UNITED STATES OF AMERICA

DEPARTMENT OF HEALTH AND HUMAN SERVICES

FOOD AND DRUG ADMINISTRATION

+ + +

CENTER FOR DEVICES AND RADIOLOGICAL HEALTH

+ + +

PUBLIC WORKSHOP - CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES

+ + +

January 30, 2019
9:00 a.m.

FDA White Oak Campus
10903 New Hampshire Avenue
Building 31, Room 1503 (the Great Room)
Silver Spring, MD 20993

FDA:

SUZANNE B. SCHWARTZ, M.D., M.B.A.
Associate Director, Science and Strategic Partnerships
CDRH

AFTIN ROSS, M.S.E., Ph.D.
Senior Project Manager/Senior Science Health Advisor
Emergency Preparedness/Operations and Medical Countermeasures (EMCM)
CDRH

REID W. D'AMICO, Ph.D.
AIMBE Scholar
Office of the Center Director

Free State Reporting, Inc.
1378 Cape St. Claire Road
Annapolis, MD 21409
(410) 974-0947

PARTICIPANTS:

LAURA M. ALFREDO
Senior Vice President, Legal, Regulatory, and Professional Affairs and General Counsel
Greater New York Hospital Association

NINA ALLI
Biohacking Village Project Manager
DEF CON

DENISE ANDERSON, M.B.A., B.A., EMT, NIMS
President, H-ISAC
Information Sharing and Analysis Center

ROB BASTANI
Assistant Secretary for Preparedness and Response

DANIEL BEARD
Director, MedISAO
CTO, Promenade Software

SETH D. CARMODY, Ph.D.
Cybersecurity Program Manager
Office of the Center Director
FDA

PENNY CHASE, S.M.
Information Technology and Cybersecurity Integrator
The MITRE Corporation

STEVE CHRISTEY COLEY
Principal InfoSec Engineer
Trust and Assurance Cyber Tech Department
The MITRE Corporation

JULIE CHUA, PMP, CISSP
Risk Management Branch Chief
HHS Cybersecurity Program/HHS Office of Information Security/OCIO
U.S. Department of Health and Human Services (HHS)

JOE CODY, M.A.
Associate Director, Research and Innovation Policy
American College of Cardiology

JULIE CONNOLLY, CISSP
Principal Cybersecurity Engineer
The MITRE Corporation

JOSHUA CORMAN
Founder, I am the Cavalry
CSO for PTC

CHRISTIAN DAMEFF, M.D.
Clinical Informatics Fellow
Department of Emergency Medicine
University of California San Diego

ERIK DECKER
Chief Information Security & Privacy Officer
The University of Chicago Medicine

PHIL ENGLERT
Global Clinical Technology Leader
Cyber Risk/Denver
Deloitte & Touché

ANURA FERNANDO, M.S.E.
Chief Innovation Architect
Medical Systems Interoperability and Security
UL LLC

BRIAN J. FITZGERALD
Senior Technical Manager
FDA

ALLAN FRIEDMAN, Ph.D.
Director, Cybersecurity Initiatives
National Telecommunications and Information Administration (NTIA)
U.S. Department of Commerce

KEVIN FU, Ph.D.
Associate Professor
Archimedes Center for Medical Device Security at the University of Michigan
Chief Scientist
Virta Labs, Inc.

REBECCA GAGLIOSTRO, M.B.A., M.S., PMP
Director, Security, Reliability, and Resilience
Interstate Natural Gas Association of America

GREGORY T. GARCIA
Executive Director for Cybersecurity
Health Sector Coordinating Council

CHRISTOPHER GATES
Principal System Security Architect
Velentium

LISA GILBERT, CISSP
Cybersecurity Instructor
Air Force Cybersecurity Control Weapon System Forward Training Unit
Applied Research Solutions

PAMELA WINER GOLDBERG, M.B.A.
President/CEO
Medical Device Innovation Consortium (MDIC)

JULIAN M. GOLDMAN, M.D.
Medical Director, Partners Biomedical Engineering
Anesthesiologist
Director, Program on Medical Device Interoperability and Cybersecurity
Massachusetts General Hospital/Partners HealthCare System

JOHN GOMEZ
Chief Executive Officer
Sensato

MANU HAHTI
Stryker Corporation

TOM HARDY
Draeger Medical Systems

KEN HOYME, M.S.E.E.
Director, Product Security
Boston Scientific

JIM JACOBSON
Chief Product and Solution Security Officer
Siemens Healthineers

MICHELLE JUMP, M.S.
Vice President, Cyber Program Initiatives
Nova Leah, Ltd.

TARA LARSON, CISSP, HCISSP, CSSLP, CISM, CEH
Senior Principal Systems Engineer
Medtronic

ART MANION
Vulnerability Analysis Technical Manager
CERT Coordination Center
Software Engineering Institute

KEVIN McDONALD, B.S.N., MEPD, CISSP
Director of Clinical Information Security
Mayo Clinic

MICHAEL McNEIL
Global Product Security and Services Officer
Royal Philips

COLIN MORGAN, CISSP, CISM, GPEN
Director, Product Security and Services
Global Product Security and Services Program
Johnson & Johnson

MIKE NELSON
Vice President, IoT Security
DigiCert, Inc.

SCOTT T. NICHOLS, HCISPP, CHPSE, MCP
Director, Global Product Privacy and Security
Beckman Coulter/Danaher

JAY RADCLIFFE, CISSP
Cyber Security Researcher
Thermo Fisher Scientific

INHEL REKIK, M.S., B.S.
Director, Health Technology Security
MedStar Health

BILLY RIOS, M.B.A., M.S.
Co-Founder
QED Secure Solutions

DANA-MEGAN ROSSI, J.D.
Associate Director, Product Security Policy, Strategy and Incident Response
Becton, Dickinson and Company

ZACH ROTHSTEIN, J.D.
Vice President, Technology and Regulatory Affairs
AdvaMed

ALAIN SILK, Ph.D.
Acting Diabetes Diagnostic Devices Branch Chief
CDRH/FDA

GREG SINGLETON, M.S.
Director
Health Sector Cybersecurity Coordination Center (HC3)

ROB SUÁREZ
Director, Product Security
Becton, Dickinson and Company

NASTASSIA TAMARI
Senior Manager, Product Security Incident Response and Vulnerability Management
Becton, Dickinson and Company

MICHELLE TARVER, M.D., Ph.D.
Director, Patient Science and Engagement Program
Office of the Center Director
CDRH/FDA

JASON TUGMAN, CISSP, CRISC, CCSK, ITPM
Vice President, Cyber Risk Engineering
Axio Global

EUGENE VASSERMAN, Ph.D.
Associate Professor of Computer Science
Kansas State University

CHAD WATERS
Senior Cybersecurity Engineer
Health Devices Group
ECRI Institute

CHARLES WILSON
Senior Architect
Draeger Medical Systems

AXEL WIRTH, M.S., B.S.
Distinguished Technical Architect
Symantec

BEAU WOODS
Cyber Safety Advocate
I Am The Cavalry

ASHLEY S. WOYAK, CISM
Business Information Security Officer
IT Security & Risk Management
Baxter International, Inc.

MARGIE ZUK, M.S.
Senior Principal Cybersecurity Engineer
The MITRE Corporation

INDEX

M E E T I N G

(8:00 a.m.)

DR. CARMODY: Good morning, everybody. Welcome to the ad lib version of our show. The weather has helped us out a little bit. We're going to recap yesterday and I'm walking around the audience because I need your help in discussing the topics of yesterday. Is everybody okay with that? There's only -- hey, there's three microphones, all right. So I think we can get it done.

I had one really key takeaway for myself yesterday. There was a lot of discussion about how does -- we're talking premarket here, but also the sort of topics that commingled with postmarket and I just want to be clear that the impetus for revising the guidance was the things that we were seeing happening in the environment, so we're talking routine vulnerabilities that came through our door, we're talking about very public vulnerabilities that came through our door that you may have heard about. Talking WannaCry and NotPetya and other response activities that we all heard about.

And we saw fundamentally that at the design level we weren't giving ourselves the best shot at success so when we took a look at the premarket guidance, what we would do to revise that, how would we get at some of these problems at a design level. When the products were coming through our door and we were taking a look at them, what are the things that we could do to really give ourselves the best chance at success.

They can't see me online? Okay, all right. Where is the webcam?

UNIDENTIFIED SPEAKER: Over there.

DR. CARMODY: Can they see me now?

(Off microphone response.)

DR. CARMODY: Okay. You heard it, folks. Can I at least be here?

(Off microphone response.)

DR. CARMODY: Okay, great. All right. What?

(Off microphone comment.)

DR. CARMODY: Eugene, get your eyes checked. All right.

So I just want to make sure that everybody understands that the guidance really is to facilitate and lessen the pain points in the postmarket. Right? Is that clear? Any thoughts on that?

(Pause.)

DR. CARMODY: What?

(Off microphone comment.)

DR. CARMODY: I just went through a spiel about how the premarket guidance is designed to lessen the pain points in the postmarket, it doesn't solve every problem that healthcare and public health has, and asking for you to maybe possibly comment on that. Is that clear, is that not clear, is there something that you'd like to see changed about the guidance to address anything that we've left out? It's an open question, not to you specifically.

(Off microphone comment.)

DR. CARMODY: Got it.

(Off microphone comment.)

DR. CARMODY: What's that?

(Off microphone response.)

DR. CARMODY: Yeah, was anything left out? Did we forget something? While you're thinking about that, you can come to the microphone at any moment. Legacy was the first panel. The takeaway from this for me, interested to hear from other folks, was that we still have similar problems to 2014 and this is really frustrating. Anybody else feel the same frustration? Yeah. Okay, so we have a lot of work to do. I think, for me, in

personal reflection, that this is a big problem, a little bit too big for us to get our arms around at the moment, so I think the first steps to success are breaking the problem down into discrete chunks and then saying how are we going to go about solving it? Any thoughts on legacy? Oh, gentleman at the microphone.

MR. HAHTI: This is Manu Hahti (ph.) from Stryker. I think what I see is currently legacy is a problem because we make devices that are long-life cycle, right? So, yes, we had this problem in 2014, but products that we sold before 2014 are still in the market. So I think it's a good idea that the premarket guidance, especially the revision, is meant to help the postmarket pain but I think before we see the effect of it, it's going to be a few more years because we still have older devices were even before the 2014 guidance came out. So just my thought on that.

DR. CARMODY: Yeah, I agree, and I think Josh Corman mentioned this yesterday that at some point we'll start seeing the benefits of the policies that have been put out in 2014 and then the draft guidance, once it goes final, during that dwell time we'll have a bolus of devices that are what would meet a loose definition of legacy and what does that mean. So what I encourage -- what I ask folks to do is to think about, when you go back to your respective organizations, what does that one thing, the biggest impact thing that I can do, start doing today to start chipping away at the problem and then bring it up for conversation. And if you have an epiphany, I would like to hear about it. What is the first step to success? Go ahead.

MR. CORMAN: This came up a little bit last night. I think we just need more words because there's always going to be a delayed effect or legacy as a relative term, whereas I think what many people mean is pre-guidance or before we got to minimum viable defensibility or -- and it's mostly not so much for bringing new products to market because they're going to be conformed to the new guidance, it's more about how hospitals and

patients depend upon things that were developed prior to our new form of enlightenment. So instead of just legacy as a binary thing, I think we need a couple of different, like, eras of label that could let a hospital or a patient know that this device is something I'm going to want to get rid of if I can, sooner because it's pre-, you know, era, you know, modern era or whatever.

DR. CARMODY: Nicholas.

UNIDENTIFIED SPEAKER: Yes, I would like to think at what you have said over the -- what we have seen yesterday during the -- when we're trying to define what legacy is, is we have different opinion and different point of view on -- of legacy. At the same time, also, we need to consider the hospital and the manufacturer, how they use a legacy product. Before a hospital change a product, sometime they need funding or they need additional information, they may not one day decide okay, I'm going to change it. There's multiple effects on that. So we need to come with a good definition of what a legacy is and all to -- in terms of cybersecurity because we can define legacy into a product and cybersecurity may have a different type of definition on that one, needed to help the organization, the community to better use and manage this product.

DR. CARMODY: I think definitions would help us put it into buckets and then we can start to crack open those problems.

Go ahead.

MR. HARDY: My name is Tom Hardy, Draeger Medical Systems. I think I really appreciated the discussion yesterday that was brought by, I think, Mass General, I think, you know, the hospitals having such a narrow sort of margin of profitability. I think that's of concern to our customers, definitely. We have a fairly large install base out there that we struggle with, you know, supporting and maintaining. I liked the discussion about the life cycle and especially the -- you know, the consideration of risk, I think, in that definition of

legacy and definitely, you know, un-updateable -- I mean, our systems are updateable, but it's debatable whether we can ever update them to the full extent, you know, that they need to be, so we struggle with that, too. So we, you know -- I just wanted to say those are probably the most salient points that we saw yesterday.

MR. TUGMAN: I just have an observation and actually kind of gets to both of the points that Josh was just making and you were making. So as you guys know, I come from the energy sector and the finance sector and I'm reasonably new to the medical sector, specifically MDM, and just an observation that I have is I keep hearing the language of replace or get rid of or all that and my question would be is that a nonstarter and if so, the language -- I would propose that instead of saying replace, it's more about recognition of what a legacy device is.

The conversation yesterday was very helpful and I think very fruitful, but once the definition of legacy is determined, the guidance should, in my opinion, be potentially not about the life cycle of it but about the guidance for compensating controls and potentially reference architectures to deal with legacy devices rather than the guidance of I have 400 of these devices, I can't afford to get rid of them because of margins. So can we change the conversation into compensating controls, reference architecture, as opposed to this language of getting rid of?

DR. CARMODY: Thank you, Jason. I just want to clarify when I meant pain points, when I talked the guidance revision, I meant we went out and said okay, what were the problems -- are experiencing for end users, both hospitals and patients, right, and also manufacturers, too. We know there are key things to get out within our own organizations and we're trying to do that, as well, but we looked at how hospitals and operational environments were suffering and what we could do from the design aspect to mitigate some of those sufferings.

Julian.

DR. GOLDMAN: Good morning, Julian Goodman, Mass General Hospital.

I just wanted to put out on the table that when we think about risk, so there are two big buckets that we look at initially. One of them has to do with clinical risk, meaning risk to the patient or risk to delivery of clinical care or something in that area, and the other is risk to the rest of the ecosystem, so risk to the hospital network or backbone and so forth. And it's helpful to look at those separately in that legacy devices, you know, one of the problems they may introduce is not related, really, to the effectiveness or usability of that device for clinical care, but the risk to the rest of the system and then also the maintainability. So as we go forward, I would propose that we consider those buckets.

DR. CARMODY: Excellent. At the risk of not getting to anything else --

(Laughter.)

DR. CARMODY: -- this is a very fruitful conversation, I hate to end it, but we should wrap up.

MR. CORMAN: Just the last thing for me is FDA is regulating the devices, right, the devices we bring, and the other half of this more than two-person relationship is the hospitals, and I think part of my driver of using the word replace is we have had safety communications that have been ignored. I mean, my hospital still uses the Hospira bedside infusion pump that is hackable and un-remediateable, and they're not putting on a special VLAN, they're not doing anything different. It's been 3½ years since that safety communication.

So I don't mean replace all the things, but if we get to the level where FDA puts out guidance or action or takes a regulatory step or the manufacturer does a voluntary recall, this room is not the place to be regulated, it's the hospitals and insurers and JCAHO and whatnot, but the relationship between what FDA says about medical devices and how it's

heard by the HDOs and clinicians and patients should be very much clarified because I don't think we can make the argument of well, we have razor thin margins and continue to use, you know, a less safe device than market alternatives that have been developed in the modern era.

DR. CARMODY: And, Anura, you have the privilege of last legacy comment ever --

MR. FERNANDO: Thanks.

DR. CARMODY: -- for today.

MR. FERNANDO: I'll make it quick, too, so --

(Laughter.)

MR. FERNANDO: Anura Fernando from UL. So I just wanted to say real quickly, you know, we've been dealing with legacy software issues for over a decade now in the standards world with standards like IEC 6304 having been modified to deal with legacy software. So it may be beneficial to look at some of the standards and requirements there and practices that we have in place and just map those over to the world of security now, as well.

DR. CARMODY: Thanks, Anura.

Threat modeling. I personally enjoyed this panel, and I'm also probably significantly biased by being part of the panel, but a couple of things that we saw coming out of the notes, the breakout groups are here. I love the practicality that did come out of the panel, I love the idea of the whiteboard session, it's actually a theme that we use ourselves and just curious to think -- hear what people thought about threat modeling in general and if you're going to go back tomorrow, I think was the call, tomorrow, who's going to have a whiteboarding session about threat modeling. Anybody? Do you threat model every day, Josh? Okay, all right. Who doesn't, right? Go to the gym, threat model, get lunch.

