of the Collaborative Vulnerability and Threat Information Sharing Function of the MDISS NH-ISAC Initiative.

December 28, 2016 FDA released its final guidance on the original draft by the same name that was issued last January. During today's Webinar we will address the changes to the draft that resulted from the responses we received during the public comment period. We will walk through the policy using examples and allow time at the end for Q&A. We want to take this opportunity to thank all of the stakeholders in the medical device ecosystem for their constructive and collective feedback which we believe further strengthens the framework and approach articulated.

Bottom line up front: addressing medical device cyber security means implementing a proactive comprehensive risk management program that incorporates these key tenets: applying the NIST framework to strengthen critical infrastructure cyber security, establishing and communicating processes for vulnerability intake and handling, adopting a coordinated disclosure policy and practice, deploying mitigations that address cyber security risk early and prior to exploitation and very important - engaging in collaborative information sharing for cyber vulnerabilities and threats.

For today’s Webinar we’ll begin by contextualizing medical device cyber security within the broader healthcare and public health sector of critical infrastructure. FDA’s approach is grounded in the total product lifecycle framework driving towards an ethos of continuous quality improvement. As a community, it’s essential that we maintain a holistic end to end view of medical device security from its initial stages of design through its use lifespan until it is obsolete. Anything less than that would misalign with the nature and the very landscape of security of the Internet of Things where vulnerabilities evolve and new threats emerge demanding continuous vigilance.

We will identify what has changed from draft to final. We will then go over key terms that are introduced into the guidance. Following that we’ll do a walk-through of the cyber security risk assessment explaining how FDA policy leverages the use of the Information Sharing and Analysis - - otherwise known as - - ISAO function, providing an overview of controlled and uncontrolled vulnerabilities with examples. Dale Nordenberg will then speak about the initiative that MDISS, working in partnership with NH-ISAC has stood up for medical device vulnerability and threat information sharing. And finally before we open up the Webinar for questions we’ll wrap up with key messages - the foundational elements that should be incorporated in a comprehensive medical device cyber security management program.

Healthcare and public health is one of the 16 sectors of critical infrastructure and represents a significant attack surface today for our nation. It’s considered to be a soft target. Intrusions and breaches occur through weaknesses in the system architecture. Healthcare delivery organizations are constantly fending off attempts at intrusion into their systems. These can be of varying motivations. Connected medical devices like all other computer systems are vulnerable to threats. And it's worth noting here that even if the device is not connected but it possesses software that device may be vulnerable.

Security vulnerabilities can directly impact medical devices or hospital network operations. And when medical device vulnerabilities are not addressed and remediated they can serve as points of entry into a hospital and healthcare network. This can lead to compromise of data confidentiality, integrity and availability. Worse yet, it can introduce safety concerns for the patients who rely on the safe and effective use of their devices whether in the hospital, at the bedside, at home or implanted.

Let's take a few moments to step back and contextualize FDA's policy and approach to medical device cyber security within the broader national architecture. In February 2013 the President issued Executive Order 13636. And I highlight for you a key statement from that order that in essence encapsulates the direction that our agency has taken: "We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cyber security information sharing and collaboratively develop and implement risk based standards."

For us at FDA this statement incorporates some very critical concepts worth underscoring: Partnerships of owners and operators; information sharing; collaboration; and implementation of risk based standards. Our approach has been one of fostering collaboration, engaging the many diverse stakeholders within this ecosystem, recognizing that we'll only make progress when the whole community takes ownership and responsibility harnessing all of our collective efforts to improve medical device and healthcare cyber security. It was this Executive Order in February 2013 that further directed the creation of the NIST framework for critical infrastructure cyber security with Department of Homeland Security charged with spearheading its adoption across all sectors of critical infrastructure.

To further deploy the concept of information sharing for cyber security another Executive Order was issued in February 2015. And that called for the establishment of Information Sharing and Analysis Organizations or ISAOs for short. Efforts have been ongoing across the US to further characterize what an ISAO would be, how it would work and what protection it would afford? With this background, FDA has taken a multipronged approach to medical device cyber security. In the broadest of strokes and as depicted on the slide it is characterized by three C’s: coordination with our federal partners; collaboration across both public and private sector with a targeted focus on stakeholder groups that are new to the healthcare space; and communication to the public at large through several mechanisms - safety communications, convening of public workshops and articulating our policy through written guidance as well as through outreach.

Our approach to medical device cyber security as I mentioned earlier is a total product lifecycle approach from the earliest of design and development stages out to obsolescence. Therefore in June 2013 we issued pre market guidance in draft, finalized in 2014. The key principles are: number one: shared responsibility between stakeholders; number two: address cyber security during the design and development of the medical device; and third: the importance of establishing design inputs for device related to cyber security. Because vulnerabilities will continue to evolve, premarket controls alone are not sufficient to manage cyber security of devices through their lifespan. We have therefore put forward policy for managing the cyber security of devices in distribution.

The key principles are: number one - use a risk-based framework to assure that risks to public health are addressed in a continual and timely fashion. Secondly, we articulate the manufacturer's responsibility by leveraging existing quality system regulation and FDA's post-market authorities; third - to continue to foster a collaborative and coordinated approach to information sharing and risk assessment; and fourth - to maintain that close alignment with the executive orders and this framework.

So what's changed from the draft to final guidance? The initially proposed 30 days remediation timeframe has now been expanded to include a 60 day tiered approach. To more closely align with current FDA recognized standards so that the community and the ecosystem at large are all using the same lexicon. Essential clinical performance is now safety and essential performance specifically scoped to patient harm. And you'll hear more about that in later slides. We received many questions about ISAOs the Information Sharing and Analysis Organizations. In the final guidance, we clarified the definition of active participation by providing specific criteria. And finally the scope of the guidance has been further clarified with respect to privacy as well as confidentiality harm. I'd like to turn this over now to Dr. Seth Carmody who will walk us through the meat of the guidance.

Dr. Seth Carmody: Thank you Suzanne. This is Seth Carmody. I'm the Senior Program Manager for Medical Devise Cybersecurity at the Center for Devices of Radiological Health. With the background provided by Dr. Suzanne Schwartz we are well-positioned to dig into the guidance policy. A key principles of the final guidance is cyber security risk management. The guidance provides a suggested risk-benefit framework and assessment methodology with which manufacturers can use to meet the regulatory obligations under 21 CFR 806.