(Off microphone comment.)

DR. CARMODY: Okay. Anybody have any thoughts on threat modeling? Oh, somebody -- oh, sorry. You didn't get a personal microphone delivery, I apologize.

MR. WILSON: Oh no, that's okay. I know the camera's there and it can't see me when I'm here. Charles Wilson, Draeger Medical. The way we actually do it is the thought that I had originally was yeah, do a whiteboard but I would always have leads and such going back to the desk and then going into their favorite applications whether that be PowerPoint or whatever have you.

And so I switched it to getting a huge role of craft paper and making them sit in a room without any other electronics and taking the physical device, putting it in the center of the craft paper and starting there with here's the device, here's all the outside of the device, let's talk about it and then speak to those particular things. And then at the end of the session, I didn't have to capture a whiteboard or deal with any of that, it's like here's your piece of craft paper and we've written your homework on here of things that you're supposed to have for the next session that we're going to talk about.

DR. CARMODY: Very cool. What is it about a giant piece of white paper or whiteboard that this is inspiring? I don't know, it's -- love the idea, thank you.

UNIDENTIFIED SPEAKER: So one of the things that I think I'm hearing from this is there's a lot of anxiety about threat modeling and threat assessment. One of the things I take my customers through is just there's six categories so it involves, like, patient safety, patient health, financial risk, privacy risk, and then the sixth one is something regulatory, it doesn't care about, which is risk to the reputation of the company. And then we look at each one of those on a scale of one to five of how serious they are. It doesn't have to be like this anxious thing that where, you know, it's nebulous. It is pretty straightforward if you take it device by device. If you're looking at a system as a whole, then it is -- it is hard to understand.

DR. CARMODY: Eugene.

DR. VASSERMAN: Okay, just a brief comment and a suggestion. The comment is actually exactly what was just stated, it's this is much harder to do with a system. So this is, again, I think from elevation of privilege or from a lot of other concepts of how you play with such analyses, you would draw that system on the board with as much detail as possible and then remove all the markers and then use that craft paper to study the system when you can't have a device.

If you are going to have a device that you put in the center of the table, include screwdrivers. We were just having a conversation about the combination of physical and electronic security and I think it's worthwhile to have some tools to see how reasonably you can play with something without seriously damaging it while keeping in mind the intended context of use.

DR. CARMODY: Julian.

DR. GOLDMAN: Julian Goldman again.

So when it comes to threat modeling, I'd like to emphasize that there are things that can be done in a generic way, at least speaking from an HDO perspective, identifying single points of failure of a system, plans for disaster recovery, so if something happens. But when it comes to something specific, for example, when there's a known vulnerability, a new vulnerability, it's extremely difficult, if not impossible, for this to be done independently of a manufacturer. And in our experience, we -- one approach we've used is to present the manufacturer with the scenarios that we've developed under threat modeling, kind of under urgent conditions, and asked if these were reasonable because we don't -- we can't be certain of what the impact of a vulnerability will be on a device or a system function. So I would like to raise the point and ask that we find ways to disseminate threat modeling scenarios from manufacturers when there's a specific vulnerability and

then it might be up to the users to determine whether those are viable, you know, potential threats in their own environments.

DR. CARMODY: Thanks, Julian.

Chris.

MR. GATES: Chris Gates, Velentium.

I've been doing threat modeling for clients for about 10 years now and one of the things I've come across is unstructured approaches such as whiteboarding, especially with an average development team, it only exposes very few vulnerabilities in a system and they go in with a false confidence. Whenever you introduce a structured approach such as STRIDE or anything that decomposes your proposed system into a list of potential vulnerabilities you pick up many, many more vulnerabilities.

There has never been a case over all of these clients that have done this that I haven't seen this to be true. Every time I've taught someone how to do this and they applied it on their own, it's also the same case over and over again. This is through some of the folks in here who, like Christoph from IEEE, there have been groups in there where they've applied this thing and it works. Every time they said we thought we knew all the vulnerabilities.

So first you decompose your system using a methodology that you can then assume you've got reasonable coverage because if you're doing it ad hoc you don't have coverage. How do you know when you're done when you're whiteboarding? Who's in the room? Is it a bunch of staff engineers that know nothing about security, are they all security SMEs? I highly doubt it. Even somebody like myself, I'll forget things, I'll miss things, I'll make holes if I do it that way. I want a methodology that ensures I get good coverage. Then when I'm done with this, something Brian Fitzgerald brought up yesterday on one of the panel meetings, of those potential vulnerabilities you need to apply a scoring rubric to them for

that use case. That scoring rubric identifies where there's issues, where you have to put your time and money and mitigation into these systems. Don't just go ad hoc because it will wind up with a really poor end result.

DR. CARMODY: Sure. So I'm hearing that there's a whiteboard portion if you're just getting used to it and then some conversion to maybe some tools and then I think Eugene mentioned formal methods.

Eugene. Anura, sorry.

MR. FERNANDO: Oh.

DR. CARMODY: You will not get the last comment. We're going to move on.

MR. FERNANDO: No problem.

DR. CARMODY: You can stay right there, though, because you're going to talk about risk assessment work.

MR. FERNANDO: Okay.

DR. CARMODY: A lot of discussion about the tier systems, conversations on the sidebar, wasn't a lot of discussion in the groups, I think that was an artifact of the setup for the breakout groups, but I'll sort of summarize what I've been hearing and that is that the tier systems are -- it's interpretable and that makes it difficult. I'll stop there.

What I will ask of you is submit formal comments to the docket. Remember that we're trying to get at a risk-based approach, right, so is there a different alternative risk-based solution and then -- and that goes hand in hand with least burdensome, meaning that if I do my threat model and I have something that doesn't need all of these things that we've outlined in the guidance, is it appropriate for you to do them, does that make sense? So it's not just enough for you to -- I appreciate getting back to, let's say, Tier 1, Tier 2, we're very confused by -- we're struggling with it. It's another thing to say here's what I propose the solution be and that's what we really need to hone this policy and get it tighter.

Anura, do you have any thoughts?

MR. FERNANDO: Thanks. Anura Fernando here again.

So this actually links very nicely with the comment I was going to make on the previous threat modeling discussion. When we look at the full breadth of different standards that medical device manufacturers have been using for a number of years now, IEC 60601, IEC 6304, 14971, 13485, and the list goes on, but manufacturers are very comfortable with these standards, they've used these standards, they have internal verification and validation processes that leverage these standards and these are the very standards that address the safety aspects that we've now integrated into security.

So when we start thinking about security related threat modeling and you know, running security related processes within our organizations, I think, as a previous commenter mentioned also, it's really important to look at this from a multidisciplinary perspective. If you think about, you know, EMC requirements, for example, electromagnetic compatibility, those are the same kinds of attack vectors we've seen with side channel attacks like EMI-based induction of pacemaker triggering, you know, those kinds of things.

So taking current practices for threat modeling and risk assessment and mapping those in with the security thinking and the fact that what used to be a natural phenomenon like EMI and like cosmic radiation that caused bit-flips in the software, there's now a forcing function which is malicious users, hackers that are trying to go after the product. So, again, going back to another comment from yesterday, you know, we can't think of this as easily from a probabilistic point of view; we have to think, you know, if this failure mode exists there's maybe a hundred percent likelihood that somebody's going to go after it. And so this threat modeling, risk assessment, all of these concepts really need to come together, I think, and link with safety.

DR. CARMODY: Agreed. Eugene, I'm going to ask you to pause, I got the hook, the 1-minute hook. We talked about trustworthiness and this was a subject of the breakout. I hear the take-home message is these will be available, I'm assuming. CBOM was -- we laid out all the things out here, all the paper that was generated, it was by far generating the most discussion. I'll summarize in a couple of ways. Hardware is going to be tough, but in general people agree that a software bill of materials is an element of transparency that's needed. And then I think the other thing was, I think some of the stuff that NTIA is trying to tackle right now, and that is breadth, depth, frequency, format, you know, some standardization.

And I'm going to stop right there, so I apologize, Eugene. This is the end of the session, but it's not the end of the discussion, so save what you were going to say and take it to the breakout groups, all right? Thank you, Eugene. And Michelle, sorry. Thank you.

DR. VASSERMAN: Fortunately, I have something that ties together with --

DR. CARMODY: Oh no, he's -- go ahead.

(Laughter.)

DR. CARMODY: You can't stop him, okay. Go ahead, Eugene.

DR. VASSERMAN: I'm sorry, I must have misunderstood. Okay, sorry. Two previous comments. It's very difficult to do probabilistic reasoning and therefore arguably it's difficult to do scoring, arguably. Perhaps ranking is better. What's the worst that could happen from each one and then rank them in the order of horrifying to meh and then fix from the top.

DR. ROSS: Thank you. And because we had CBOM up there last, we did want to give Allan an opportunity to make a brief announcement. Allan, are you in the room? Okay, maybe he's out. Oh, thank you. Come on into the room, you can make your announcement.

DR.. FRIEDMAN: Thank you, Aftin. So a number of you expressed interest in learning a bit more about what NTIA is doing around software bill of materials, so if you're interested, over lunch we're going to have a brief meet-up and happy to talk more. Hopefully, Jim Jacobson or Jennings will be able to join that conversation, as well, so you can learn what the healthcare concept working group is doing inside that initiative, but we'll give you some big pictures and tell you how you guys can participate, if you're interested. Thank you.

DR. ROSS: Okay, if we can now have our patient panelists come up. We're going to go ahead and get started with the program.

(Pause.)

DR. TARVER: Good morning. Thank you all for braving the frigid temperatures, and I guess, compared to other parts of the country, this is balmy.

I am Michelle Tarver. I'm the Director of Patient Science and Engagement here at the Center for Devices and Radiological Health, and today we're going to have a patient panel. But before we embark on that, I want to take a step back and really talk about what's at the center of everything we've been talking about and that's patients. Patients are baked into our mission, our values, they're also baked into what our programs are focusing on here at CDRH. In fact, our patient program is fostering innovation in the collection, analysis, and dissemination of information that can inform the patient/provider conversation, help our other stakeholders so that they can make an informed decision, such as our payers and other industry members as they design medical products, that they take those considerations into account.

The other thing that I'd like to also emphasize is that we've learned over time that patient perspectives are instrumental in helping us understand nuances of devices in ways that we may not have considered because they live with a device every day and they live

with the condition. And so today we have the pleasure of having this illustrious panel of patients and I'm going to ask that they start introducing themselves from my left.

MR. RADCLIFFE: Hi, my name is -- there we go. My name is Jay Radcliffe. I am a Type I diabetic. I am also a cybersecurity researcher. I'm kind of known for research that I published in 2011 on my own Medtronic insulin pump, finding wireless vulnerabilities in it, and also in 2016 the replacement pump for that, a Johnson & Johnson Animas pump, I found similar wireless vulnerabilities. And I currently work for Thermo Fisher Scientific in their product security division working on medical devices and helping to make them safer.

DR. D'AMICO: Good morning, everyone. I'm Reid D'Amico, and I'm a scholar with the American Institute of Medical and Biological Engineering and a member of the cybersecurity team here at CDRH. I am a patient with cystic fibrosis, also known as CF, which is a rare disease, and most notably, I use airway clearance medical devices.

MS. GILBERT: I'm Lisa Gilbert. I am not actually a patient, my daughter is. She has an implanted neurostimulator for chronic pancreatic pain. I am actually a cybersecurity instructor for the Air Force.

DR. SILK: My name is Alain Silk. I have Type I diabetes, I was diagnosed as an adult about 14 years ago. I'm also the Acting Branch Chief for diabetes diagnostic devices here at CDRH at FDA.

MR. NELSON: Good morning, my name is Mike Nelson. I'm a Type I diabetic, and I'm a father of a beautiful 4-year-old Type 1 diabetic as well. I work for a company called DigiCert, we work with a lot of manufacturers to provide authentication encryption and integrity. It's great to be here.

DR. TARVER: All right, so I'm going to stand up just because I cannot see to the side of the podium. So I want to start off the question with do you all think about the cybersecurity of your devices, those of you that have them or have a child or a spouse or

someone you care for that has a device? Do you all think about it? So we're starting very broadly.

MR. RADCLIFFE: I mean, I certainly think about it all the time. You know, I've got something that attaches to my side that takes my blood sugar readings and transmits them up to the cloud every 5 minutes and displays them on my iPhone. So I think that I'm always very aware and connected to the status of my body and what the technology -- kind of how that technology works.

MR. NELSON: I would say that the panel up here is probably unique in terms of do we think about it or not. I think most in this room, if you have a loved one who is using a connected device, device security probably crosses your mind. I would guess, for the average American, when they go in -- I mean, when my daughter was diagnosed with Type I diabetes and I see her get hooked up to an infusion pump that I know has had vulnerabilities in the past, I have a unique view of it

But I don't think most American -- most patients think that way and I don't think that they should. I think they should be concerned for the well-being of their life and there should be an assumption of safety and that the responsibility falls on those of us in this room to help provide that assumption of safety so that when you go in you can be focused on what is most important, which is the safety and the well-being of the patient.

DR. SILK: Yeah, you know, I have to say before I came to FDA this is not something that ever crossed my mind as a patient. I took it for granted that my devices were secure, I acted as if they were secure, and as I think about how I behave on a day-to-day basis today, even coming from here and being part of this conversation, I still act that way. I assume that my device is secure. That's how I behave and that's my expectation.

DR. D'AMICO: So I started here at CDRH on October 1st, and that's when I first started thinking about the cybersecurity of my medical devices, and I come from a

background where I actually used to instruct students on how to actually build the hardware for medical devices, so it's something that wasn't really in my thought process at all. And so just to go through a little bit of what my experience was like getting a medical device that I got 2 months ago, talked to my nurse, she told me oh yeah, cool, you can get this device, talk to the doctor, talk to the social worker, an at-home nurse came to fit the device and no one ever told me about the cybersecurity concerns that might come with it and instead they saw the Bluetooth capabilities as, you know, a bell and whistle, like oh, you now can control this from your phone by -- you know, since I started here at CDRH I've even called the company and said, oh, so do you all update this thing, and they say, no, we have no plans to update it. It's mostly so you can have an ease of use with your device.

MS. GILBERT: I certainly talked to my daughter's surgeon before her device was implanted and as other panelists have said, we assume they're not going to implant a device that isn't secure. Coming from a cyber background, I did ask questions and our surgeon said well, there's patient information in the device but -- and they could probably access it but there was no other discussion of actual safety type security and I think that's something that really has been lacking in the industry.

DR. TARVER: So I think you all touched on the fact that we assume trustworthiness, we assume safety of the device, but as we learn of more threats, since we learn of more vulnerabilities, how do you think the patient/provider conversation should evolve? As you mentioned, you mentioned it to your healthcare provider. How quick was your healthcare provider to answer those questions and how can we, as a community, help equip healthcare providers to be prepared for those kinds of conversations?

MS. GILBERT: I think one concern I have is when we're talking to our healthcare providers, our daughter's surgeon is the best neurosurgeon in the world for this particular surgery and I don't expect him to be an IT person. I think there needs to be that person

who does understand the technology, does understand security, and I don't know that those people exist at this point. The monitoring service, I think, would be a -- probably in our case, the people who should understand the IT and the security of the device.

MR. NELSON: Yeah, it's funny. I started asking my physician, as I was connecting my daughter to a CGM, continuous glucose monitor, questions about the technical capabilities, updateability, and my doctor was like you think I know that stuff? You know what I mean, you can't expect a trained physician to have the technical background to be able to talk to you about the security, but what I was impressed by, and I think it's a good practice, is he actually had a technician in his office that was there to help with technical difficulty, so if patients had questions -- so as I started asking questions, he said you need to talk to Matt, you need to set up an appointment with Matt and then if he can't answer your question, he'll direct you to the manufacturer.

And so, you know, I sat down with Matt and it was -- it was actually a really good experience. I was trying to decide between infusion pumps and he was -- I was kind of surprised when he said well, this one is updateable and the manufacturer sells -- one of its marketing pieces is the fact that they provide regular updates to it and I was like, yeah, well, you know, that's a step forward. And so, you know, I hope we'll start seeing more and more of that, but to expect a provider to be able to get into the technical details and explain the security posture of a device just is not -- I don't think it's practical and I don't think we should expect doctors to be doing that.

DR. TARVER: As a healthcare provider, I second that. Anybody else want to make a comment?