The assessment methodology combines concepts from the FDA recognized standard ISO 14971 and the common vulnerability scoring system known as CVSS. Combining the concepts provided in ISAO 14971 and CVSS provides medical device manufacturers with a repeatable methodology for assessing risk of patient harm due to vulnerabilities within medical devices and accessories while ultimately providing a triage tool for the prioritization of remediation as well as cyber security routine updates and patches.

Now that we've introduced the key risk assessment methodology let's get acquainted with a few key terms. The terms safety and essential performance are derived from the FDA's definition of safety and the international electrotechnical commission's definition of a essential performance. The FDA's intent and use of the terms is twofold. One to align with current FDA regulatory jurisdiction and existing definitions and two to articulate when manufacturers should be concerned about the impact of a potential exploit on a device's functionality.

Utility of the term safety is to key medical device manufacturers in on the functionality of a device which must remain authentic, integral and available for a devices safe and effective operation and delivery of the intended use. To further clarify with respect to existing FDA recognized standard definitions and particularly IEC's use of the term basic safety FDA views basic safety as a subset of the FDA's definition of safety. The use of the term essential performance is in alignment with IDCs 60601 2012 definition of essential performance and is synonymous with the intent of the draft guidance introduction of the term essential clinical performance.

The utility of the term essential performance is to key medical device manufacturers in on the clinical functions of the device where loss or degradation due to an exploit would result in an unacceptable risk. The risks may be any number of business and organizational risks including loss or degradation that presents a risk of patient harm. The intent of the term safety and essential performance are not intended to be mutual exclusive. The idea is that some vulnerabilities may create the potential for the compromise of a device functionality such that safety is compromised directly while other vulnerabilities may affect functionality such that the compromise of safety is indirect and not readily apparent. Vulnerabilities that could potentially affect the essential performance may or may not compromise the device such that safety is compromised resulting in an unacceptable risk of patient harm. Manufacturers are responsible for defining the safety critical functionality and essential performance of the device.

Another key term in the final guidance is patient harm. The intent of the introduction of patient harm is twofold one to align with the existing FDA and FDA recognized standard definitions and two to appropriately scope vulnerabilities with a potential to affect the safety and essential performance to those that could impact patients only. As we'll discuss further the assessment of risk of patient harm is key to determining the appropriate actions by medical device manufacturers specifically when changes are made to reduce risk of patient harm. And we'll go into this in later slides however I wanted to introduce that changes to address uncontrolled risk of patient harm - are called remediation's and are considered corrections. Changes to the devices to address controlled risk of patient harm will be considered as cyber security routine update and catches.

The risk matrix that you see is a visual representation of the proposed risk matrix with exploitability on the Y-axis and severity of patient harm if exploited on the X axis. Together the assessment yields risk of patient harm. The manufacturer must assess whether the risk of patient harm is controlled or uncontrolled. With respect to the Y-axis exploitability the suggested approach is to use the Common Vulnerability Scoring System. We've proposed the use of CVS 3.0 however we've received feedback that organizations may also be using 2.0 or both. The guidance proposes suggestions of tools that are security centric so that manufacturers may adopt and adapt them for their use. And the FDA is supportive of the use of tools that facilitate the fulfillment of device manufacturer's regulatory obligations under 21 CFR 820.

CVSS is broken down into three main parts base scoring, temporal scoring and modified base scoring. Base scoring seeks to establish a quantitative and repeatable scoring based on characteristics of the vulnerability and its potential to impact confidentiality, integrity and availability. The base score does not take into account defenses or controls of an organization or a product. When monitoring resources such as the National Vulnerability Database maintained by NIST please note that the CVSS score base score may be the only information provided which necessitates the medical device manufacturer conduct further analysis including filling in the temporal score. The temporal score are risk factors the change over time such as the availability of exploit code and we recommend going to CVSS 3.0 to explore that topic further. And the modified – and moving to the modified base score the modified base score takes into account defenses or controls of an organization or product and should be assessed by the manufacturer.

With respect to the assessment of severity of patient harm on the X axis manufacturers should already have processes and experience for assessing the severity of impact of a device defect on patients. Shown here is a suggested approach from ISAO 14971. Generally speaking the severity of patient harm increases from minor, and temporary and inconsequential to requiring medical intervention as well as death. While this is a suggested approach to fulfill the risk assessment regulatory obligation the intent of the guidance is to align with current manufacturer processes. The terminology used by medical device manufacturers could be from already established risk assessment methodology.

Now we're going to turn to a key concept in the final guidance regarding Information Sharing and Analysis Organizations or ISAOs which I'll discuss briefly. We have the benefit of having Denise Anderson from the NH-ISAC and Dr. Dale Nordenberg from MDISS who'll be speaking to these concepts. Specifically, Information– analysis organizations are organizations that will serve ultimately to reduce risk by leveraging information from one organization to be used by another organization. While ISAC or Information Sharing and Analysis Centers have existed for some time Information Sharing and Analysis Centers have traditionally been sector specific. FDA has entered into a memorandum of understanding with NH-ISAC and MDISS.

In the final guidance the FDA has articulated the concepts of active participation in ISAO or where actions of a manufacturer that meets the intent of the post-market policy first and foremost is the emphasis on active participation. Active participation means that manufacturers have to share information and process shared information. FDA has purposely called on ISAO and manufacturers to share and process vulnerability and threat information as well as customer communications. FDA does not expect that this is the only information that is valuable to manufacturers in order to reduce risk and therefore FDA is not trying to limit the types of information shared. Manufacturers should participate in ISAOs that have defined governance structures such as participant agreements, business processes, and operating procedures and privacy protection such that a trusted environment is fostered.

Now to an important flow chart and representation of the assessment and various assessments and outcomes that can be described and are described in the post-market cyber security policy. First and foremost the risk of patient harm must be assessed. And you can see the box in the upper left-hand corner. As discussed in an earlier slide the FDA provided suggested framework and methodology based on the evaluation of exploitability into various patient harms that the vulnerability be exploited.

Walking through the flowchart directly down if there is no risk of patient harm changes to devices are considered cyber security routine updates and patches, and aligned with the current FDA guidance device enhancements versus recall. This is the same outcome for changes to device as you - if there is risk of patient harm but that harm is – that risk is deemed to be a controlled risk. When changes are made to the device to address a controlled risk of patient harm those changes are considered cyber security routine updates and patches again which is aligned with current FDA guidance, device enhancements versus recalls. In other words for there to be no risk of patient harm means that an exploit could not itself allow a threat avenue to compromise the safety and/or essential performance of the device. In some cases the assessment may determine that the vulnerability may present risk of patient harm but the risk is mitigated by the presence of controls such that the risk is reduced to an accessible level. In general the concept is, that whenever - if there is risk that it’s controlled.