MR. RADCLIFFE: Yeah, I think that what we're going to have to do as a security community and people that are aware of that security is kind of reach out into the other arenas. You know, I was fortunate enough to be invited to go to the cybersecurity summit

at the University of Arizona in December where they had medical simulations with doctors, and this was a medical school, simulating what problems might occur with highly technical devices. And that's the kind of outreach that we're going to need. We might not need doctors, nurses, medical practitioners to be security experts, but they need to be aware that there are security issues so they start that thought process. And maybe that means we need to start publishing in things like medical journals, we need to go to medical conferences and not just to security conferences and kind of that kind of outreach, I think, is going to help with that patient discussion and educating practitioners.

DR. D'AMICO: Yeah, I agree with all of that and then one thing that I would like to say is, so when I go to the clinic, you know, I see a dietician, I see a social worker, I see a nurse, I see my actual physician, and I see a physical therapist. There's no reason why a certain cyberware technician couldn't also be part of that group, you know. So there are ways to integrate people who are going to be cyber aware without having to reeducate the entire clinician community.

DR. TARVER: So I think you all have mentioned an evolution of a care paradigm, essentially that it will no longer be the standard paradigm that we typically have interfaced with but maybe there should be some expansion with new roles being defined.

One of the points I think you -- Mike, I think you brought up, which was the ability -- and I think Reid, you also brought it up -- the ability to opt for certain options that may make you more or less vulnerable to cyber threats. So I wanted to talk a little bit more about that. Did that impact any of your decisions about which device you would choose? Would you have made a decision to use an older model that may have been less vulnerable to a cyber threat or would you want the state-of-the-art model that has certain capabilities? So I'd just like to open that up and whether or not that should be part of a provider/patient conversation.

DR. D'AMICO: I know one thing for me where I might stand out is that, you know, I have a rare disease so I usually don't have options to shop around for different medical devices, so usually I only have this one choice. So if it's not cyber safe, I really don't have any other option and if I'm not able to get that device or if something happens to it, you know, I'm kind of camping out at Johns Hopkins until I can get a new one that is more secure. So in rare disease, you know, we're all kind of patients here, but different disease groups are going to have different needs and have different amounts of shopping they can do.

MS. GILBERT: We were kind of in the same boat when our daughter was under discussion of getting the neurostimulator. Her surgeon only used one kind and he had recently changed to a new kind from an older model that he felt was better, but I don't believe that that had any security implications of betterness, just he thought it performed better, so like Reid, we didn't have any options. If we were given options, certainly the security implications would've played a role in our decision.

MR. NELSON: You know, as a consumer, I make decisions based on function and convenience and the way it improves my ability to manage my disease. So as I look at connectivity, connectivity brings so many enhancements in the way that, as a diabetic, I've been diabetic since I was 16 and when I was diagnosed I had to wait 45 seconds for a blood sugar reading and I had to wait 45 minutes for my insulin to kick in and now I get a glucose reading every 5 minutes to my phone automatically without me having to do anything.

I can sit here and I can look at my daughter's blood sugar from my phone here, so when she's at school, I'll get an alert if she's high or if she's low. I mean, those types of conveniences is what drives purchasing behavior for me. Those types of conveniences also present cyber risks, right, because of the connectivity and so I'm going to make a decision not based on the cybersecurity posture but based on the features of that device but, as a

security expert, I also realize that there is risk with that. I don't think most consumers, again, think that. They think bells and whistles, this is really cool, I want those features as part of my management because it will help me to be healthier, it will help me to be able to manage my disease better. And so I believe those types of features are going to be coming in all types of medical devices. And so as those come, again, I said it earlier, the responsibility to do it the right way, to build those devices in a way to make sure that those connections are authenticated, to make sure that the data is treated sensitively, right, and to make sure that there's integrity with the things that you're doing is critical. And so, you know, I'm not going to make a decision based on the security of it because I'm going to assume that if my doctor is telling me I can use it, it's safe.

DR. SILK: Yeah, I agree with what Mike said about the way that I would choose a device because there's options available to me. I mean, it's so hard to gauge the security risk as a patient, that that doesn't even really factor into the equation. There's so many other elements of my care that I'm looking to manage through the different features of these devices that that's really what weighs heavily in my mind and that's what influences my decision. I mean, partly it's an awareness issue that I'm not fully aware of the risks, it's hard to communicate those. And if I was, it's hard to know, you know, how would I gauge those because we just -- as we just heard, you know, probabilities and the extent of the risk can be difficult to understand and for a patient it's kind of -- can be very difficult to understand.

MR. RADCLIFFE: And, ultimately, I think the reality for most patients is they don't have a decision. Their doctor or their insurance company is making that decision. We only support Brand X, you will get a Brand X and if you don't, you might die. And there's not a decision there. Yes, there are some cybersecurity risks, but ultimately they're very low relative to surviving the disease or the treatment that you need to get. So there really isn't

a ton of a decision-making process in -- for most patients when it comes to that.

DR. TARVER: So to that end, does it -- should this be part of the dialog that patients and providers have or does it just create unnecessary anxiety that's unmitigateable? So I'm curious as to what you all think about --

MR. RADCLIFFE: Well, I have a strong kind of opinion on that. When I published the research in 2016 on the Animas insulin pump, I specifically went out of my way to say if my child was diagnosed with Type I diabetes today and they had to go on this insulin pump, I would be comfortable with that. Even with the vulnerabilities that were in that device, even though that some of those vulnerabilities were not solvable, I would still feel comfortable because I feel like that device gave good treatment and was a good option for that, because I think that that's a very important thing.

But I think that the focus of the decision making needs to be more making sure that we can, through the FDA process, through educating doctors, through educating HDOs so they're making good decisions for their patients, so we can get kind of upstream of that so patients can have that sense of if my doctor says this is safe, then it is safe.

DR. SILK: Yeah, I agree with Jay. I think all this should be happening upstream of patients and ideally this wouldn't even have to enter into the conversation because any patient with any device could just safely make that assumption that if they're getting this, it is secure and it is safe for them to use.

DR. TARVER: What about home use devices? We've talked about security patches being available and patients sometimes would be the critical component to download those safety security patches and other things. How, then, should we better initiate a conversation with patients? We've talked about labeling is one way of communicating but often labeling is designed for providers, not necessarily for patients. So how can we better empower patients? With the movement of a lot of devices into the home setting, how can

we better inform them and what process should we go through to develop that messaging?

MR. RADCLIFFE: I actually think that's pretty easy, from a patient perspective, like, I use a Dexcom CGM and it updates all the time and there are software updates and it's just like it is on your cell phone, oop, there's an update, press the update button and it applies the update. Like, I think that patients understand that mentality, they know that there are devices, technology needs updates, that's just a reality now.

DR. TARVER: Could I pause on that, just --

MR. RADCLIFFE: So I think that that's --

DR. TARVER: I'm sorry.

MR. RADCLIFFE: Yeah.

DR. TARVER: I didn't mean to interrupt you. Just to pause on that. There's also a lot of consumers who are concerned about updates because their phone doesn't work anymore when they do the update, so there are people who will not do the updates. And so how can we better engage in that conversation with patients, understanding that yes, we're familiar with that concept but people have certain inhibitions and anxiety and other concerns around doing updates.

MR. RADCLIFFE: That's true. I don't know.

MR. NELSON: Yeah, I kind of align with Jay on this, that as consumers -- I mean, let's face it, all of us have to get used to updates because if you have a smartphone or -- it happens all the time without us even knowing and so we have to create it in a way that is seamless and can be trusted and again, there's an assumption of safety. If knowing well, if this is coming, it's been tested, it's been cleared, they've done -- you know, they've made sure that this isn't going to break my device. And if you start releasing patches and that doesn't happen, then there will be a breach of trust and there might be some timidity with, you know, applying the patches. But I think, in this day and age, and I grant I can't speak for

all demographics, but I think updating, we talk about it here like it's this really, really scary thing for patients and I think it's more scary in the hospital setting for HDOs, but as a patient and consumer I'm not worried if Dexcom updates my app because I haven't had any issue with it.

DR. TARVER: I think you've highlighted the importance of messaging around whatever modifications are being made to those devices. One other question that we have is if there is a threat, and this is a question that we got from one of our participants, if there is a threat, would the -- would you all prefer to get the information about the threat before there is a solution, at the time of the threat when the company is aware of it, or would you prefer to get it once there is a solution available?

DR. D'AMICO: I'd prefer to get it before a solution is available because that might inform what I'm doing with my life before a solution does become available. So for instance, I might decide not to travel, I will probably always make sure that I'm near a clinic that can take care of me in case I do lose the ability to use my device, so I'd like to prepare as much as possible.

MR. RADCLIFFE: I think there's a lot of variables in that equation as far as, you know, what the impact is of given vulnerability, how long it is between the distance of disclosing the vulnerability and when it was reported. You know, I don't need to know about it right away if takes, like -- I'll give you an example. With the Animas insulin pump, you know, it was 9 months between the time I reported it and the time that it went public and it went public with information regarding what you should do if you feel like you're worried about that issue. And I think that consumers and patients, if you tell them hey, there's a problem but we don't have a solution, I think that you're just going to get them more worked up, especially if the risk is very low.

MR. NELSON: You know, yeah, I think I agree with Jay. It depends on the

vulnerability. If it's impacting the integrity of the data, so if my daughter's blood sugar reading is coming in and it's telling me it's 400 and her blood sugar is a hundred and I misdose her, yeah, I'd like to know about that vulnerability, that data can be compromised so that I can adjust the way that I manage the disease. So I think it depends on what the vulnerability is.

DR. SILK: And then, obviously, I think it depends on what the device is being used to manage. I mean, in some cases there's very easy choices. If it's a serious vulnerability with an insulin pump, you can just disconnect from that and use a manual insulin delivery to manage. With other conditions you may not have a choice or may not -- it may require surgical intervention to remove the device or -- I mean, that would -- that complicates things.

DR. TARVER: All right. And I think we're drawing close to the end of time, so I'll take some questions from the floor or comments from the floor.

UNIDENTIFIED SPEAKER: Thank you all for being here. One thing, as device manufacturers, we're always thinking about is onboarding the patient. Can you tell us a little bit about what worked with the devices that you've used in terms of information you were provided at the beginning of your -- you know, using your medical device, in terms of cybersecurity and if there wasn't much, then what would you see manufacturers provide? One thing to note is many or all of you are very well aware of the issue of cybersecurity but not all users are, so it's a difficult balance, but how should that information come about? What would make you feel sort of not TMI, not too much information, but enough information that you can manage your device in your day-to-day lives?

MR. RADCLIFFE: I think less is more. I really don't know if you can educate the consumer all that much about it. I mean, getting a medical device is such an overwhelming medical thing that adding the, oh, by the way, there's going to be personal data and it's not

going to be encrypted and we don't do updates, it's just going to make things worse for a patient. I think that those decisions get made upstream and I think it's more you need -- the medical device manufacturers need to educate the doctors and the HDOs that are making the decisions and by proxy the patients will feel safe because the doctor feels safe with using the product.

MS. GILBERT: I think in our case, we did not get any information as far as the cybersecurity of our daughter's device. Even though I asked the questions, the technician simply didn't know and it wouldn't have kept -- certainly didn't keep us from having the device because it has improved her quality of life dramatically. It's not necessarily a lifesaving device, per se, like the folks who have insulin pumps or say a pacemaker but certainly, the improvement in her quality of life made it worthwhile. But the technological information was pretty slim. I think if you're going to give technical information in regards to cybersecurity, I would couch it in reassuring terms that we're doing these things to keep your information and your device safe for you rather than being alarmist, certainly.

UNIDENTIFIED SPEAKER: Thank you.

DR. TARVER: Next question or comment.

MR. TUGMAN: So first of all thank you, everybody, for sharing your stories, so thank you for that. Each of your devices have different kinds of security needs and so I'm just curious, for each of you and the devices that you're using, you know, we all know the CIA conversation we were having last night and about the energy grid. We also used the word reliance, right -- so, Beau, you were right on that, by the way. So confidentiality, integrity, and availability and/or reliance. So for each device, like you had mentioned integrity, so can you identify, kind of, for your device what that is -- which one of those would be most important to you specific to the device that you have? And the comment that I would make to that is, you know, Mike, you also said that nobody's kind of touched on it, that you each

have kind of a risk tolerance and so you can risk-accept a lot of that but, unfortunately, we are in a risk ignorance world so we can't be risk aware, so therefore we can't accept it even though we have a tolerance for it, right? And so for the device, I was just curious, if everybody could just say I'm concerned about, you know, confidentiality, integrity, availability or if you want to infer reliance, please. Thank you.

MR. NELSON: It's an easy one for me. It's integrity, because you use the data to make treatment decisions and if you don't have integrity with the data in those readings, then that can be catastrophic.

DR. SILK: Yeah, yeah, I would support that. I think, you know, availability of the information is also pretty critical because that I directly use as well.

MS. GILBERT: With a neurostimulator there's not a lot of information flow but, for our daughter, certainly we're concerned most about availability. Confidentiality, integrity not playing nearly as big a part of the solution.

DR. D'AMICO: I'm probably more concerned about confidentiality, so I didn't know that my device was actually kind of beaming to some other party and sharing my data and I was worried that insurers would get access to it. So if they can think I was being -- adhering enough to my device they could take it away from me, which I know that's not exactly kind of in the realm of cybersecurity, but I do like to know where is my data going.

MR. RADCLIFFE: I think for me, it would be data integrity for my personal device decisions, but I think for a majority of patients it would be availability because availability generally tends to be the most focused on in medical environments because if that device is not available or its denial of service and somebody has a heart condition, they die, so availability would be king in most scenarios.

MS. LARSON: Hi.

DR. TARVER: Next question.

MS. LARSON: It is on? Okay. Hi, thanks for your time. I really appreciate your perspective and hearing from you as patients, I appreciate you sharing that. My question is you are all very technical and obviously well versed in how your devices work, how your conditions are managed, but how would you suggest informing someone who's not as technically advanced? As a former caregiver for a person with diabetes, any time an alert came on on the integrity of her data or something, she would call me and I understand that burden on people, also, so I was kind of just looking for your feedback on how would you share that information with less technical people?

MR. RADCLIFFE: Yeah, that's something I gave a ton of thought to. When I disclosed in 2011, I was overwhelmed with email questions from parents about should I wrap my kid's insulin pump in aluminum foil, should I take them off their insulin pump, what do I do? In 2016 I made a point to put something in the disclosure statement to parents, to people that were not technologically informed, which was to say yes, this is a risk; no, you should not take your child, your patient, off of this device. You need to be aware of these risks but it is not -- you know, learning how to understand that risk was a very important thing to me because I recognized that in the first go-around.

MS. LARSON: Thank you.

DR. TARVER: Yes.

MR. WIRTH: Okay. Axel Wirth, Symantec. So actually following up to that point right away, what I think is missing is a risk model that defines the tradeoff between clinical benefit and cybersecurity risks and you gave examples on you got phone calls and they were phone calls many of us got when St. Jude had the pacemaker recall. So I think we, as an industry, lack that risk model, clinical versus cybersecurity, and I think where that really would come to bear is once we're post-event, once we had the first cyber-related patient incident, which hopefully is far in the future, but how will patients react? Will they decide

and maybe reject perfectly sensible treatment options because of what they heard on the evening news the day before? And if we don't have that model, we're going to all be scrambling to make sure that people don't harm themselves by rejecting, again, perfectly fine medical devices.

DR. TARVER: And the last comment from the floor.

MR. CODY: Hi, Joe Cody from the American College of Cardiology. I want to thank you for having this panel, I think it's an important discussion to be had because clinicians are often the first line that patients reach out to, to try -- if they have concerns or questions. So I think some important points were raised. One is reaching out to the clinician community, whether it's through journals, publishing, attending scientific sessions to provide information on cybersecurity threats for medical devices so that clinicians are able to start to learn about cybersecurity threats so they are informed when patients come to them.

The question I have from a patient perspective is what is the best way for clinicians to present this information to their patients? If they necessarily aren't IT experts, is a pamphlet, is referring them to the manufacturer, is providing them additional information through online -- what is the best way that patients should digest this information in an easy and understandable way and how can clinicians be better prepared to have these conversations with patients?

DR. D'AMICO: I would hope that it's a group collaboration among my physicians, my disease foundation, and the manufacturers. So I would hope that perhaps they could have surveys that are sent out, so what's the best way to reveal this information without causing anxiety. So I think it's going to need to be a big group collaboration among many parties.

DR. TARVER: Any other thoughts?

MR. NELSON: Yeah. I mean, I think that the risk you run is you start using technical

terminology and then also the patient, you know, feels uncomfortable asking questions because they don't want to demonstrate that they don't know what you're talking about, I do that all the time when people talk about things I don't understand, and so I think there's a sensitivity of breaking it down so that it's understandable. I mean, if my doctor said to me look, there's an issue with this device that has come out recently, it has the impact of manipulating or altering the readings that you get on your meter and because of that, you know, we encourage you to do a finger poke if you feel like it's off, I get that, I can digest that.