And further articulation of the policy when the risk of patient harm is present and you can see on the top, and the uncontrolled arrow, changes to reduce uncontrolled risk of patient harm would be considered corrections and removals requiring adherence to 21 CFR 806. However if manufacturers can meet three criteria including, one there are no adverse events associated with a vulnerability, two, corrections and changes to a device that reduced the risk within the provided timeframe, these corrections, defined as remediations, must reduce the risk to an accessible level. Three it must meet the criteria for active participation in ISAO. If all three criteria are met than the reporting requirement under 806 would not be enforced. However manufacturers would be required to document the correction in their quality system, failure to correct a device when a vulnerability presents uncontrolled risk of patient harm could mean that the device is in violation of the act.

As stated in the previous slide in some cases the assessment may determine that the vulnerability may present risk of patient harm but that the risk of patient harm is mitigated by the presence of controls such as the risk is reduced to an acceptable level. The FDA has provided manufacturers with the opportunity to strengthen their cyber security through enhancements and a minimal oversight when risk of patient harm is controlled including reduced post-market and pre-market burden. For Class III devices FDA has asked manufacturers to provide cyber security changes as part of the annual reporting requirements.

As stated in previous slides when a risk of patient harm is present there are not controls or controls present do not adequately mitigate risk and reduce risk to an accessible level than the risk of patient harm is considered uncontrolled. Changes to reduce uncontrolled risk of patient harm would typically be considered corrections or removals requiring adherence to 21 CFR 806. You can meet the – if manufacturers can meet this criteria again including no adverse events, remediation of the vulnerability within the provided timeframe -- and we’ll speak to those timeframe specifically in subsequent slides -- and meet the criteria for active participation in an ISAO then the reporting requirements of 806 would not be enforced. Manufacturers would be required to document the changes in their quality system. And it bears repeating that failure to correct a device when vulnerabilities are present represents uncontrolled risk of patient harm could mean that the device is in violation of the act.

Having already discussed the criteria regarding adverse events and active participation in an ISAO I'd like to discuss the timeframe for mitigating risks including remediation. Recognizing that vulnerability assessments, risk assessments and validated remediation can take longer than 30 days the FDA expanded the timeframe to a 30 and 60 day tier. FDA's intent for keeping the 30 day timeframe is to encourage manufacturers to provide immediate risk reduction which could include communication to customers and users as well as compensating controls and most importantly develop a plan for further risk remediation.

They 60 day timeframe was provided to give manufacturers sufficient time to validate their mitigations which by definition includes more permanent risk reduction measures. These risk reduction measures must reduce the risk to an acceptable or controlled level. Within the 60 day timeframe remediation should be made available to customers and given a reasonable timeframe for the receipt and operationalization for the remediation. It is expected that manufacturers will be continually updating their products and therefore need robust patch management capabilities. And these capabilities should increase over time.

With regards to the customer communication the customer communication should at minimum describe the vulnerability including an impact assessment based on the manufacturer's current understanding state that manufacturer's efforts underway to address the risk of patient harm as expeditiously as possible, describe compensating controls if any and state that the manufacturer is working to fix the vulnerability or provide a defense in depth strategy to reduce the probability of exploit and/or severity of harm and will communicate regarding the availability of a fix in the future. FDA recognizes that not all vulnerabilities will be able to be completely remediated within the 60 day total timeframe. FDA hopes that the policy serves to initialize and optimize manufacturers patch management programs such that 60 day total timeframe can be met.

Moving on to guidance examples of controlled risks vulnerability identification control – steps that may lead - so walk through the controlled risk example I'd like to step through a couple of waypoints. First vulnerability identification then followed by vulnerability assessment and validation, impact analysis, risk determination and then manufacturer action. Secondly with vulnerability identification for example a researcher may publicly disclose an exploit called for a 4-year-old vulnerability in commercial off the shelf database software. The vulnerable version of the software is in a percentage of the manufacturers install base and in two separate product lines including multi-analyte chemistry analyzer.

In the assessment and validation process the manufacturer determines that the vulnerability is the result of a misconfigured database setting and could allow an unauthorized user to view patient health information in database. But the vulnerability does not permit the unauthorized user to edit or manipulate data in the database. Thus the manufacturer determines the vulnerability has acceptable and controlled risk of patient harm. And the manufacturer's actions they communicate and give appropriate mitigations in the communication. The manufacturer notifies its customers and the user community of the issue. Details the secure configuration setting and documents the effectiveness of the cyber security routine update for the configuration setting.

And an example in the guidance of uncontrolled risk we have a vulnerability known to the security community yet may be baked into a Class II device during development unbeknownst to the manufacturer. During the identification assessment and validation process in a post-market sense the manufacturer becomes aware of the vulnerability and determines the device continues to meet its specifications and that no device malfunction or patient injuries have been reported. There is no evidence that the identified vulnerability has been exploited.

It is determined that the vulnerability introduces a new failure mode to the device that impacts the essential performance. But despite that there’s no evidence in the field the manufacturer determines that the essential performance is impacted. The manufacturer determines that the device design controls do not adequately reduce the risk of the impact to essential performance and the risk of patient harm to an acceptable level therefore without additional mitigation the risk of patient harm is uncontrolled.

The actions followed by the manufacturer in communicating appropriate mitigations: Manufacturer does not have a fix immediately available to mitigate the vulnerability impact therefore within 30 days of learning of the vulnerability the manufacturer notifies its customers the ISAOs and user community of the cyber security risk and instructs them to disconnect the device from the hospital network to prevent unauthorized access to the device.

The company’s risk assessment concludes the risk of patient harm is now controlled with this additional mitigation. This connection of the device from the network is only a temporary measure not a viable long term solution and may introduce new risks in clinical workflows. Therefore the manufacturer distributes a patch within 60 days of learning of the vulnerability in order to provide a longer term solution. If the firm is an active participating member of the ISAO FDA does not intend to enforce compliance with the reporting requirements under 21 CFR part 806. And now it’s my pleasure to turn it over to Dr. Dale Nordenberg from MDISS and Denise Anderson from the NH-ISAC. Dale?

Dr. Dale Nordenberg: Thank you very much. Good afternoon everybody. On behalf of Denise Anderson from NH-ISAC the President of NH-ISAC and myself we would like very much to thank the FDA for the leadership that it has demonstrated as the stakeholders for medical device and safe medical device operations have come together to address this large public health challenge. In addition we've been for several years now working with other stakeholders including manufacturers, healthcare systems, technology companies and other government agencies. And it's been very impressive to see the community's active and deliberate response to this important public health challenge.

We would like to cover today just a couple of slides that will give a high level introduction to the Medical Device Information Sharing and Analysis Organization that will be operated by NH-ISAC and MDISS in a joint collaboration under the umbrella of the NH-ISAC which is the health care sector specific ISAO. The first slide that we will review is a system description of the vulnerability information sharing initiative for the support of the FDA guidance.

At a high level there are a couple of key aspects of the system that we're going to go over. Next week February 9, January 19 we will be doing an in-depth review of the Medical Device Information Sharing Analysis Organization function. And we will be posting the specifics for this Webinar on both the NH-ISAC and the MDISS Web sites.

So the purpose of this initiative is to have a medical device vulnerability information sharing system. It will be based on the 21 CFR 806 reporting. And the reason this is being done is to make the reporting process very familiar to manufacturers. We recognize that the idea of sharing cyber security related information is new as well as the notion of having a medical device

ISAO. So the premise was to try to create familiarity for both the process and the content.

The Web based system will be available through the nhisac.org Web site. The mission will be secure and via either an uploadable PDF file or an online form. The vulnerability will be shared by the manufacturer to the ISAO. If any other third party is interested in reporting a vulnerability, they will be referred to the manufacture so that the manufacturer can evaluate the vulnerability and determine the appropriateness of reporting to the ISAO. All vulnerability information that is being shared via ISAO will be - - the word we used on this slide deck is - - ‘embargoed’. And the idea here is that at launch of the ISAO we want to be very conservative about how that information is shared. And it will be shared with entities once the manufacturer has acknowledged that the sharing will occur, be that with the FDA, ICS-CERT or any other entity.

The next thing we’d like to review are some of the key attributes of the system. It’s important for all of us to recognize that this is a service. This is a service to the medical device stakeholder community. It’s a service that is designed to support the FDA guidance. And ultimately it’s a service to support the public’s health. It’s been collaboratively developed. There have been many manufacturers, healthcare systems, and again government agencies and other technology companies that have come together over well over a year to better understand what a vulnerability is, and how to define them, how to evaluate them and ultimately how to report them. We all recognize that this is a process that is constantly ongoing - undergoing evolution. And that there is a good deal of maturation that’s still required. And one of the key functions of the - of this initiative of the information sharing initiative is to also provide a venue for key stakeholders to continue to deliver required learning and to improve our best practices.

We already mentioned the facts that it’s been designed to be a familiar process. We will also work with other partners to ensure that there is more coordination and efficient coordination regarding the reporting of vulnerabilities. For example when reporting to the ISAO - there will be attempts to make sure that we can interface with ICS-CERT, and the FDA and other entities in a way that a manufacturer, if it desires, can leverage this initiative to simplify and streamline reporting across these entities.

The collecting and sharing of data is going to be based on public health best practices. This again is a large scale challenge public health challenge. Many healthcare systems many, many different kinds of devices, large exposure to patients so that we will be leveraging methodologies and practices that have been used for many other types of public health problems. Again we’ve already mentioned that this is a service that can be service driven. It will be based in scientific foundation and ultimately drive to have both - to ensure safety and privacy.

In addition to providing the service and support of the FDA guidance there are a couple of high level outcomes we also wanted to mention. Number one is to improve the understanding of vulnerabilities in medical devices. And number two is to improve stakeholder communities solution development around medical device vulnerabilities, three is to support the harmonization of best practices for medical device security information sharing and four is to improve the efficiency to market for medical devices while at the same time improving the security, safety and privacy profiles for medical devices and their associated networks.

So as has been mentioned the purpose of this short presentation was to give a high level introduction to the medical device and security stakeholder community. Denise Anderson and I look forward to having a Webinar next week January 19, details to be posted on our Web sites. We're very happy to have the FDA participate in this Webinar. And a number of the key elements of the information training analysis function will be presented by stakeholders in our community from manufacturers, health systems or other government agencies. Thanks very much.

Dr. Suzanne Schwartz: Thank you Dale. In summation we'd like to emphasize the core principles for implementation of a proactive comprehensive risk management program. Once more, to go through those: its application of the NIST framework to strengthen critical infrastructure cyber security; number two - establishing and communicating processes for vulnerability intake and handling; third - adoption of a coordinated disclosure policy and practice; fourth - to deploy mitigations that address the risks associated with cyber security vulnerabilities early and prior to exploitation therefor prior to harm, and finally to engage in collaborative information sharing for cyber vulnerabilities and threats. Thank you.

Irene Aihie: We'll now take questions.

Coordinator: And thank you. We will now begin the question and answer session. If you have a question please press Star followed by the number 1. Please unmute your line and record your name clearly as prompted. To withdraw the question it will be Star followed by the number 2. Again with questions please press Star followed by the number 1, one moment for the first question. Eric Decker your line is open. You may ask your question.

Eric Decker: Hello. Thank you. And thank you for this presentation. It was very helpful. My name is Eric Decker. I'm with the University of Chicago Medicine. In the…

Irene Aihie: Operator did we lose…

Coordinator: Yes. Eric Decker please press Star 1 again. We did happen to lose your line.

Irene Aihie: In the meantime can we go on to the next question?

Coordinator: Yes, one moment.

Irene Aihie: Thank you.

Coordinator: (James), your line is open.

(James): Thank you very much. ISAO is a centralized source of product system weaknesses would we agree with that? That said assuming the system is hacked these weaknesses will now be clearly identified providing hacker with at least some period of opportunity. The ISAO itsself then becomes a cyber security risk entity, any comments to that? Thank you.

Dr. Dale Nordenberg: Thank you very much for the question. This is Dale Nordenberg. The public health community has been collecting highly sensitive data and information for many years. And has strived to ensure the confidentiality, integrity and availability of that information if and when it should be shared and it should be shared only in appropriate instances. The NH-ISAC this – the ISAO will be hosting its data on the NH-ISAC infrastructure. That infrastructure has been evaluated from a security perspective in a very rigorous manner. It will continue to undergo that type of evaluation as part of its normal operating procedures. And that should help to safeguard the information that you are referring to. So we take this very seriously. And I'd like to give Denise Anderson an opportunity to also respond to this question.