If he says to me, you know, there's a man-in-the-middle attack that's going on and most people, I think, would tune out and so I think you need to learn how to present it in a way that's understandable to the patient and helps them understand the impact to the way they're treating their disease. And I think you can do that with most -- most of the cyber issues that I've seen, you break it down into a way that's digestible for the patient.

DR. TARVER: So I'm going to just end this session with two points, I heard two important things: How do you explain a risk to a patient if it's something technically challenging? And we see that with healthcare already. I mean, a lot of times we have to explain complex disease processes to patients, there is methodology that's been developed, shared decision-making tools have become available, and I think this is one area which could lend itself also very nicely to a shared decision-making model where you can explain the risk to patients in a way, or the potential threats, in a way that may be reasonable and keep them from having irrational fears that are not substantiated.

The other thing that I also heard was the benefit-risk tradeoff. I think all of you alluded to the fact that the benefits far outweigh this risk and I think there is methodology that has been developed to capture that from a body of patients with very heterogeneous preferences, it's called patient preference research and we've been doing quite a bit of that

at our center. So I will say that there are methodologies that are evolving to help facilitate this process and we look forward to all of you working together with us collaboratively as we advance how we communicate to patients as well as how we make changes in this ecosystem. So thank you all very much for your time. And I want -- thank you for the speakers and panelists.

(Applause.)

DR. ROSS: So good morning, everyone. We're going to have our next panel come up on leveraging innovation and collaboration. This is going to be a split panel because we have quite a few topics we want to cover. So for those panelists that are going to be part of the coordinated vulnerability disclosure discussion, you can go ahead and come up, and I'm also going to put your name tags here as well, in case you've forgotten whether you're part of this discussion. So just give us one second and we'll get started.

(Pause.)

DR. ROSS: So if we could please have Art, Daniel, Pamela, Denise, Scott, please come to the front.

(Pause.)

MR. WOODS: Hi, everybody. Are we ready to go? Just let me know when. Aftin, do you think we can start? Okay. So welcome to Plenary Session VII - Leveraging Innovation and Collaboration to Advance Cyber Safety. This is going to be a little bit of a different panel. We've got one panel now, then in about a half an hour we'll stand up and switch seats and we'll have some more folks come on and talk about some of the new and innovative solutions to vulnerability, exploration, discovery that are kind of coming around. So I want to give everybody a chance to just very, very quickly introduce themselves and then maybe start at the far end and go from there.

MS. ROSSI: Hi, everyone. I am Dana-Megan Rossi. I am with BD where I'm Associate

Director for Product Security Operations, and I think, technically, I'm on the second half of the panel, but I decided to sit in on this one, too.

MR. WOODS: Welcome.

MR. MANION: Hi, Art Manion, CERT Coordination Center. I manage a bunch of coordinated vulnerability disclosure work there. Primarily, I come from the general computing IT sort of side of things but we have obviously observed lots of safety critical embedded stuff getting connected, so that's my background here.

MR. BEARD: Did I get it? Hi, Daniel Beard, Director of MedISAO. One of the services we offer our members is a coordinated vulnerability disclosure program.

MS. GOLDBERG: Pamela Goldberg, President/CEO of the Medical Device Innovation Consortium. We're a public-private partnership between the medical device industry and the FDA.

MS. ANDERSON: Good morning, everyone. I'm Denise Anderson, I'm president of the Health Information Sharing and Analysis Center or H-ISAC and also chair of the National Council of ISACs.

MR. NICHOLS: Good morning, I'm Scott Nichols, Director of Global Product, Privacy and Security for Beckman Coulter/Danaher.

MR. SINGLETON: Good morning, my name is Greg Singleton. I'm the director of the Health Sector Cybersecurity Coordination Center at HHS. Our role is largely to work with the private sector on health cybersecurity, support the collaboration and cooperation mission.

MR. WOODS: And I'm Beau Woods, I am with I am the Cavalry, also the Biohacking Village at DEF CON and a number of other things, and I'll be the moderator for this -- for both parts of this panel. So the first question I want to throw out there, and I want to kind of keep it short and succinct, is what is coordinated vulnerability disclosure and what are

the roles and responsibilities? And I think maybe, Art, if you could start with that one.

MR. MANION: Sure. So it turns out lots of software has bugs, some are security bugs, that's the world we live in, no judgment there, right? These bugs are discovered, as we'll talk about more in the second half of the panel, I think -- and very often that is a security researcher or somebody outside the vendor or supplier or manufacturer organization. So this whole CVD process is that a manufacturer would have the capability to receive a report externally, you know, there's a bug in your insulin pump, in your pacemaker, in your device. A way to receive it, the process is roughly that that reporting happens, there is a period of time, typically, that the report remains non-public, this is time for the manufacturer to develop a fix, test things, figure out a deployment strategy.

Typically, and this may vary a little bit for the medical space, there's eventually a coordinated publication date, right, the researcher wants to post a blog entry, a CVE number may get assigned to the vulnerability, it gets made part of the public corpus. Ideally, a fix is ready at the same time, the manufacturer may release information about the vulnerability. So the publication of all the information is coordinated and then afterwards there's follow-up sometimes, you know, adjustment to a fix, further mitigation and feedback on what happened. But those are the basic steps: find, report, delayed private embargo period, sort of end it in publication and that's the high-level process.

MR. WOODS: So a fairly well-understood space, right?

MR. MANION: Yes. Again, however, it's all relative, right? If you are a manufacturer or a vendor, a software supplier, and you're at the first time you've had one of these encounters, it's new to you, obviously, but there's lots to stand on, there's a lot of -- there's documentation out here on the space, we've written a bunch of stuff, there's plenty of writing out there on it. So, yeah, we've -- it's well covered and you can learn from what's been done before.

MR. WOODS: Okay. And what medical device makers do we have on the panel? Just raise your hands really quickly. Okay. Daniel, yeah. Okay. And of those medical device makers, how many of those have coordinated vulnerability disclosure policies?

MS. ROSSI: Yeah, so Becton Dickinson, we are committed to coordinated vulnerability disclosure. In fact, my colleague, Nastassia, who leads our PCERT team is with us today and you're going to hear from her later. If you look at our website you'll see a list of all the bulletins that we have put out there and it's a really integral part of our product security program.

MR. NICHOLS: Beckman Coulter launched our CVD in 2017. Beckman Coulter is also owned by Danaher, so I also lead an effort to cross the other operating companies and so we have an active effort right now for the other OPCOs to develop a CVD as well.

MR. WOODS: Okay. Daniel, do you want to talk about your experience within the ISAO and disclosure policies?

MR. BEARD: Yeah, so many of our members have taken advantage of our CVD program and we act as a coordinator there where we take in the information and then coordinate with the researcher and the manufacturer. It's tough for some of the smaller ones to kind of get going on it and get buy-in and my advice to them is to kind of leverage what they've used for their complaint handling process and make it similar to that. It is a similar process, not the same, but similar and I think we've had good success when we've gone down that route.

MR. WOODS: What other lessons are there from around the ecosystem, around the industry? Maybe some of the folks who aren't medical device makers, what have you seen in looking at coordinated vulnerability disclosure?

MS. GOLDBERG: So back in October we put together a report, we interviewed a number of medical device manufacturers to gather together data on what a variety of

pathways are. And so we do have a report on our website based on information from the FDA and from industry on what might be optimal coordinated vulnerability disclosure. We followed that up about 6 weeks thereafter with a webinar on the subject and actually have that webinar also on our website with a case study of what is the process a company can and should go through.

MS. ANDERSON: So, basically, I think, you know, the organizations that have done it a few times, I think the process is kind of working out its kinks but there still is a lot of confusion from the various players in the ecosystem as to how to go about reporting a vulnerability and then also how do you get it out to the broader community at large.

MR. SINGLETON: From our part, I mean, I'd like to add where we typically get engaged in these incidents is when we see a vulnerability or communicating with our folks at FDA or others on a vulnerability that has come out and just the contrast between the coordinated disclosures and the non-coordinated ones is immense. There's a different process that we go through depending on what we're seeing.

If it's just something the researcher put out on Twitter, there's a lot of background work that goes into okay, what is this, how significant is it, how do you manage it and from the patient's and practitioner's perspective, I think that leads to a lot more questions and uncertainty because they've been told "alert, be warned" but without the "and this is what you do about it."

I contrast that with the coordinated disclosures where you kind of get a package that is this is the issue, this is why it's important, this is what you do about it, and you're able to communicate that out to the sector and others in a way that maintains confidence in the devices and maintains confidence in the firms.

MR. WOODS: Okay. So I wonder what challenges still exist for especially the device makers here who have stood up a coordinated vulnerability disclosure policy, like what was

the critical threshold you had to get over and how did you successfully overcome it?

MR. BEARD: So I think it's important before you're going to attempt to start building and framing the CVD, you really need to get alignment with various, you know, stakeholders in your organization, legal, QRA, R&D leadership, service, and support. That was one thing that was effective was to get senior leadership buy-in on that first, educate them so they understand exactly what the intent is, and we basically used FDA's postmarket guidance as really kind of our instructions to start building that.

And out of that actually came more than just a CVD but also not creating new processes, but inserting product security into existing processes. So when there's a complaint that's filed or customer feedback, you know, how does that feed into the CAPA system, how do we follow the existing processes to follow the 30/60-day rule and -- but it's very critical to get senior leadership buy-in across multiple stakeholders.

MR. WOODS: Okay.

MS. ROSSI: Yes, I will second that as well. Having that cross-functional collaboration is really key to having a successful coordinated vulnerability disclosure program within your company because it's not just product security, it's not just PCERT that is doing a coordinated vulnerability disclosure, we're working across different functional lines with our colleagues and when you start to build that bridge and you bring everyone together, what you start to find is that you have a consistent practice, driving the consistency, having the process be less tense, less scary for everyone who may not be as aware of what that process entails. Bringing that to the table each time in a consistent manner is really an essential part of making it so that it can be an everyday practice, that it's not something that anyone particularly from let's say like a legal perspective would ever feel alarmed or uncomfortable with.

MR. WOODS: So just a point of order, I hear we've lost the video feed, so before you

speak just say who you are so the people can identify you by your lovely pleasant voices. So looks like we got a couple of folks doing questions. Allan, why don't you go and just state who you are and who you represent.

Dr.. FRIEDMAN: So Allan Friedman from NTIA, and this is actually going to be a shameless plug rather than a question to the panel. For those of you who are interested in a coordinated vulnerability disclosure policy and want to know how to start, in 2016 NTIA published a document that was drafted by many people in this room on how do you start having coordinated vulnerability disclosure policy. This document is explicitly aimed at safety critical industries. It was developed by security researchers, by product vendors, by lawyers and the FDA was also involved, the FDA team, Suzanne's team was involved in this. So it's an early stage, there's a template, there's a guide on how to use it, you can copy and paste it, you can do whatever you want to it, it's free and open and I've heard from a number of companies in the room that it's actually a great way to start the conversation with your company.

MR. WOODS: All right, thank you. Next question, just who are you, who do you represent?

MS. REKIK: I'm Inhel Rekik. I'm the Director of Health Technology Security at MedStar Health. So I've read the coordinated vulnerability disclosure and it's a little confusing to -- because it says so manufacturers are supposed to collaborate with an information-sharing organization and have researchers submit vulnerabilities but, at the end, in the document it does say that the FDA does play a role into making sure that the known vulnerability is disclosed too early in the process. So I'm asking the manufacturers who have already, like, a coordinated vulnerability disclosure program, is how do they make sure -- what does the FDA play role into this program and how do they make sure that these vulnerabilities, that they -- that have been released, that they have actually compensating

control or they have a fix for it before they communicate it to the customers? And if you communicate to the customers, how do you communicate to them, is it through a letter, who do you send that to? Because I've had -- in the contract, I've been adding provisions where I -- this is an email address that I wanted to receive vulnerability information from and the response I got you have to go into the portal and log in and you will receive, so is that the way you communicate to your customers? So it's actually two questions in one, sorry.

MR. WOODS: Yeah. So maybe throw that to one of the device makers who's been through a coordinated vulnerability disclosure in the last year or so since the postmarket's come out?

(Off microphone response.)

MR. WOODS: Say your name again.

MS. ROSSI: Yeah. So we at Becton Dickinson -- sorry, I forgot. Dana Rossi again with BD. So at Becton Dickinson we work closely with our government partners, including the FDA, and so there's that established relationship that you have. So before you're going to release something publicly you want to make sure that there is something to tell, right? We don't want to prematurely expose customers to potential risk and so we work hard internally and with our industry partners in order to establish what it is that we need to provide for, you know, risk mitigations, compensating controls.

And then what we do is that website that I referred to earlier, what we do is we have a coordinated disclosure, right, so you're coordinating with your partners while that process is happening, as we discussed earlier, and then what you're going to do is you're going to look at our website, it's also going to be released through government channels and so we want to make sure that we have as much -- as much knowledge in the industry of what -- where that bulletin is going, what that bulletin states, so there's a couple of different

communication channels. But I would be interested in hearing a little bit more about what you're looking for, setting up an email address, let's say. If you have, as a manufacturer, a portal on a website, is it something that you would like to see be more searchable, is it something that you would like to have, let's say, a distribution list where you could sign up for, you know, particular types of bulletins. I'd be interested in hearing a little bit more about what you're looking for.

MS. REKIK: So, yeah, having the portal where you post vulnerability, it doesn't mean that these products, I have them.

MS. ROSSI: Um-hum.

MS. REKIK: So what we have with the recall process, which is a little bit easier, so we do receive notification letters of product and serial numbers that are infected with vulnerabilities. So we've had so far only received one letter for uncontrolled risk and it lists actually the serial number. So what is not happening with vulnerability securities that you have the notification but you have to go through the exercise of knowing what -- do you have that software version, what serial numbers are infected.

And when you're in my role, so I oversee the medical devices, medical -- beds and it's a lot of stakeholders that you have to go legwork, that we need to go to figure out if we have those products. So if with a new portal you can actually track MedStar has these devices, Mayo has these devices, it makes it easier to kind of locate the product. So I would just -- that's the whole point, like, knowing exactly which product because instead of wasting time, knowing if you have the actually software versions that is infected by the vulnerability.

MR. MANION: Yeah, so -- sorry. Art Manion, CERT Coordination Center. To speak very briefly to some of your -- what I believe I'm hearing from your general question, so two small things. Knowing what you've got and what's affected is kind of based on the -- we

have a large CBOM discussion going on, right? So the inventory problem, unsolved everywhere, all software unsolved and not just medical devices, right? We're working on that, okay? We are.

UNIDENTIFIED SPEAKER: Yes, we are.

MR. MANION: Like, everyone in this room is working on it, right? Hopefully, okay. We are working on it. A note about this disclosure, coordinated disclosure process, right? There's a process, you can read the documentation on it, it gives you a lot of good advice. However, in the interior, you've got the person or organization with knowledge of the vulnerability, secret knowledge, private knowledge of it, has the power to publish or disclose whenever they choose to. No one can control, for instance, what a researcher might choose to do and that's why a lot of the process is a lot about cooperation, right?

If I'm a researcher and I feel that the vendors are responding to me, working on things, cooperation is going well, coordination is going well, I'm happy, I'm going to follow the guidelines, right? If I feel the vendor is stonewalling me, not communicating, taking too long, I might decide one day, you know, I'm frustrated with this process, I'm going to publish, you know, have an uncoordinated release, that costs more, it's more harmful, it's bad. So there are no rules people are going to follow or sign NDAs about, you have to sort of guide the process with people you don't fully control, there's a lot of trickiness in there, a lot of edge cases, but that's part of the thing.

MS. ROSSI: Yeah, I just want to follow up on that again. It's so much about building relationships and it's not just about that cross-functional internal coordination. It's about the external coordination, recognizing that we're all part of this as industry stakeholders together, working in partnership towards a common goal, right? And so exactly what you just said, it's -- you don't necessarily have control over everything so part of our job is to make sure that we're proactively reaching out and building those relationships within the

industry so that we can have those constructive collaborative conversations.

MS. REKIK: And as part of the coordinated vulnerability disclosure, are there plans of making the coordinated vulnerability disclosure a little bit more targeted towards certain serial numbers or -- that are, you know, impacted or is this going to be -- remain, like, the same, these software versions, you're going to have to go to look for if you have them or not? Is it something in the roadmap?

MR. MANION: I can't speak personally for the FDA's plans. Again, though, this concept of the external parties involved, right, the external process and the relationships, I don't know that anyone's got control and I think we're going to talk about this in the next half of the panel, right, on there are lots of ways people come across these bugs and find them in the first place and report them. So, you know, again, the FDA and the device manufacturer don't control the fact that, you know, Jay or someone's going to go do research on the device in their body and that's going to lead to, finally, a serial number list of what needs to be worked on.

So the strict parts of the FDA process, I'm not an expert on whatsoever but, again, you have some external uncontrolled forces that are generating the findings and the discoveries in the first place. And, again, you covered it very well, the -- you don't control things here, but having a CVD process in place in advance gives a manufacturer influence over what happens and that is much better. Even just for the manufacturer itself having more influence over the process is a good thing, costs less, better PR, better safety, better lower risk, all those things.

MR. SINGLETON: So one thing I wanted to add -- Greg Singleton, HHS. One thing I wanted to add on that, just reemphasize the point on you're working on your relationship with external parties and we're -- for our organization, we're largely working with the IT communities, cyber community, and understanding the incentives that those researchers

are facing and what they're trying to do in terms of build credibility, build their research base, build awareness, and also hopefully do some good and bring some remedies to the table. They are facing different incentives than, perhaps, the manufacturers and other folks they're working with and it's really important to partner with them and understand how they're approaching it. And as I think someone down there mentioned, you know, building that relationship and maintaining the tight communication, giving them care and feeding and saying yes, we're working with you, we're working towards a common goal, it's just critically important in bringing people into what is ultimately a voluntary process.

MR. WOODS: So I want to ask one last question of the panel and then I'll get yours, Jim. What can we do, as a community, as an industry, to increase the adoption rate of coordinated vulnerability disclosure programs for medical device makers because, you know, a lot of the folks in this room already have one or one is in progress, but for the people who don't or maybe don't know about it, how do we get from awareness to action quickly and how do we get awareness to begin with?

MR. BEARD: I'm just going to plug the I Am The Cavalry list of medical device manufacturers that have coordinated vulnerability disclosure programs. It's huge for getting adoption from senior leadership because they say who else is doing it, here's everyone else doing it, they figured it out, let's learn from them.

MR. SINGLETON: Well, for those that have it, I mean, can you speak to your success with it? Of the disclosures released since you stood up your program, how many have come in through the process versus were uncoordinated disclosure? I mean, to the extent the process is successful, I think that would be the best promotion of it. Any comments?

MS. ANDERSON: And I think a lot of the medical device manufacturers are very good about that, especially the ones that have developed programs, they're very good about mentoring others and sharing their lessons learned and best practices, I mean, we see it all

the time in our collaboration forums, so -- but I think it takes -- you know, we just need to get out to the broader community, I think.

MS. GOLDBERG: And I would just add I think that all the major manufacturers are actively engaged in this process. I think it's the startups and the smaller companies that are struggling more and that's why it's important that we publish reports, that -- guideposts for those companies that haven't yet had a chance to think about cybersecurity issues and that the trade associations also get engaged with us.

MS. ROSSI: Yeah, and I'll add for our part at BD, we've been very active and engaged with the industry and so coming and speaking on panels like this, but also participating in white papers, publishing our policy and procedure on our website, making awareness around what it is that we're doing, being as transparent as possible so that we can provide guidelines and best practices and lessons learned as an industry. And also, I think, as a -- you know, a global medical device manufacturer, one of the things that we'd be, you know, very interested to see us move forward as an industry is on international harmonization and adoption of coordinated vulnerability disclosure.

MR. WOODS: All right, Eugene.

DR. VASSERMAN: I stepped out for a moment so I apologize if this was covered already, but I have a question for the room. Of the manufacturers in this room, how many post the PGT key to securely submit this highly sensitive information?

(Show of hands.)

MR. WOODS: A handful of hands.

MR. MANION: Or https website counts, right? Close enough?

DR. VASSERMAN: Well, sometimes a website form isn't the easiest place to fill in a highly complex set of -- and submit a hex dump of numbers.

MR. WOODS: All right, at this point I think we're going to switch over panels. So for

the next panel that we've got, why don't you come on up here or if you're going to be on that one, too, just stay where you are.

(Pause.)

MR. WOODS: So while we're doing the transition here, the second part of the panel is going to be new and innovative ways that we're seeing across the industry for exploring vulnerabilities, discovering them, collaborating together with security researchers, medical device makers and others in the ecosystem. So I'll do the same thing again, just start, give a name and briefly introduce yourself.

MS. ROSSI: Dana-Megan Rossi, BD, still here.

DR. GOLDMAN: Julian Goldman, Mass General Hospital and Partners HealthCare.

DR. DAMEFF: Christian Dameff, University of California, San Diego.

MS. ALLI: Nina Alli, project manager of the Biohacking Village at DEF CON.

Dr.. FU: Kevin Fu, the University of Michigan and the Archimedes Center for Medical Device Security.

MS. GILBERT: Lisa Gilbert, Applied Research Solutions.

MR. WOODS: All right, so I wanted to go around and just ask a handful of folks who are doing some of these really interesting collaborative ways of finding bugs or understanding impacts, to just describe them. So maybe Kevin, start with you and we'll hit some of the other folks along the row.

MR. FU: Okay, here we go. I'm not that great with technology.

(Laughter.)

MR. WOODS: He breaks things.

MR. FU: Well, so it's interesting you say that, but so there are students in my lab who do what you might call breaking or security analysis, but most of what we do is about finding security principles and practices to improve security design and security in. But

you'll mostly hear about when we break something because it tends to be a little more newsworthy and nobody cares when we fix something. I wish there was more attention to the fixing, but on the breaking side, I think my perspective might be -- I think will complement some of the other speakers, but in academia we tend to focus on identifying new classes of flaws as opposed to individual flaws in products. So we won't typically generate a vulnerability disclosure, at least from my laboratory, for a particular product, but we might discover that a large swath of products maybe have forgotten some kind of design control for computer security.

I have to keep adding one every year, but it's been 11 years since we published our pacemaker defibrillator security paper where we showed how to induce ventricular fibrillation, a deadly heart rhythm, using a homemade radio transmitter that my students built. So that was a wakeup call for us and I think the industry and regulators and all stakeholders, but I think it's -- there are many different pathways to doing bug finding and vulnerability disclosure, but with my students I usually ask them a simple question, is why does it work and then they -- it's inevitable they're going to find that something doesn't work because that's human nature and how engineering is, but we try hard to keep things secure by design.

MR. WOODS: Okay. Julian, do you want to go next and talk about some of the work you're doing in your lab?

DR. GOLDMAN: Sure. Thank you. Over the past year or so we've been working on a project to understand the role of a virtual hospital sandbox for medical device cybersecurity preparedness. This is a project that is formed, has been formed, developed with MITRE Corporation and funded by the FDA to share the results of the -- of this exploration with the broader community once we wrap things up, which will be in a few months. One of the activities that we performed was to collaborate with a regional group of hospitals and

better understand some of the challenges and gaps that occurred with the response to WannaCry and a lot of that information was put forth -- that and from other events, was put forth in a report published in October by MITRE, and so it's a playbook which is publicly available. We learned from a number of these activities with the healthcare -- with other healthcare organizations and manufacturers and working with other third parties that support biomedical equipment management, we started to learn what they see as the value of a sandbox in a sense as a go-to environment as well. So when there's an event and one has to respond, how can we do that as a community?

As the manufacturer either identifies the vulnerability, where can we duplicate that or replicate that in a manner that it can be examined and look at its effect on the rest of the system in the hospital including caregiver workflow, impact on the networks, impact to other devices. And then as solutions are identified, mitigations, other patches, whatever they might be, although manufacturers can do everything in their power to develop and validate those internally, you know, deployment is another matter, as we all know. There are differences in complexities with different network architectures in hospitals with different skills and capabilities for deploying some of these patches, and so the idea is that the sandbox becomes a place where these can be demonstrated and tested and the lessons learned can then be shared to facilitate deployment around the rest of the country.

So those are some of the ideas behind it and the work that's been preceding includes the development, using our lab at Mass General Hospital, which is a medical device interoperability and cybersecurity lab which we founded in 2006 but has been greatly updated in the last year with capabilities to support implementation of different network architectures to emulate different hospitals, the ability to deploy different medical device networks that fulfill the requirements of manufacturers and to look at end-to-end dataflow and clinical workflow using simulation, simulated patients, other physical and software-

based simulations. Also, we had to implement segmentation and micro-segmentation for obvious reasons when dealing with cybersecurity. It's nice to share the information that results, but it's not nice to share the infection. So all of those things have been -- you know, have been considered and that's the work that we've been doing.

We've worked very closely with a couple of select manufacturers, medical device manufacturers, as a partnership in this project because part of the plan in the next phase is to demonstrate the risks that occur with unpatched devices with known vulnerabilities, using known vulnerabilities for this, demonstrate the risks in terms of the effect on workflow and clinical impact and the importance of mitigating those risks through appropriate means, demonstrating that in the lab and really better understanding the implications. And so we're working with Philips, and there may be someone that wants to speak to that later in the panel or during Q and A, and also with Becton Dickinson and you're going to be here? You're not leaving your seat for the next few panels, right?

MS. ROSSI: Yeah, I'll be here.

DR. GOLDMAN: Yeah, okay. So I think, you know, that's -- so a big part of this is the concept of a project to understand the needs in a lab, in a sandbox, what are the considerations for a go-to environment. We're looking at the complexity of developing the relationships, the legal agreements, nondisclosure activities to preposition all the relationships and that's challenging, and we'll have lessons learned to share about that with the FDA which will help inform some of our national need. And we've also identified that a lot of the stakeholders that have come in and out of the work said we need some kind of a way to share information as a community as a collaborative, and so we've laid a foundation to start a collaborative and start to just build those relationships and that's been done with the support of Dr. Shuren of CDRH. So that's a summary of what we've been up to.

MR. WOODS: Okay. Christian, why don't you talk about some of your work with,

like, especially the CyberMed Summit, but other things to help bridge the gap as both a doctor and a hacker.

DR. DAMEFF: Briefly, can anyone raise your hand in the audience if you practice clinical medicine or allied health nursing, anything else, you actually take care of patients on a regular basis? Yeah.

(Show of hands.)

DR. DAMEFF: Real patients. Yeah, a vast minority. I'm seeing one hand. And that was the genesis of the work behind CyberMed. We recognized that there was clearly a stakeholder that wasn't showing up to these conversations where device manufacturers, security researchers, hacker community and other health delivery organizations, etc., would show up, regulators. Amazing. But we didn't -- we lacked that clinical aspect of it and what we often ended up having was vulnerabilities in medical devices that were being publicized that lacked truly the clinical insight on how it would impact clinical care, how it actually would harm a patient or perhaps other viewpoints from clinicians that might help inform and catalyze change for a more secure environment.

So the CyberMed summit is a free, not-for-profit conference that brings clinicians, medical device manufacturers, hackers, regulators and other stakeholders into a simulation environment where we run clinical simulation, so something akin to what you'd see in pilots training for taking off and landing. In medicine we practice clinical simulations with fake -- with actors and fake patients in fake clinical environments. So we took unsuspecting clinicians, put them in environments and used real research to base simulations of what happens when a patient's pacemaker AICD has been compromised and it's repeatedly shocking them despite their appropriate rhythm. What happens when their insulin pump actually delivers too much insulin because it's been compromised or when there's a ransomware attack and they're trying to take care of a stroke, a heart attack or a trauma

and they lack some of these clinical systems to help support care. We take unsuspecting physicians, throw them in these simulations and see what would happen. So that's the CyberMed Summit. And then I think, hopefully, we'll be able to spend a lot of time talking about kind of outreach into the hacker community.

MR. WOODS: Yeah, perfect segue. Nina, why don't you talk about the Biohacking Village that Suzanne mentioned yesterday and how that's an innovative model for collaboration and vulnerability research?

MS. ALLI: Can you hear me? I speak really low. Good? Awesome. Okay, so the Biohacking Village is about 5 years old and last year we were having a discussion about the genesis of how it worked and how we can make it better and one of the things that we realized was that we're not -- we were not completely showing how the ecosystem of the hospitals was working. We just had talks, we had a couple of medical devices, and then last year we bought a whole ecosystem of various equipment, devices, to show the hackers how a hospital really works.

And it was a beautiful somatic relationship, the hackers were coming in, they were having face-to-face conversations with the medical device manufacturers and it wasn't a cloak and dagger situation anymore, it was let me show you what I found in your device because I have this at home, I bought it somewhere, but let me show what I did and how you can replicate it and how you can make it better.

So one of the ideas that we've been working on along with I Am The Cavalry and Bug Crowd is when we go to DEF CON, indeed, the medical devices are out there, the hackers come in, they have full conversations with the medical device manufacturers, there's back-and-forth conversation, they're helping each other, what's going on, can we discuss the back end, the software, the hardware, how is this working, and they get full informed disclosures with real names, they have contact information, so that they can reach out back

to the hacker and the hacker can reach back out to the medical device manufacturer. This way now there's some relationship rather than just getting a random email saying I got into your stuff, here's some details, go fix it. They can work together to create something better for patient care.

MR. WOODS: Good. So if we're talking about innovative approaches, innovative solutions, that kind of indicates that there might be some kind of a problem and that there's some value to come from the innovative solution, so just open up to the entire panel. What value do you see coming from these different types of approaches or what problems exist that need to be addressed? Go ahead.

DR. DAMEFF: So I work in the emergency department and when I'm not working clinically I love doing security research and I'll tell you briefly about a project that had some flaws and problems last year. I bought a medical device off of eBay, it cost $150, it came from the secondary market, none of which many of the device manufacturers in the room have control over. When I obtained this device, I quickly found that it had over 3,000 patient records on the device and the only way to "wipe the patient records" was to download a script off of a random ftp site that didn't actually delete the patient records, it just deleted the log of the patient records.

So what ended up happening was this, this problem with vulnerability discovery and disclosure is that the devices are accessible rather easily, I can call many second -- secondary market organizations and get nearly any device or a board off a device that I want and what ended up happening was we immediately had roadblocks, you know, we had to build this test environment to actually see the clinical implications and be able to replicate a vulnerability that we found. And so we reached out to the manufacturer, and we had this really interesting collaboration develop where we basically came to them and said we're going to do this anyways, we have the devices, we have the vulnerability, would

you like to work with us on this and they said yes. I'm not sure if that's because I said I was going to do the research anyways or if they really did want to collaborate, but they lowered the bar for us to actually deliver our research, they gave us proprietary middle ware that allowed the operation of the device to be much easier, they provided us some technical support, and that was actually a really amazing part of this.

One of the things I would say was a problem was that there was so much discord within the medical device organization itself, there was so much bureaucracy and to get approval to even give us a medical device or a cartridge for the device, etc., like a reagent cartridge, it took talking to 15 different people and once it reached the right person we saw a catalyst for our research, someone was able to cut through that bureaucracy. I really encourage that, perhaps in collaboration with your coordinated disclosure program, to have some type of point person who understands the security implications, can liaison with the researchers, and then collaborate in a meaningful way for the researchers that they'll want to engage with you because they don't have to reverse engineer anything else that's unnecessary or -- a great example of this was we had to reverse engineer a cartridge solely because we couldn't get it in time.

Let me rephrase that. We bought a medical device, it needs a reagent cartridge, the reagent cartridge had a 30-day software limitation, so once you activate it, it only could be possible to be used for 30 days. We asked for another cartridge from the device manufacturer, some were willing but because of all this discord, it took too long so we actually had to reverse engineer the security on the cartridge so that we didn't have to spend another $2,000 to continue to do our research. That's the type of thing I think that you can really reach out to security researchers when they're doing vulnerability discovery on your devices, reduce those types of unnecessary burden from the researcher's side, you'll develop a very nice relationship with them and they also won't reverse engineer your

protected cartridge software which counterfeiters would love.

DR. GOLDMAN: I'll take the next stab at the gap or the need. I think we have to realize or recognize that operational medical device cybersecurity requires the collaboration with a lot of stakeholders. We have clinical staff, biomedical engineers, IS or IT departments, technology platform or infrastructure manufacturers that are used by organizations, and regulators. I'm sure I'm missing a couple more. And so effectively collaborating on a technical topic for operational purposes, especially when there's a sense of urgency, is really difficult to do just by talking on the phone.

And so that's the problem that we're trying to address and trying to think about that in advance of a need, so on the preparedness side, and then think about how to leverage those types of resources on the response side and trying to get a sense from the community of how to do that and it's complicated, there's technology and relationships. But, basically, it has to be a team sport, and it's pretty hard to prepare for a team sport in a game by sitting around the conference table and talking; you have to practice somehow and that's what this project is essentially about.

MR. WOODS: Dana.