Denise Anderson: Thank you Dale. Thank you for your question. Yes the ISACs themselves have been, you know, obviously have been full of information over the decades that they've been in existence and it's always been a – obviously a concern. But the ISAC have taken very good steps and NH-ISAC, you know, being one of the ISACs to protect the data that gets shared within their environment.

We also take really big steps in what we call the traffic light protocol system where everything is marked according to the originators desire as far as how they want the information to be shared. In most cases the information that comes through the ISACs are stripped of any kind of attribution and PII. So that's another further level of protection. And it may seem like it's shared outside of the ISAC it's also made anonymized. So we tried to do as much as possible to first of all protect the data but second of all to strip it with any and all attribution so that it is protected no matter whether or not it is distributed or accessible which to, you know, to date of course has not happened.

Irene Aihie: We'll take our next question.

Coordinator: All right, thank you. Our next question is from (Karen). Your line is open.

(Karen): Hi. I just have a couple of basic questions. So one is around timing for compliance, one is to ask you to repeat your Web site because I can't seem to find it. So maybe we start with those two.

Dr. Suzanne Schwartz: This is Suzanne Schwartz in FDA. Can you clarify which Web site you're asking about, an FDA Web site or the NH-ISAC?

(Karen): I thought it was the mdiss.nhisac.org.

Dr. Dale Nordenberg: Right. So that will become live at the time of the Webinar next week. And…

(Karen): Okay.

Dr. Dale Nordenberg: …any information about the Webinar and that site will be posted on the nhisac.org and the mdiss.org Web sites.

(Karen): Okay perfect. I can at least find the NH-ISAC Web site. And then timeline I understand the premarket piece would be, you know, if you had a submission or made a change that required a submission but with respect to the post-market a lot of this is new joining in ISAO et cetera. Is there a time line? Is it immediate? Can anyone speak from FDA around compliance dates for the post-market?

Dr. Suzanne Schwartz: This is Suzanne Schwartz. That's a great question. The post-market guidance is for implementation at present. We do recognize that there will be a learning curve associated with first of all, you know, joining with an ISAO and understanding the processes that are involved. But in terms of it going into effect with the release of the final guidance now being published you can assume that it is presently in effect.

(Karen): Okay.

Dr. Suzanne Schwartz: We – we're providing various email addresses that you can address any specific questions to as they arrive so that we can help our stakeholders with that process because we recognize there's going to be some fits and starts associated with it at the beginning.

(Karen): Perfect. I'm sorry one last question. And forgive me I haven't had a chance to really look at or speak with anyone about the ISAO organizations. Based on your combined experience like I'm in regulatory affairs, quality I have a scientific background but not a software background. My company is small. Recommendations for people that you think would be successful within a company, types of backgrounds for participating in that organization, thoughts on that?

Dr. Suzanne Schwartz: Participating in the ISAO organization…

(Karen): Yes.

Dr. Suzanne Schwartz: …is that what you're asking?

(Karen): Yes. Like who, you know, is there - I realize there's probably no requirements but were you to say the folks that are probably going to be the most knowledgeable with respect to understanding vocabulary and being able to be more effective participants what types of backgrounds? Are we looking towards our software engineers? I realize it's not a requirement again but just if you could give me some idea of the types of folks that might be most appropriate within an organization to be kind of that active participant within ISAO?

Dr. Dale Nordenberg: Thank you very much. This is Dale Nordenberg. And I'll ask Denise to see if she has any follow-up comments. The nature of your question exposes a challenge that we recognize across the entire industry which is cyber security and medical devices device functions and ultimately the evaluation of that function vis-à-vis patient harm is really a multidisciplinary capability or expertise. And many companies have been going through a process of standing up cyber security focused activities bringing people in with that particular expertise. They're bringing together activities that had historically been siloed: the software development, or device development R&D activities, with the cyber security or cyber security engineering activities and the regulatory activities. So it really depends on the specific company, how large your staff is and how it's organized.

So if for example you're a small company and without getting into the details about exactly what that means the expertise that would be required is a technical expertise, a cyber security expertise and regulatory expertise. And one of the things we would recommend is you should feel free to reach out to the NH-ISAC and actually explore becoming a member of the NH-ISAC, or a member of MDISS or other organizations that are already in the community and convening so that they can help organizations companies like yourselves understand how you need to mature, what types of expertise you need to develop and ultimately to help you answer your question.

(Karen): Great. Thank you guys very much. Appreciate it.

Coordinator: Thank you. Our next question is from (Doric Gund). Your lines open. (Doric) your line is open.

(Doric Gund): Hi. Can you hear me?

Dr. Suzanne Schwartz: Yes.

(Doric Gund): Can you hear me?

Dr. Suzanne Schwartz: Yes, we can hear you.

(Doric Gund): Thank you for letting me ask a question. So I have two questions. Question one what I hear from everyone is essentially having a mature security or information security practice including application and product security can address this guidance. Am I right?

Dr. Suzanne Schwartz: Can you repeat the question? I didn't hear it in its entirety?

(Doric Gund): Sure. Sorry about it. So if you have a mature information security practice that includes technical, physical and administrative controls including applications and products that capture every requirement from FDA guidance?

Dr. Seth Carmody: This is Seth Carmody. I do understand the question. I don't - I couldn't say totally without looking at your organization processes and outputs in terms of what the - a device or application might look like or testing. So it's hard to broadly say yes to your question. But I do understand it.

(Doric Gund): And I understand but thank you so much. The question was more at a high level for instance when this came up at the guidance on cyber security the gist of the matter is having a mature information security practice. And the reason I'm asking this question the lady who asked the question in terms of what type of a stakeholder should be involved essentially that is any stakeholder required to address information security right?

Dr. Suzanne Schwartz: The point that we're making here is that there's a lot of heterogeneity with regard to maturity in the healthcare public health sector and specific to medical devices. And we recognize that depending upon the size of the organization as well as again the degree of expertise within the organization in this particular area. So there is going to be variability organization to organization with regard to not only the maturation in this matter but also who would be the appropriate representatives of that organization interfacing with the ISAO function with a - being, you know, being a participant there.

And to some extent - - that's to a great extent - - that is going to be an organizational decision as to who is that appropriate or where does that appropriate expertise and representation desired within the entity? But as per the NIST framework which provides the type of architecture for maturation starting with an organization that is a lot less mature and moving now to more sophisticated organizations we realize and we apply the same principles with respect to the medical device industry also.