MS. ROSSI: Yeah, and I'll follow up on that. So BD is -- as we discussed yesterday, Rob Suárez announced that we are once again committed to the DEF CON Biohacking Village. We participate in several other collaborations including the sandbox that Julian mentioned earlier. We are also participating in the NTIA SBOM working group and one of the -- I mean, just from a very basic level, one of the reasons that we participate in these collaborations is that you help us make our product better. There are things that we can only do working together as an industry, simply put. But there are challenges. So as Julian mentioned, you know, in putting together some of these agreements and collaborations, there is a need in this industry to make this the norm, to go beyond what we've currently

done because from, let's say, a legal, you know, contracting perspective, what happens as a manufacturer when you're working with a relationship with an HDO and you've got a procurement contract currently going on and yet you're donating demo product for a cybersecurity collaboration. There are ethical considerations and things that you need to consider from a contracting perspective that we need to get past some of those -- some of those potential issues and look at creative ways like putting CRADAs together, collaborative research and development agreement, working together with government partners in order to bridge the gap and get over some of those potential hurdles when we're looking to establish the relationships and also help our partners, our legal counsel, to understand what it is that we're doing and putting together our statement of work so that we can more collaboratively start to look at this from a proactive perspective and make it the norm and not look at this as a special project or even from the perspective of looking at demo equipment.

If I'm putting my equipment in my product in a potential lab situation where I want people to hack it, right, I want people to try and break my product. Well, then, it's not going to be product that you're going to want to do a demo on in order to look at whether or not you're going to put that in some other type of function or capability. And so we have to start making these collaborative projects the norm and look for ways to bridge that gap in creating agreements to streamline this and make sure we get over some of those potential ethical hurdles.

MS. ALLI: Just as an addition to what you just said, I loved everything. The FDA has a cyber medical safety advisory board and one of the things I was thinking about last night was what if there was a hacker in residence here at the FDA and they had some sort of Rolodex or active directory of people, of hackers that they knew that if there was a situation going on with a medical device you could call the FDA and say we need a human,

we need a hacker, to come help us fix this thing, figure it out, can you help us, whatever that situation would be and the FDA can provide you a person, a team, a group, and the hackers could get in there and help fix it.

MR. WOODS: So the desk has been awfully quiet. What do you think?

MS. GILBERT: I come at this not from a medical perspective per se, but from a military perspective and what we teach our students, I teach my students a defensive cyber weapon. And so I think it would be really good to be able to help develop, especially in the manufacturers, a defensive operator mindset so they are thinking about and anticipating potential attacks as they're working on their design.

MR. WOODS: All right, Michelle.

MS. JUMP: I figured I'd come up here early this time so I don't lose my opportunity. Michelle Jump from Nova Leah. I really enjoyed the panel discussion today and it kind of reminded me of something that came up in our breakout session yesterday which was I think that it's fantastic to see the collaboration between hospitals and hackers and medical device manufacturers. But I think there's also something to be said if we decide what kind of information we need to collaborate on and we get clearer on what we expect from manufacturers and hospitals. Something that Allan had said yesterday was, you know, you will start to find that tool manufacturers will actually start to develop solutions, as well, and I joked that, you know, we're here, actually.

I left the manufacturing world last year to try to help drive more innovation and collaboration and make those tools available and I think that there is something to be said for also trying to leverage technology to help drive some of this as well as bringing people together as well because I think that the amount of data we're looking to share, it really is a massive amount of information and trying to leverage technology. I wrote an article for AAMI, actually, that was supposed to come out with their *Horizons*, but I think it's coming

out sometime soon, about this very issue. We have a lot of design issues to handle and we have a lot of other things to handle, but there's also making sharing information easier, which I think is a great thing and it would be great to see more development in that space.

DR. GOLDMAN: Michelle, if I could comment about that. We have been meeting with a number of medical device cybersecurity appliance and tool manufacturers and have deployed some of those in our lab as well. What we hope to have set up within a few months is the ability to capture data, for example. And so that's part of the collaboration, right, to empower companies that are doing what you just described to do a better job, so provide access to different types of network configurations, for example, different topology, because those are all important for the deployment of the tools. So that's been -- that's kind of early stage work and look forward to discussing it further with anyone that's interested.

MS. JUMP: Great. Thanks, Julian.

MR. WOODS: Next up at the microphone.

MR. TUGMAN: Hi, Jason Tugman with Axio. So I want to -- Julian and Dana said some really interesting things. First of all, Dana said, you know, we need to make these interactions, you know, the norm, right? They have to be. And then Julian, just prior to that, Julian said that it's very difficult to have time sensitive conversations over the phone, right? So one of the things that we do in the energy sector is we bring in -- we do tabletop exercises as a part of our incident response. That can be cybersecurity incident response or ATP-based incident response to the power, to the grid. One thing that we do for the tabletops is we bring in our field -- our FBI local field officer or coordinator for the FBI depending on where we do the tabletop or for what organization, but it's the norm to have that person in the room so (1) you have the relationship with the person and (2) it's a part of the tabletop exercise. So in this case you could replace the FBI field coordinator with a

hacker, right, that you were kind of mentioning, having that Rolodex of people, so that your organizations can do tabletop exercises about what if something happens or how would something happen and have the person in the room from a tabletop perspective and make that and to get to Dana's point, you have to make it regular, make that a part of your built-in annual incident response program to have this tabletop. And so I just wanted to say that's how we do it on the energy side and it might be applicable to kind of addressing some of what you guys are doing.

MS. ROSSI: Yeah, I absolutely agree and having exercises, regular exercises, is critically important and that's something that we do at BD, as well, and you're going to hear about it a little bit more later.

DR. GOLDMAN: And just to clarify, I didn't mean to imply that there isn't value in getting on the phone in an emergency, right? It's just doing -- exclusively working in that without a technical environment, you know, leads to ideas that just are not effective, solutions that can't be implemented or deployed and so forth, so right, just to clarify. Thank you.

DR. DAMEFF: Real quick. We do exactly the tabletop simulations that you mentioned at the CyberMed Summit, and those are actually some of the most insightful parts of the conference because we have multiple stakeholders there including law enforcement, including hackers, medical device manufacturers, and we'll simulate an attack on healthcare infrastructure quite often embodied in a fake hospital, if you will. So the insight, for example, that an attack might take out the elevator, what blew people's minds, because when I asked the clinicians what are they going to do with the patients in the ICU when you can't take care of them, they said we're going to transfer them and I said the helipad is on the roof and the elevator doesn't work, or perhaps they attack the air conditioning in a Phoenix hospital in the middle of the summer, it's going to greatly increase

the urgency of taking care of these issues because the patients will suffer in extreme heat.

So those tabletop simulations happen to be -- the unfortunate reality is that healthcare delivery organizations rarely do these tabletops. They are, at most, under the banner of what's called a technical failure, maybe they'll do these once every couple of years. They actually don't have to do a simulation for hospital accreditation, that is a cybersecurity attack, they just have to do a tech failure, if you will. And it's very infrequent, I imagine it's horribly immature and we don't really know, honestly, how many hospitals out there have even table-topped this with the people in their own hospitals. It's probably a vast minority.

MS. ALLI: As an add-on to that, I feel like the yearly meeting between the medical device manufacturers and the hackers is at DEF CON, at the Biohacking Village, so just coming off of that. We have at CTF, a capture the flag where there are live exercises for people to work from within the medical devices. We have the trainings to help the hackers build out toolkits and interact with medical device manufacturers, we have the tabletop exercises with I Am The Cavalry for emergency readiness and then we have the rest of the conference where there's a hands-on lab for people that have never worked on anything, the talks and the medical device breakdown village.

MS. CHASE: I'll just take it out. So just to build on what, you know, Nina and Christian were saying and to give a plug to the last panel of the day to encourage you all to stay here, it's on preparedness and response and so we'll be talking about some of these cyber exercises and other kinds of things. So, you know, hang around. But one of the other things I wanted to bring up, another opportunity for collaboration that brings together security vendors and device manufacturers is NIST's NCCoE, the National Cybersecurity Center of Excellence, and it's another opportunity to bring people together to try solutions to defend devices. You know, Dana's nodding because BD has been one of the

manufacturers involved in the wireless infusion pump work they did there and -- you know, and folks, anybody can go and join their communities of interest to help shape what they do. So I think Sue Wang may be here, I know she was here yesterday, but she's one of the NCCoE folks and you can grab a hold of her and find out more about it.

MR. WOODS: All right.

DR. GOLDMAN: Penny is a member of the MITRE team that we've been working with on the project, on the sandbox project, and so if anyone has other questions, feel free to talk to Penny or Margie or Steve or the others that are here for those, if you know them.

MR. WOODS: All right. And that is our time, so thank you very much for being here, and we look forward to seeing you around.

(Applause.)

DR. CARMODY: Thanks again. All right, everyone, we're going to take a quick break, and we plan to start off again around 11:10.

(Off the record at 11:06 a.m.)

(On the record at 11:18 a.m.)

DR. D'AMICO: If you are a panelist for the scoring vulnerabilities panel, please come to the front.

(Pause.)

MR. ENGLERT: Very good. Welcome back, everybody. I think we have a great panel here. I think we'll start out with just quick introductions, starting with Art on the right.

MR. MANION: Sure. Hi again, everyone. Art Manion, CERT Coordination Center, background in traditional compute-coordinated vulnerability disclosure. Guess what? Trying to assess the severity priority risk of a given vulnerability has been a problem for -- since the beginning of vulnerabilities, so 30-40 years, it is not solved today.

MR. TUGMAN: Jason Tugman, Vice President of Cyber Risk at Axio. I have

developed scores, scoring systems for Lloyd's of London, also for various product companies, and specific to some of the vulnerability scorings, I have a love/hate relationship with it and we'll get into the reasons for that later.

MR. JACOBSON: Jim Jacobson from Siemens Healthineers. We are participating in the CVSS rubric piloting from MITRE and so you'll hear a lot more about that as we go along.

MR. RIOS: Hello, everyone, I'm Billy Rios. I'm a cybersecurity researcher, I do a lot of work on medical devices but had a chance to look at other complex systems like airplanes and locomotives and cars and things like that. So I have some perspective on risk associated with these devices, but from an assessment standpoint and also like an impact standpoint as well.

MR. COLEY: To finish Billy's introduction, he has also worked on a risk scoring metric that's broader than medical devices, but does focus on medical devices. I mention that because we are coopetition, so to speak. I'm Steve Christey Coley for The MITRE Corporation, working with my colleague, Penny Chase, on the CVSS healthcare rubric, and I have a background in helping to develop CVSS, and I agree with the notion of having a love/hate relationship with metrics.

MS. CHASE: And I'm Penny Chase from the MITRE Corporation, and I'm working with Steve on our CVSS rubric, and one of the things I think we all see are love/hate relationships, that there are different kinds of values of these systems here, there's the score itself, but there's also trying to provide better communication between all the different stakeholders who care.

MR. ENGLERT: Very good. Thanks, Penny. And I'm Phil Englert. I've been in the healthcare technology management field for 30 years, 23 years with Catholic Health Initiatives, leading their clinical engineering operations for, you know, a hundred-bed -- or excuse me, a hundred-hospital system. So have seen it all, have asked to do it all, and

understand the challenges in trying to figure out just how do we measure risk on medical devices in the clinical environment.

And so, very quickly, I want to talk about a little bit what does clinical context mean. And so we started there, but let's come back to Penny and say, you know, MITRE has had to look at the CVSS and how it can be adjusted, they put together a team to discern just what that was, and so just don't go into the technology of the scoring, but let's just talk about what your group talked about or identified as clinical context.

MS. CHASE: Yeah, so clinical context came up in two respects. So for those of you who know what CVSS is or, you know, I'm not going into detail, but some of it explains what the exploitability characteristics are. So what's the access vector? How can an attacker exploit the vulnerability and get into a system? You know, do they have to be physically on the device? Can they do it from anywhere in the world over the Internet? The complexity of the attack, whether you require elevation of privileges and other content elements for exploitability. And so although CVSS, you know, breaks this down and has a good rubric for general IT, we recognize that when people try to think about it in a hospital setting there sometimes could be confusion. You know, what is an adjacent network in a hospital setting, you know? And so we wanted to, in the rubric, clarify some of those kinds of issues.

The other part that we focused on were the technical impacts, the confidentiality, integrity, and availability impacts and we tried to, in the rubric, create a systematic way to go through the different kinds of data and processes that you would see in a hospital setting and make sure, as you were doing the scoring, you really would step through each of those kinds of data. You know, is there PHI, is there data that has to do with diagnosis and monitoring, is there data that has to do with delivery of therapy and so on and force people, when they're doing the assessment, to really look at everything and consider those. So those were kind of two main areas. I don't know if Steve wants to add anything.

MR. ENGLERT: Very good. And, Billy, how about you, when folks talk to you about clinical context, or how do you think about that?

MR. RIOS: Yeah, I think it's -- I think some people know the story, but in 2010 me and some other folks basically got selected to look at one of our national weapon systems, like one that the president can launch. And so we did some work a couple months and at the end of the day we created this report that may have had some vulnerabilities in it and we were asked to stack rank them, rack and stack, as the military would say. And so we did that, and we gave it to some folks, and they looked at it, and they're like this is totally worthless and we're like how is this worthless, right? Like, there's a lot of vulnerabilities here or maybe potentially a lot of vulnerabilities.

But at the end of the day, they were like, hey, man, this doesn't tell us whether or not we could still use this thing. Like if we need to launch this thing, it doesn't tell us whether we can still do it, it doesn't tell us whether someone can stop that from happening, and like we actually don't even care about the vulnerabilities themselves, we just care about the capability, whether the capability is still available. And so I think that lesson applies to healthcare, right, like man, you could have a report with a thousand vulnerabilities, but if it doesn't mean anything to a patient, then I'm not saying we shouldn't care about it, but maybe we shouldn't care less.

And so if we look at what we have in place right now, like CVSS, some people say hey, you know, the numbers don't lie, but when you have vulnerabilities that could potentially kill someone and those are a lower CVSS score than vulnerabilities in supporting systems, the number is lying to you, right? In fact, CVSS, like pathological liar, right? So lying all the time, habitual. And I think when you take a look at why that happens, it's because CVSS obviously was not made for healthcare, it was made for IT and really the biggest metrics, the most heavily weighted metrics in CVSS are vulnerability characteristics,

so the characteristics of the vulnerabilities themselves. And that's important, but in healthcare the most important thing is probably the patient, right, and what happens to the patient. And so instead of focusing on the vulnerability characteristics themselves, I think it's more important to focus on what could happen to a patient, right?

And so it's very much a shift in the way that you think and so I hope that, you know, any scoring system that we have in the future focuses more on patients and less on vulnerability characteristics. And there are some other benefits to doing that, but I think that's probably the single most important piece when you're kind of thinking through this problem.

MR. ENGLERT: Very good. And, Jim, you interact with customers, with healthcare customers often. And so what are the keywords or phrases? How do you know, how does your customer base express the need for clinical context?

MR. JACOBSON: Right. Exactly what Billy was talking about, when a customer is talking to us about a vulnerability they want to understand the risk to patient safety, not necessarily a CVSS score. There may be some elements at the HDO that have an interest in CVSS itself, but it's much more important, is this a safety risk? Is this something that we need to act on immediately? So they want to understand the context from the standpoint of patient safety as well as information control.

MR. ENGLERT: So very good. And from the HDO perspective, you know, when I think of clinical safety or when I talk to peers in a healthcare delivery network, you know, they talk about patient safety and we've heard that several times, right? And privacy is a big thing, right? The incentives in healthcare for the delivery side is really around protecting the privacy, protecting the data. But also they talk about operations, the ability to continue to deliver care and not just care, quality care, right? And I think the third one, the third element that gets often overlooked, is the impact on revenue, you know, or the

financial impact, and it's not just the immediate, you know, lack of revenue, right? It could be the opposite of that as penalties and then the long-term reputational risk to the organization and how that might go, right?

So, Art, how about -- you know, what do you see as some of the challenges we have with current scoring systems or how can you wrap, you know, the risk of a vulnerability or a scoring system into that kind of context?

MR. MANION: Sure. First, it's actually a fairly difficult problem. You're basically asking did you do, you know, a good risk assessment on every vulnerability that you encounter? In the IT space, we're at around 20,000 publicly disclosed ones per year, who's going to do a full risk assessment on each of those, right? So we've got a scale problem. This was just covered a minute ago, but context is probably the very most important thing here. CVSS, even for the IT stuff it was designed for, is very limited in how it can account for context. So even in the IT space people taking CVSS-based scores and racking and stacking them are going to get bad answers, they're doing it wrong.

If you are using CVSS, please, please, please, it is in the input to your risk decision and do not use base scores as they stand. Even though, you know, NIST and BD is providing them free, free number candy, don't take it, that's input to your bigger scoring systems. Context, super, super important. CVSS is local technical severity of a vulnerability. They are much, much different things.

MR. ENGLERT: So very good. And, Jason, an outsider, you know, industry perspective, how would you advise this or look at this?

MR. TUGMAN: Right. So really I think we've hit a lot of the major points and I'll just follow on to read. So specifically to CVSS -- and I wrote this down because my love/hate relationship with any scoring model, regardless if it's CVSS or not, one is the misunderstanding, the radical misuse of the score, the radical misuse of scoring, because

the scores are numbers. They are not ratios, right? So they are information sources and represented in number form. So what that means is -- so the way that this CVSS is specifically, they said "intended to be used as a qualitative information source to inform prioritization," to inform prioritization. So if you rack and stack it, right, you are ignoring its purpose. It is to inform.

So if we look at how a score is developed, we really have to understand what data is. Nominal data, yes/no. Ordinal data, high, medium, and low. CVSS is an ordinal. In other words, an ordinal says that it has a rank but it doesn't have a distance. Red is bad, green is okay, right? Intervals, think about temperature, right, 33 degrees or 20 degrees and if you add 10 degrees, right, is it -- if you add another 20 degrees, is it twice as warm? No. So you have distance and you have a relationship but still no defined quantitative distance. Ratios are numbers. That's math, right? It has a true zero. A zero is a zero. There is no zero temperature, right? So CVSS uses a mix of all of those.

So the reason that I don't like CVSS or scoring models -- it has nothing to do really with CVSS -- is the way that people use that as a data input. It's not data, it's information. Information is data, yes, but we have to stop looking at the number that it spits out as a rack and stack and say what is that number in relationship to my defense in depth? So a four on my exterior network or my exterior, you know, surface is going to have a larger attack surface. I might want to remediate that even if I have seven nines directly touching each other in the same sphere of trust, the adjacency of my critical data, right? But that's four layers of -- but if you just say nines first, eights second, right, you're misusing that, so you have to think of your network and how that number relates to your network and most people don't do that. There's another piece that I won't talk about, you can talk to me about it afterwards, is how vendors radically misuse this as a number in their credit scores or other things. So they use it as data, it's not. So those are really all the things you need

to consider, is what a data type is.

MR. ENGLERT: So a very interesting analogy. I like that, I like that. And I can tell Steve is just dying to respond to this, so let's turn the microphone over.

MR. COLEY: Hopping in my seat. As a follow-on to that, one of the things that Penny and I found in developing the healthcare rubric, along with working with many members of the CVSS healthcare working group, some of them here on the panel, is it's really about the process of going through and figuring out what aspects of a vulnerability you want to look at and how it's relevant. The score may be informative, but it's certainly not the final decider. And the way that the rubric is structured, if you look in the upper right here, is effectively as a series of questions, almost a decision tree. It is a decision tree which provides some healthcare specific kinds of questions to help people narrow down into areas that are important.

So as Penny had mentioned earlier, when it comes down to confidentiality, integrity, availability, you know, the key aspect of the CVSS, we still ask about that, but we ask about that relative to different types, different kinds of data that may be processed such as, as Penny had mentioned, you know, PHI, data that may impact clinical workflow and so on.

Part of the structure of the rubric and part of the hope for the rubric is that it avoids or at least minimizes some of the potential vendor abuses that have already been referred to. Looking for consistency of scoring, looking to avoid common pitfalls that we have seen occur through our analyses and our investigations. So a greater breadth of consideration for healthcare-specific characteristics as one is looking at a vulnerability is one of the key outputs, effectively, of the healthcare rubric.

MR. ENGLERT: Yeah, Penny and then Billy.

MS. CHASE: So, you know, people often say, you know, it's all well and good, you have CVSS, you get this number, but the number doesn't really mean anything, you have to

look at the vector. But even if you look at that vector it can be very hard to interpret what all of those vector assignments mean and so one of the things that we're really trying to do in the rubric is provide this set of questions, record the answers so in the -- the table at the bottom right kind of shows that for each set of questions associated with that decision tree there's a vector element and you record the value that you made. And so our hope is that people will -- you know, you got the number and you have the CVSS vector, but now you also have this extended vector and it provides information that can be input to your true risk assessment and safety assessment processes.

MR. RIOS: I think I know that, like, from an academic standpoint, folks will take a look at the RFC for CVSS and be like the numbers don't matter but those numbers freaking matter, right? Like, if you go to ICSR or DHS, to their advisory, like that number is on there, right? Like, if you look at the premarket or postmarket guidance, it talks about CVSS. And so for us to sit here and say hey, the numbers don't matter, they matter, right? And so unless we give folks another way to do this, right, and I think, I hope that -- and from what I've seen, people are doing this, right? If there is a vulnerability in a product the manufacturer is going to do a safety analysis on it and that's the right thing to do, but one of the problems is that these manufacturers do it in different ways.

And so when someone comes out, a manufacturer comes out and says there's no patient safety implication for this particular vulnerability, we have no idea how they arrived at that and it may be a strong, rigorous methodology that they used that's gone through multiple levels of review, created by a PH, we just have no idea. And then at that point the manufacturer has to explain to us what their process is and their process will be different from manufacturer X and their process will be different than manufacturer Y and their process will be different from manufacturer Z, right? So one of the things that we're trying to do with this scoring system, that risk scoring system -- play with it, is making sure there's

a common ground. And so when someone says hey, we don't believe this particular vulnerability impacts patient safety, we can ask well, how did you come to that determination and there's some common ground that we can actually compare and say okay, hey look, I disagree with your characterization of this, right, and now you know exactly where you disagree, right? Right now we don't have that and so that's an important piece of this, as well, right, and we can't forget that.

And so at the end of the day, you know, I think everyone in this room, like, we're the choir, right? And so we're going to look at CVSS and be like, yeah, whatever. I really don't care about that score. But for folks outside of this room that aren't here at this workshop, that number means a lot, right? And, in fact, that number may drive something in their process, right? They're not going to do the analysis, they're not going to call 50 people and ask what's your opinion or what's the technology or the engineering behind this, they're not going to do that. They're going to look at the DHS/ICS CERT report and be like this is a nine-five and if the score is above an eight, we got to fix it tomorrow, right? So that's how it works in the real world, right? And so we need to move away from that, that's all I'm trying to do is just -- let's just move away from that, right?

MR. ENGLERT: So very good. And Jim.

MR. JACOBSON: So Art was talking about using CVSS as an input or using scoring, whatever scoring approach, as input and that's critical because the -- it's critical that there is a method of scoring that is compatible with the way it's done at medical device manufacturers where it's not necessarily security personnel purely providing this scoring, but often it's people with other specialties, people with product knowledge that are involved, also. So the easier that you can make it for those people to score and to use that as the input into the risk analysis, the better it is. So if it's easier, if it's more consistent between vulnerabilities, because we have different vulnerabilities that might be scored

differently but really come out the same from the standpoint of the impact to the device, it's that device-to-device consistency is there as well. But also talking about the vector, I think, that Penny was discussing before, if there is this extended vector that exists, it's a way that a manufacturer can communicate to the HDO exactly how we evaluated that vulnerability and they can inspect the details of it. Now, it doesn't have to be CVSS to do it that way, but if the scoring system exposes this information so that it can be consumed by the HDO as well, so they have the context clear, if there is -- if it gives us the ability to be specific about patient safety, that's a real plus as well.

So from a standpoint of a manufacturer, is it easier than the current process that we currently use, which is maybe a more naked CVSS evaluation or some other mechanism? We also need to make sure that it's reproducible, that in the evaluation there's more accuracy and precision and that the time it takes, because vulnerabilities are occurring all the time, so it doesn't impose an additional burden on the evaluation process.

MR. ENGLERT: So very good. And, Jason, we got a line here forming, so I'll give you a quick comment.

MR. TUGMAN: Sure.

MR. ENGLERT: And then I'm going to wrap it up and turn it over to the --

MR. TUGMAN: Agree. So the score matters only because of its misuse, that's why the score matters, right? Period. So what the rubric does is it allows the questions to be asked for the prioritization to begin, right? That's great, that is good. And it also does another thing that was actually mentioned in Panel VII, about where a vulnerability can also -- could potentially trigger, so for patient care or the ability for the network to operate, it might trigger an incident response, it might trigger legal action, it might trigger an insurance claim, right, a cyber insurance claim. So all of those things can be triggered and the rubric kind of helps that severity. So the scores matter because they're misused, therefore they

need to die in a fire, but the rubric is asking the right questions about adjacency and how to use that information to then assess the risk to your network.

MR. ENGLERT: Very good, very good. So a couple things I heard that I really like, right, context is so important, right? Scalability from a healthcare delivery organization is as big a problem on our side of the fence as it is on the other side of the fence, right, it's not solved everywhere. And you know, I agree with Jim as to a credit for patient care impact context. So very good.

Michael.

MR. McNEIL: Michael McNeil. Again, first I'll say, Jason, welcome to our ecosystem.

MR. TUGMAN: Thanks very much.

MR. McNEIL: And we can have conversations out in the hallway later about that. But first off, Billy hit it on the head, you know, a thousand percent, and I'm glad he said it because it wasn't coming up until I -- you know, that's why I stood up. The score matters. You know, I'm real world, okay, I have had in 2018 at least 18 coordinated vulnerability disclosures, the majority of them through work that we did with customers, also with researchers, and I can guarantee you that as soon as something is published through DHS/ICS CERT, it goes out with the Health-ISAC and any other ISAO, our phones start ringing off the chime based upon what those scores are and what was done in order with the remediation.

Now, I agree that we need to be able to align within a healthcare continuum within the settings that the solutions are and to be able to have, as Billy said, more consistency around how we're rating and looking at that vulnerability. But again, let's not kid ourselves because I'm dealing in today's environment and the current environment is I have a CVSS score, I utilize it not only in my development in my engineering processes because I feed that data around those vulnerabilities back into that process and we put that -- as we talked

about earlier, it's a component of any of the risk assessments, any of the testing that we do and the mapping that I have and even the building of my SBOM.

So, again, I'm all for moving to something consistent in alignment, but let's not fool ourselves, you know, to make it sound like CVSS score is -- you know, is ingermane at this point in time or it's being misused or it's not being, you know, leveraged effectively. It is what we have and we need to be able to make sure that there's appropriate alignment on it. And so as a manufacturer that I think has dealt with, you know, researchers and a number of different organizations and specifically with the increase in the volume from coordinated disclosure, I think I can weigh in a little bit and welcome to talk to anybody else, you know, around that layer. Thanks.

MR. ENGLERT: Very good, very --

MR. COLEY: And I would say, very quickly, Michael, to it bring it back to clinical context, all right, maybe the score does matter, but we're still thinking a little bit simplistically that one score fits all. If you have, let's say -- this is an example that Billy uses. If you have an infusion pump that's on the Internet, that's much worse than if it's on, say, a restricted network with physical locks around the infusion pump. Those are used differently in different clinical contexts with certain kinds of controls which should radically change how people interpret what the risk is.

MR. RIOS: Yeah, and I mean, I don't dispute that. I would just wish, like -- and like I said, we have a calculator up there at riskscoringsystem.com. The five most heavily weighted, you know, characteristics of a vulnerability are whether or not it directly impacts patient safety, whether it indirectly impacts patient safety, whether it impacts a diagnosis system directly or indirectly or whether it's a supporting system. And at the end of the day, I think if we were to release a DHS advisory or something else, it should tell us whether or not there's a patient safety implication with the vulnerability and right now it doesn't, right,

we just have the score. And whether someone uses it appropriately or not, I mean, I don't know. But it should say hey look, man, this vulnerability can hurt someone or hey, this vulnerability can't, right, but we don't do that for some reason. And so whenever we put out a score for a medical device or a healthcare system, that should be in there, especially if it's going to public, right, where people aren't going to do the analysis, they're going to take this document. That's the only information some people might have, right? So we should definitely help them understand whether there's patient safety implications with the vulnerability.

MS. LARSON: I appreciate what Billy and Michael said, I definitely second that. I also appreciate the love/hate with CVSS. I think that one of the differences of what we're saying is one is an output from a manufacturer and one is an input into an HDO and there's different ways in which an HDO should be in-taking the information and I understand the need for standardization in the output. So I just wanted to show that difference because I think we're talking about it as one thing and they're really two separate problems to tackle.

MR. RIOS: Yeah, that's a great point.

UNIDENTIFIED SPEAKER: Yeah, agree, that's a really good point.

MS. CHASE: Yeah. And, you know, one of the things we heard during our working group is the frustration of HDOs looking at CERT advisories that would have, you know, a CVSS score of 10 and then it would have the mitigations, and they'd say but I already have all those mitigations in place, you know, the device is segmented, I'm doing this, I'm doing that, and there was nothing in the advisory to help people assess what the effect of the mitigations they already had on place, in place, on reducing the risk created by that vulnerability.

MR. TUGMAN: So I hundred percent agree with that and that's where the adjacency, you mentioned the rubric, the blast radius, right, how many layers do I need to get to for

that nine to be affected, and how many fours can affect the traversing of that threat vector in to potentially reach that nine, right? So the adjacency and the defense in depth matter, compensating controls matter. It's an input of information. It is not a proscriptive order.

MR. ENGLERT: Very good.

Ken.

MR. HOYME: Thanks. Ken Hoyme from Boston Scientific.

I would love to just say I was up here to take a selfie to get on the -- every active Twitter feed that's going on about the meeting. But what I wrestle with, with a lot of the scoring systems, is what we're not talking about today is the postmarket scoring world. It is I have a system and when a vulnerability is identified it's at a precise location in a particular routine, a third-party code. You know, when we learned of Heartbleed, it was a buffer mismanagement in a particular routine. You could understand how that vulnerability would happen.

But a lot of the purpose of our meeting today is talking about what's needed in the premarket and, in the premarket, I don't -- if I learn that there's a buffer problem in the custom code that my coders have developed, we fix it. That's the solution for it. It really is about once it's out there how quickly do we need to fix it. So I wrestled with how much of these scoring systems you're talking about are relevant when you want to talk about classes of things. Okay, my mitigation premarket on buffer overflow is to put in static checking tools and things that enforce certain coding standards. So I'd be interested in the thoughts of the panel about how do we make that morphing so that we're doing the right things in premarket to set us up for post?

MR. MANION: If you can reduce, you know, things at the class level, please do so. That's far, far more efficient and far more risk reducing for everyone. I don't know if an internal development process, you know, if you have a list of bugs and you need to score

them internally, you might be able to leverage a scoring system, you might want your own thing. If you're just fixing them all, you know, that's easy enough, that's your answer, right, you have a one-character scoring system fix. Yeah, if you can do classes of stuff, do it. If you can do exploit mitigation, if you have a powerful enough device to do all the fancy randomization of memory addresses and things like that, you know, go for it. But, again, your point is correct, you know, postmarket, things out there, things found, how bad is it, that's what we're trying to talk about doing here. So different things, yeah.

MR. ENGLERT: Very good.

Billy.

MR. RIOS: Yeah. I mean, you know, any large organization I'm sure you've seen deals with this as well, right? You can't fix every bug. I tried that at Internet Explorer and on my first week, they literally laughed at me. But at some point you have to rack and stack as well, right? And so what you don't want is your developer rack and stacking the wrong bug, right, or working on one product when they should be working on a different -- bug fixes for a different product, right?

And so I think there is some value to having some kind of standardized rubric that takes into consideration clinical safety as opposed to vulnerability characteristics. Otherwise you're going to get an SBOM and say, okay, we have 20, 25, 100, 1,000 vulnerabilities. Which one should we -- which library should we update first? The one with the highest CVSS. See? So we're back to kind of square one, right? So we don't want to do that, right?

MR. TUGMAN: So yesterday we talked about threat modeling, right? These two things are related. So we do our threat model and we know our device, we know the threat vectors of the device, we know what we should be paying attention to and how we can prioritize based on the loss scenarios, based on the threat vectors associated with it, getting

to this point, which is correct, which ones to prioritize, not by number but by their impact to those vectors or their ability to impact those vectors.

MR. JACOBSON: Ken asked about the relationship to CVSS in the premarket condition and in that, it -- I know a lot of people have in many different ways tried to repurpose CVSS for things that aren't strictly for vulnerabilities and for gaps in functionality or for static code analysis findings and I agree completely with what Ken said, just fix it. That's the purpose of all the work that we do during the development life cycle. Life cycle is find problems before they get to the market and there are a lot of different tools and techniques to use it, but to overly rely on a scoring system during that process can just end up spinning wheels rather than accomplishing the quality that needs to be done.