And that there is going to be different steps incrementally that different organizations are going to need to take. That's why a focus really being on a mantra of continuous quality improvement and continuous maturation. The idea of participating in an ISAO as well, is not merely about the vulnerability and threat information sharing that is obviously a key principle or emphasis of the guidance and what we're doing here, but there is a lot more to say about it from the standpoint of best practices and shared learnings by participating in a community in that matter. And that's perhaps something that Denise can speak to, Denise Anderson as the head of the NH-ISAC?

Denise Anderson: So thanks Suzanne. So the ISAC community is simply that - a community, a forum for sharing. And while we share information such as indicators of compromise like IP addresses and various other technical components we also share a number of best practices, mitigation strategies, ask questions of each other like hey are you seeing this in your environment or how do you handle this? So it truly is a group of people helping each other with the issues that they face on a daily basis so that, you know, everyone could be more effectively secure and doing the right thing.

(Doric Gund): Thanks for the information and the last part of the question if I may ask?

Irene Aihie: Go ahead.

(Doric Gund): Would the slides presentation slides be available? We had issues accessing that?

Dr. Suzanne Schwartz: Yes. They're currently available on CDRH Learn. So if you go to www.fda.gov/training/cdrhlearn it should be there now. And they're also on the Webinar Web page.

(Doric Gund): Thank you so much.

Dr. Suzanne Schwartz: You're welcome.

Coordinator: Thank you. Our next question is from (David Lerner). Your line is open. (David Lerner), your line is open.

(David Lerner): Yes. We're wondering about the applicability of this guidance to software that's not specific - specifically part of the medical device more along the lines of software that we use in the manufacturing of the medical device?

Irene Aihie: One second while we get that answer for you.

Dr. Suzanne Schwartz: Can you repeat the question? And we may need for you to elaborate a little bit further as well?

(David Lerner): Does this guidance apply to only the software that's part of the medical device or does it also apply to the software that we use for manufacturing or testing of the medical device during the manufacturing process?

Dr. Seth Camrody: No. This – if it applies to manufacturing software it does not apply. I would venture to say that the outcome or the output of a exploit in the manufacturing software would result in, what a manufacturing defect like a physical defect in the product. So no we didn't – that is out of scope.

Dr. Suzanne Schwartz: Also…

(David Lerner): Okay, thank you.

Dr. Suzanne Schwartz: …just to add Mr. Lerner, I don't know if you've had a chance to actually take a look at the guidance yet. We do address that on Page 8 of the guidance under scope where we call out specifically what the guidance applies to.

(David Lerner): Okay. Thank you very much.

Dr. Suzanne Schwartz: And if you have any further questions you can certainly direct them to askmedcyberworkshop@fda.hhs.gov for clarification purposes.

Coordinator: And thank you. Our next question is from (Eflant). Your line is open.

(Eflant): Hi. I'm not sure I understand exactly what it means when we disclose a vulnerability to an ISAC and then say you can disclose it to the ISAC community? I guess community is a bunch of joint members of the ISAC. But what if those members are somebody like Vladimir Putin Medical Devices Incorporated? How do you know that the members are acting in the interests of the group?

Denise Anderson: So I’ll take that one. This is Denise Anderson with National Health ISAC. We do take membership in the ISAC very seriously and we vet all of the people that join the organization. There’s a number of different processes that potential members have to go through such as signing appropriate paperwork and all of the vetting that we do. So we do take that membership very seriously. And the – also will be nuances in that the sharing through the ISAO sector will be a little bit more nuanced. So you don’t necessarily have to be an NH-ISAC member right now to be able to participate in the ISAO although obviously ideally ISAC membership would be important. The other thing -- and I don’t know Dale if you want to speak to this a little bit more -- that when something gets shared it’s going to be shared in a very nuanced fashion. And I don’t – I’ll turn it over to you if you want to comment a little bit further.

Dr. Dale Nordenberg: Sure. Thank you. As we all move forward into a – as yet to be experienced domain of reporting cyber security information and reporting it to an entity organization that is just being stood up to support this new final guidance the community of stakeholders is working very closely to understand how to do this in the most effective, productive and secure manner. And to ensure the if you will the safety of the manufactured that’s doing the reporting. So as we launch this activity as we launch this reporting capability as I mentioned it’s going to launch in a very conservative manner so we can all in a very studied manner understand how this works.

There are many entities that are potentially involved and interested in the data. That’s why the word embargoed was used, right? So that when the manufacturer supplies that information as we launch that information is not going anyplace until the manufacture and the ISAO has a discussion about what information goes where. And as we move forward after month one, month two, month three and as we continue to get significant input from the manufacturing community, its related associations and entities we’ll continue to evolve the way data is shared, what is shared, when it’s shared, to whom it’s shared, how is it protected, how is it secured as we move forward? So it’s a great question. It’s very important. And we’re looking forward to working with the community going forward.

((Crosstalk))

(Eflant): So even if we keep…

Dr. Suzanne Schwartz: Hi. This is Suzanne Schwartz from FDA as well. I will add FDA perspective to that in that the intent is never been to share actual exploit code or information that is highly technical around vulnerabilities or rather it will have a lot more to do with the kinds of communications in fact that a manufacturer would be issuing to its customers. So there is no intent towards providing information that’s highly sensitive that would provide a roadmap towards being able to take a vulnerability and use it in a malicious manner.

(Eflant): Do I also hear you saying though that even if we choose to keep a vulnerability embargoed that’s still considered active participation in the ISAC or ISAO?

Dr. Dale Nordenberg: So as I mentioned we’re using the word embargoed in quotation marks. And so what we’re saying is that the community has to understand how to use this information and when to share it. So the fact that it’s being shared with the ISAO is the first step. And then explicitly where it goes after that is going to be defined by the manufacturer. If the FDA says in order to be - in order to satisfy reporting to the ISAO, the FDA has to have access then it will be in the ISAO but you will if you don’t permit us to share it with the FDA then you will not have to field the criteria of reporting. So I’ll just, you know, hand this over to the FDA folks to say – to answer the very specific question about whether or not reporting to the ISAO but not giving FDA access to it would satisfy the requirements of reporting.

(Eflant): But could they also tell whether accesses fine grained enough that we can enable FDA access but not general membership access?

Dr. Dale Nordenberg: So yes that's absolutely the case.

Dr. Suzanne Schwartz: And the other point…

(Eflant): Okay.

Dr. Suzanne Schwartz: …that I would add is that as is the general process and procedure for reporting out of vulnerabilities for Department of Homeland Security ICS-CERT that function will continue. And at some stage ICS-CERT's involvement in coordinating that assessment and what's often an advisory would be integrated into this process as well. But as you probably know the ICS-CERT advisories also they do not contain information within them that would serve as a blueprint or as a roadmap for exploitation of a vulnerability.

(Eflant): Thank you.

Coordinator: Thank you. Next question is from (Elry Latang). Your line is open. I believe it's (Carter). Please unmute your line. Your line is open. (Carter)?

Irene Aihie: We'll take the next question please.

Coordinator: Our next question is from (Hei Mihn Young). Your line is open.

(Hei Mihn Young): Hi. My question is regarding the safety and essential performance requirements. From what was discussed in this Webinar that terminology is derived from 60601. For – my question is like for devices that are IVDs that may not need to comply to 60601 based on this cyber security guidance would the recommendation be to still have essential and safety performance defined so that we are able to make an accurate assessment for cyber security risks?

Dr. Seth Carmody: This is Seth Carmody. Yes excellent question. We fully recognize that in the scope of 60601 if they specifically exclude IVDs we're applying the concept to IVDs. So we're not excluding IVDs from the scope. Remember that safety and essential performance again is key and to clue in manufacturers to the risk, clinical risks that can manifest through the exploitation of avulnerability. So in IVDs that's still present it's just a terminology to help you frame your risk assessments. So if you are comfortable using it as a concept and terminology as an IVD manufacturer then we suggest that you use it. If you're comfortable using other terminology in your risk assessment feel free to do that whereas providing the risk assessment methodology and asking that if you don't use that you need to use something else.

(Hei Mihn Young): Thank you. And may I ask another unrelated question? It's regarding the relationship if there is any between exploitability and probability which, you know, probability is a terminology that's pretty familiar for those who are familiar with the ISO 14971 standard? So kind of just want to see if you can help provide some examples of what may be related or what may not be related?

Dr. Seth Carmody: Yes, again excellent question. So - and we did address this in the document. We know that and from 14971 explicitly states for software issues, defects and sabotage it is exceedingly difficult to calculate the probability of say exploitability. If you – and that you assume that the probability of exploit is one you assume failure. We recognize that. However we didn't think that was very helpful for manufacturers and other stakeholders to triage various vulnerabilities.

So again if you're comfortable as an organization and your risk appetite is sufficiently low or high will determine, you know, where you find uncontrolled and controlled level it's for you to set. So if you feel that you're not going to have good data or you don't feel comfortable around the parameters, characterization of the vulnerability and you feel like your risk appetite is low then you'll classify it as such. But we fully understand that calculating the probability is difficult but we did want to give people some parameters and characteristics that are used routinely in the security industry to assess vulnerability for triaging.

(Hei Mihn Young): Thank you.

Coordinator: Thank you. Our next question is from (Mike). Your line is open.

(Mike): Yes, thank you. Our group here has a question. Has the FDA been exposed to any medical device manufacturers who already implemented cyber security measures compliant to your standards and if so can you share some samples on that implementation like for example a medical software housed on a computer?

Dr. Seth Carmody: This is Seth Carmody again. I was with you right until you gave the example. Yes there are manufacturers that have adopted wholeheartedly the recommendations that have been put forth in the guidance. We do encourage collaboration so there are forums that you can belong to share that type of information. And actually I'm going to point to Dale Nordenberg and Denise

Anderson. That’s one of the functions of an ISAO is to share best practices. But that’s as far as I’m comfortable sharing.

(Mike): All right, thank you.

Coordinator: Thank you. Our next question is from (Wei Ping Zong). Your line is open.

(Wei Ping Zong): Hello.

Dr. Suzanne Schwartz: Yes.

(Wei Ping Zong): Hello. Can you hear me?

Dr. Dale Nordenberg: Yes.

Dr. Suzanne Schwartz: We can hear you.

(Wei Ping Zong): Okay. I have a question regarding the reporting 806 versus…

Dr. Suzanne Schwartz: We lost you?

Coordinator: (Wei Ping) if you can Star 1 again to ask your question. And we have (Matt Shaw), his line is open.

(Matt Shaw): Oh hi. This is (Matt) from (unintelligible). So actually my question is about cyber security I think similar to what (Mike) asked earlier the previous question. So we, you know, in general medical device industry the cyber security is applicable to many industries. Are we, you know, it’s good to have a community. Are we trying to, you know, a way to leverage people in the industry for example high tech, or even intelligence, you know, and part of government agency to - is there a plan involved to learn your - for those folks who joining us to help out our community?

Dr. Suzanne Schwartz: Unfortunately it was a bit difficult to understand your question. Might you please repeat it again?

(Matt Shaw): All right. So what I was asking is cyber security it’s applicable to not just medical device, you know, pretty much too all industries right now. And my question is, you know, it’s good for us to have a community we can share we can, you know, solve problems together. Is there a way for us to accept the members for example from different industries like high tech there are probably more mature solutions or even intelligence agency intelligence community?

Dr. Dale Nordenberg: This is Dale Nordenberg. I’ll take a first pass at the question and then maybe Denise Anderson can talk about the way the ISACs collaborate with each other across industries. So it is possible for example within our organization for other technology companies other than health - other than manufacturers or health systems themselves to join. And so we do have a number of general technology companies and security companies that are participating with us and we benefit from those perspectives.

There are a number of venues, workshops and other types of either symposia or conferences. And we - and there are a number of multi-industry kind of stakeholders that attend those for the kind of cross-fertilization of expertise and ideation that you’re referring to. NH-ISAC in fact has two conferences per year that includes not just medical devices but broad other types of expertise. So - and then from a government perspective we clearly benefit from that as well. So Denise, are you able to share some more detail?

Denise Anderson: Sure. I could talk to the collaboration across the ISAC. So we collaborate actually with the 21 ISACs that are members of the National Council of ISACs. And we collaborate with each other on a daily basis. So we work very closely with each other on – across the sectors including of course sectors that people that may not necessarily be part of the national health sector but are part of another ISAC such as the finance or the IT sector. So we are working very closely with all of our constituents across the ISAC communities and share information with each other very robustly.

(Matt Shaw): Okay, thank you.

Coordinator: Thank you. Our next question is from (Wei Ping Zong). Sir your line is open.

(Wei Ping Zong): Yes this is (Wei Ping). My question is about the 806 reporting and (unintelligible) share information of ISAO before and after 60 days. My question really is about original progress if I understand correctly for the 806 part (unintelligible) is for FDA to classify the records and impose it on the public for public information. And then the amended implications after that for instance if it's a Class I, FDA may come and audit a company inspect a company. So now with this criteria 60 days if it's reported to you (unintelligible). And then the FDA's other functions and disappears is that the intension for that?

Dr. Dale Nordenberg: So I don't think I understood quite bit - end of the question but I do think I understand the intent here so please correct me if I'm wrong. Reporting to the ISAO does not absolve the manufacturer from to - from giving that information and customer notifications. So it's not that the public or the customers won't know about the issue. It's not that it will go to the ISAO only it's going to your customers. And the intent of not enforcing the reporting requirement to FDA under 806 is that to facilitate the expediency of the fix.

So your customers know and that, that customer notification or field correction action letter you can focus on the fix as opposed to reporting to the FDA. Does that answer your question?

(Wei Ping Zong): I think I understand part of that. But for a recall if something is classified as a Class II or a Class I recall they are more than way more like just contacting the customers because you have to do a lot of follow-up actions for instance reconciliation. So the actions would be very different if - depending on the severity of harm you determine right? So you may have different actions there. So I just wonder what would be FDA's perspective if something just because one big difference one is for in the recall process the other one is not. What's the difference in there?

Dr. Suzanne Schwartz: So what I would say to you is that FDA takes into consideration multiple factors with regard to what subsequent activities or actions it might take. And I think what you asked at the beginning of the question was whether, you know, the idea of an audit or an inspection falls away as a result of using, you know, the ISAO function? And what I would say to you is obviously this is new, you know, this is new policy and it's evolving. But we're separating out any piece with regard to what might be down the road inspections or audits totally separate from the concept of really trying to get trying to move towards more expedient remediation's and fixes and updates to really strengthen the cyber security of devices in the post-market.

And so let's just put aside the recall or the classification of a recall at this time or what other actions might occur and let's focus primarily on what we're doing here which is trying to remove impediments that might otherwise slow down the process towards getting more secure devices that are in the field making sure that they are properly being, you know, monitored and addressed from a security standpoint so that the risk towards patient harm is reduced.

Dr. Seth Carmody: But I just wanted to add on there that the difference between the time is the time. The time - as time increases we feel that the risk increases that's why there's a temporal component to CVSS because we believe the overall risk increases with time therefore we've emphasized expediency and incentivized expediency.

Dr. Suzanne Schwartz: Yes. It doesn't - it isn't to say that inspections of firms won't occur. And, you know, over the course of that firms, you know, lifetime where cyber security will be audited as well. So that's a little outside the scope of this present guidance.

(Wei Ping Zong): Okay, thank you.

Coordinator: And thank you. Once again if there's further questions from the phone line to please press Star followed by the number 1. Please ensure to unmute your line and record your name clearly as prompted. Again if there's any further questions Star 1 from a touch-tone phone, one moment for the next question.

Dr. Suzanne Schwartz: Caller, are you there?

Coordinator: (Bob Brewer), your line is open. You may ask your question.

(Bob Brewer): Yes thank you. My question was around exploitability scoring. My take away from the presentation was that base and temporal scoring is essentially a requirement. And my uncertainty was on the third part which is environmental scoring. Is that a required portion to formulate the CVSS score? And the second part of the question is I wanted to know if what the schedule and timeframe potentially is for adapting the CVSS 3.0 to be more medical device friendly in terms of how it's – the definitions are put on?

Seth Carmody: Good questions. I'll address the second one first that, that is ongoing work within the community right now in terms of adapting CVSS to be more medical device centric and really drilling down to what confidentiality, integrity and availability requirements mean in terms of the device community. The first question that you asked I hesitate to call it a requirement. We've emphasized CVSS as a tool in order for you to assess risk.

What I'm saying of what we've tried to delineate in the guidance is that the base score and temporal score have parameters surrounding the vulnerability and the timeline of the vulnerability which will help you to assess the risk. So from a requirement standpoint I think it's a bit harsh but we do recommend that you do assess those parameters. The environmental or modify - the results in the modified base score is what you're defenses are. So you have the overall and aggregate risk and then assessment of the controls surrounding that device or device accessories. So in the requirement it's - I don't think that term fits. But in terms of assessing the entirety of your risk we recommend using CVSS in its entirety.

(Bob Brewer): Okay thank you. And which entity would be primarily responsible for adapting this CVSS 3.0 to the medical device domain further?

Dr. Suzanne Schwartz: And so FDA has been working with MITRE as a…

(Bob Brewer): Okay.

Dr. Suzanne Schwartz: …federally funded research center FFRDC tasked with this effort this initiative. And MITRE has convened a stakeholder group that has been working on the concept of translating or adapting the CVSS so it serves the medical device in a clinical environment.

(Bob Brewer): Okay thanks.

Dr. Suzanne Schwartz: If you would like further information about that again I'd recommend writing to us at askmedcyberworkshop@fda.hhs.gov.

(Bob Brewer): Okay. Thank you.

Coordinator: And thank you. Our last question comes from (Joanna). Ma'am your line is open.

(Joanna): Hi. Good afternoon. My question is in regards to the scope as the guidance applies for mobile medical applications. Can you talk to whether the scope applies to medical applications that fall under enforcement discretion?

Dr. Seth Carmody: Hi. This is Seth Carmody. I believe the mobile medical applications that fall under enforcement discretion are still classified as medical devices therefore those would be in scope.

(Joanna): Okay, thank you.

Dr. Seth Carmody: And we recommend that you apply cyber security principles to not only medical devices but other products you may have in your suite because it is a systems approach to secure these. Thank you.

Dr. Suzanne Schwartz: There is overlap with respect to taking a look at the guidance that we published on mobile medical apps as well. So I would recommend that you seek out that guidance for some further clarification. And also if there's additional questions please don't hesitate to write to us.

(Joanna): Thank you very much for your time.

Coordinator: And thank you. I would now like to turn the meeting back over to Irene Aihie. Ma'am you may go ahead.

Irene Aihie: Thank you. This is Irene Aihie. We appreciate your participation and thoughtful questions. Today's presentation and transcript will be made available on the CDRH Learn Web page at www.fda.gov/training/cdrhlearn by Monday, January 23. If you have additional questions about the final guidance document or were unable to ask your question today please use the contact information provided at the end of the slide presentation. As always we appreciate your feedback. Again thanks for participating. And this concludes today's Webinar.

Coordinator: And thank you for your participation. You may disconnect your lines at this time.

END