MR. COLEY: I would suggest, Jim, however, real quick, that there's a difference between the implementation bugs and design flaws and at some point -- I mean, I have seen some use of CVSS in the premarket area. At some point at, you know, pretty low CVSS scores you have to sort of make a decision, am I going to have a device that's going to function properly even if it's not a hundred percent exactly secure?

MR. JACOBSON: Right. So you're talking about making product decisions, product-level decisions based upon some scoring that can occur. That's a different issue than dealing with defects or dealing with other functionality gaps that -- or designs flaws that come up during the development process.

MR. CORMAN: So just to build on this and tie it back to the premarket part because a lot of this is postmarket, and you touched on it, Jason, but the quality and caliber of a threat model is so vital to this, whether we're doing CVSS or a replacement for CVSS. I mean, it was very stunning when Billy showed that a medicine cabinet got a higher risk score than a bedside infusion pump that could kill somebody. So I've been sold on this, anyhow. But to other people's points, CVSS is going to get used whether we want it to or

not. So one method I see commonly -- you know, the Cavalry gives a lot of free advice to safety critical device makers. One mistake we tend to see is either they don't have a good threat model or even when they do it, they only triage against the threat model to lower a base score. So if they see it like it's above a seven or higher, they'll do their triage and they'll lower it, but that threat model works two ways. And one of the other mistakes people make is they don't look at chaining attacks. So with the OpenSSL Heartbleed, it was a 5 that is essentially a 10 because it's just a small leak of info, but the info leak became, you know, at admin rates or whatever.

So especially in safety critical, and we did this on our congressional task force, we didn't have a confidentiality, integrity, and availability column. We had a confidentiality, integrity, availability, and patient safety. And, yes, maybe they were done in certain cases, but instead of torturing the CIA trainer, you're torturing the CVSS. Any time we do our internal triage, for us, we say could anyone be hurt through any sequence or combination of events as our primary filter, in the context of the threat model. So if we've thrown in the threat model and if we don't get clarity on how good the threat model should be, you know, should it be an independent third party, should it conform to a certain standard. If we don't do a good job on the threat model, that up-and-down scoring goes away and the chaining visibility goes away.

MR. RIOS: Yeah. Actually, I want to add something. So if you look at the calculator that we have at riskscoringsystem.com, it's essentially that, right? So it's essentially confidentiality, integrity, availability and then a patient safety score and the patient safety score is like the heavy -- most heavily weighted item of the whole thing. And so I think the reason this is important, at the end of the day we have to agree on something, is because until we agree on something, like DHS and, you know, these other organizations, they're not going to put that measurement out on their advisories, right? And so CVSS is a standard

that a lot of folks use. That's why it's on the ICS CERT advisory, right, that's why it's going to be on every vulnerability report that you'll see that's made public. Once we come to an agreement on some rubric that says hey, we have to measure this piece, too, then maybe DHS is going to say okay, yeah, we can put that on our advisory now, right, or it's okay for a manufacturer to use that measurement when they're doing their risk scoring, right, it's okay for them to put that out there as long as we know how it's calculated, right?

So that's why I think it's important. And so I know there's a lot of different, kind of, viewpoints or approaches to doing this, but at some point in time we've got to pick one of these and say this is something that -- this is what we're going to use and that way folks outside of healthcare can use that to help people understand what the impact of vulnerabilities are.

MS. CHASE: And one of the things we do in the rubric in the CIA scoring part is flag places where there could be a potential impact on patient safety and we don't believe that CVSS itself is the right tool to make that patient safety assessment, but we're kind of saying, you know, this is the kind of data or process or function that is being affected at this point and it has something to do with diagnosis or it has something to do with therapy or it has something to do with some system-level behavior and we think there could be a potential impact on patient safety. So then you need to go and do your safety analysis and consider some of the other characteristics. And we actually had an interesting discussion last week at Archimedes about how we would integrate doing the vulnerability analysis with the safety analysis.

MR. TUGMAN: So you can go to my slide, I just want to -- I'm going to support his -- Billy's comments here. The other -- yeah, this one. So attributes to look for in a vulnerability scoring system is critical, right, it has to be standardized, we all have to agree on it. It has to have transparent characteristics and it has to be widely used in the industry

and it has to be accepted, right? So if we're going to do this exactly, we've all recognized, you know, the positives, negatives and all of that stuff, but those are the things that we have to make sure we do and we all have to use it. So it doesn't matter what it is, it's more about recognizing what a scoring system isn't and then as we do the patient care portion, then as that's rolling out, that is our opportunity to communicate that, right? The reason that I got into quantification was because Assizo (ph.), at a very large power company, asked me how many reds do I need to mitigate to get to a yellow, and I said wow, right? And that's where I began more work in quantification, so that's -- yeah.

MR. ENGLERT: Very good. And, unfortunately, we are out of time, so we'll just leave you with this. As you go to break, when you communicate with your friends, the input/output thing, we need to bridge that gap, we've got to figure out how to bridge that gap, right? Take the vulnerability score on a device and contextualize it with the risk within the environment that that device sits. So take that and let's go solve that and come back next year and have it done. Thank you very much.

(Applause.)

MS. ZUK: So before we move to the breakout session, I wanted to provide a little bit of framing on CYMSAB. Can people hear me? A little bit? So last April, FDA published the Medical Device Safety Action Plan, and in that action plan there was an action about exploring the development of the CyberMed Safety (Expert) Analysis Board. This is intended to be a public-private partnership complementing existing coordinated disclosure and response activities, not something that would take the place of those, and to include a broad range of experts, including hardware, software, networking, biomedical, and clinical experts. So we're very excited to have this breakout session to get more stakeholder input on this concept of the CYMSAB. The goals of the CYMSAB are really to assess and validate high-consequence vulnerabilities, which are high-risk, high-impact vulnerabilities, to

evaluate the patient safety risks, to adjudicate disputes, to assess mitigations, to provide consulting to organizations that might request it, and also to have a go-team concept to be -- you know, actually go to a physical space to assess vulnerabilities. And we certainly heard a lot of needs over the last 2 days for something to help us validate vulnerabilities quickly, particularly when they are high-consequence vulnerabilities.

And so thinking with all the minds in this room about how can we move forward with this, who are the right experts? What would a go team mean, where would they go? Could the concept of labs come into this? Could we take advantage of existing labs that might provide a clinical environment to be able to test? So as you move to your breakout groups, we've outlined a number of questions for consideration and we are very encouraged to have everybody really think about this in our next breakout session and you will definitely be contributing to the future here. And Aftin wants to add a few things

DR. ROSS: Thank you, Margie. So we had on our last panel a lot of discussion related to, you know, risk scoring and how do you look at risk and how you quantify that. And so one of the things that we do think that something like a CYMSAB might be helpful for is to Margie's point, trying to help us get to an understanding quickly about the potential impact or high-consequence, high-impact vulnerabilities such that steps can be taken to try to address those very quickly. That's really the challenge area that CYMSAB is seeking to address, is to try to think about how we can do this even more quickly, especially when you're thinking about high-impact, high-consequence vulnerabilities.

One of the things that we think it is very important, though, for everyone to understand is MITRE has been doing some exploratory work in this space for FDA with some seed money that we got from -- or seed funding that we got from the Commissioner's office. However, if there was not a congressional appropriation there would not be a CYMSAB. So right now this is all an exploratory stage, if you will, proof of concept to

understand if there were to be this public-private partnership, what value add would it have for the community? What are the types of things that would be of benefit for this group to do to work on that would help us, as a community, move forward? Or that (b), some of the things, you know, Margie was talking about in terms of adjudication, whether it has to do with the communication piece, we've heard a lot about that here, about trying to take on that cybersecurity concern and trying to push it out in a way that's understandable for those recipients. And so that's really one of the things that we're going to want to do in these breakouts and we've tried to come up with a couple of different categories of questions to try to help us understand what the potential role or value of something like the CYMSAB would be.

Now, with that in mind, we do again have up the breakout groups, so your breakout groups, for the most part, should be the same as you had yesterday. If you were not here yesterday and today's your first day with us, you will get your breakout group by looking at your badge. So we have a majority of the members again are here in the room, but there are a couple who are in other rooms, and so you should go to where you were yesterday. So, again, there's a couple of rooms that are outside and to the right, near the bathrooms and then there's also a room behind us on the left.

And we had Group 20 as well, your breakout room got moved for today. It's going to actually be in Section A, where we were yesterday. We also had learned that some of the staff that were thought to be in Section A are not going to be there today. So if you find, for some of those breakout groups that are on the edge, that you're a little crowded, we do have space for two or three more groups to go into Section A as well, if that would be of benefit for the dialogue and the discussion.

We're going to go ahead now and get ready to break for the breakouts. We're definitely very much interested in what will come out of those discussions, and thank you

for helping us to understand what you think might be a value add in this space.

(Breakout Session from 12:06 p.m. to 12:55 p.m.)

(Whereupon, at 12:55 p.m., a lunch recess was taken.)

AFTERNOON SESSION

(1:47 p.m.)

MR. GARCIA: Okay, everybody, let's get started and please have a seat. All right, good afternoon. My name is Greg Garcia. I am the Executive Director of the Healthcare Sector Coordinating Council, the Cybersecurity Working Group, and I'll give you a quick briefing on what that is before we get started with our panel. We are with the Establishing Trust, Embracing Transparency, Increasing Resilience: Best Practices and Tools. If that doesn't shake you out of your postprandial torpor, I don't know what will.

(Laughter.)

MR. GARCIA: We have a great panel. We're going to split it up again, half and half, with a lot of discussion about some of the tools and then we'll jump to the second half to talk about some of the standards that may animate some of those tools. The Health Sector Coordinating Council, show of hands, who knows what it is, even vaguely?

(Show of hands.)

MR. GARCIA: Okay, not quite half. Very quickly, the Healthcare Sector Coordinating Council is one of 16 critical industry sector councils recognized under presidential executive order, and you think of financial services and telecommunications, electricity and water, transportation, like that, and we are all organized in a public-private partnership with government and we -- in our case we work very closely with, of course, FDA and Health and Human Services and the ASPR division, and we seek to address those cross-cutting challenges, in our case, cybersecurity, but there are physical security issues facing every industry sector as well. We try to address those cross-sector challenges from a policy and strategic, longer-term strategic way versus the ISACs. The Health Information Sharing and Analysis Center focuses on the same kind of critical infrastructure protection issues at a tactical and operational level. So we are two sides of the same critical infrastructure

protection coin. In all of these critical sectors, the protection, the preparedness planning is overseen in general, broadly, by the Department of Homeland Security. So this is a public-private partnership. The Cybersecurity Working Group consists of 200 organizational members, about 400 people representing those 200 organizational members and that includes government representatives as well, so it is truly a joint cybersecurity working group. We have on this panel two members of our executive committee, Erik Decker and Ashley Woyak. It is chaired by Terry Rice, the global CISO for Merck, and vice chaired by Theresa Meadows, the CIO for Cook Children's Hospital System in Texas.

So let's get right into this, and I'll just ask, starting from my left down to the right, to have each of our panelists introduce themselves and then we'll launch into questions.

Colin.

MR. MORGAN: Sure. thanks, Greg. Colin Morgan, Director of Product Security at Johnson & Johnson and also a member of TG1B, the Medical Device Cybersecurity Working Group in the Healthcare Sector Coordinating Council.

MR. DECKER: Erik Decker. I am the Chief Information Security Officer and Chief Privacy Officer for the University of Chicago Medical Center, and I'm also the industry lead for TG1F under the Healthcare Sector Coordinating Council. This is the Health Industry Cybersecurity Practices document that was released on December 28th.

MS. CHUA: Good afternoon. Julie Chua from HHS Office of the CIO. I am the Risk Management Branch Chief and also the federal lead for the Health Industry Cybersecurity Practices document, 1F.

MS. WOYAK: Hi, I'm Ashley Woyak. I'm a business information security officer at Baxter, and since we're representing our task group, I am a representative of Task Group 1B.

MR. McDONALD: I'm Kevin McDonald from Mayo Clinic, and I'm one of the co-chairs

of Task Group 1B.

MR. SUÁREZ: Hi, my name is Rob Suárez and I'm the director of product security at BD, and I'm also a co-chair for TG1B, Medical Device -- Med Tech Cybersecurity.

DR. ROSS: Hi, I'm Aftin Ross. I am at the FDA in the Center for Devices and Radiological Health, and I am also co-chair for 1B, and I'll also be speaking a little bit about the International Medical Device Regulators Forum.

MS. JUMP: My name is Michelle Jump, and I am vice president of cyber program initiatives at Nova Leah. I am not a co-chair of 1B.

(Laughter.)

MS. JUMP: I feel like I'm which one is the odd one out. I actually am a U.S. technical representative on ISO/TC 215 Joint Working Group 7, and so I am a project lead for a new standard called 81001 and participate in a large number of international and domestic standards.

MR. GARCIA: Thank you, Michelle. I'm sorry, I should have warned you about 1B, 1F, what are they talking about? We have 13 task groups in the Cybersecurity Working Group and for reasons I won't go into, we have a 1A through 1F and then we go on to Task Group Numbers 2, 3, 4 through 8, all very specific outcome oriented, deliverables oriented task groups and you have two of the task groups here today representing some pretty outstanding work that we have come together as a sector, across subsectors, to produce guidelines and resources for the broader healthcare sector.

And we release these within 30 days of each other. December 31st, right, for 28, 29 -- 28, the health industry cybersecurity practices, which are devoted toward hospitals' best practices for cybersecurity and then just this Monday we released, from Task Group 1B, the Medical Technology -- or Medical Device and Health IT Joint Security Plan. And I'm going to ask the co-chairs, starting with the first release, HICP. It's okay to call it hiccup. The health

industry best practices. Erik Decker will start off, and Julie, you can play backup.

MR. DECKER: Thanks, Greg. So just a kind of quick orientation on this. So this is a directive that we had under the Cybersecurity Act of 2015, Section 405(d). More acronyms for you. That ultimately called for aligning health information security practices across the healthcare industry. It's the sister statute to the task force report, that was 405(c), the task force report that was released in June of 2017.

So we came together as an industry and government partnership, about 150 individuals, and to be concise about this, what we decided to do was focus on what we felt were the top five prevailing threats that healthcare industry providers, HDOs, face although what we produced could be certainly extended beyond the HDO space. And then ultimately, the 10 cybersecurity practices that we felt would mitigate those threats.

Within the 10 practices there are 89 sub-practices. It is a big voluminous document, it has four volumes, 250 pages total. We've had more than 200-plus individuals go through the peer-reviewing process in total with -- between the task group numbers and the peer reviews that we did across the country and ultimately, what was produced was what we affectionately call hiccup. So please do call it hiccup, is what I would say.

(Laughter.)

MR. DECKER: You know, but ultimately what this is, is we broke this up between three different organization sizes, small, medium and large, pretty self-explanatory, as well as all the various methodologies to help individuals guide themselves and figure out where they fit. And then within the small, medium and large, the main document first talks about sort of the call to action and brings cybersecurity into layman's terms for the C-suite and the physicians and the uninitiated and then the technical Volumes 1 and 2 really dive into how do you actually do any of these things. It's more like a recipe -- a cookbook and a set of recipes for how you actually implement these practices if you're a small-sized

organization versus a medium versus a large, because obviously the resources are different, you know, based on how you're set up.

So, Julie, do you want to talk about the partnership?

MS. CHUA: Sure. So in line with what we're calling our panel, so transparency and trust, I think this was an excellent example of how government and industry, when we do come together, we come out with a robust and pretty good document that a lot of our stakeholders will be able to use. So I wanted to highlight the makeup of the task group because I think that's a very important and quite unique aspect of the HICP document.

We had medical professionals, we had, for example, nurses, nurse practitioners, home health providers, rural and community health participants who provided input into this document, and that includes also our CISOs and our CIOs. We had the opportunity to actually reach emergency management professionals. So we really tried to make sure that this document was not just from an IT or a security perspective. We really wanted to make this come out as this is the healthcare sector status today when it comes to cybersecurity, from awareness to the lack of awareness of what we are trying to do.

And one thing that is also quite unique with this partnership that we did is we had a rigorous assessment process, we had peer reviews, we had -- pretesting is what we called it throughout seven cities across the U.S., in person and then in addition, I think, about six or so virtual sessions and these pretests were for those participants of these focus groups to look at the first draft of the document and tell us what they think. Did we meet the mark? We gave them the objectives, we gave them what we wanted this document to be and they provided us pretty candid feedback which was very helpful and that's why what you see today is something that is, I think, quite evident that it came from a lot of different perspectives.

So two things that I would like to close in terms of, you know, making you aware of

how we produced this document. There is a main document that is very plain language. It focuses on the cybersecurity status of the health sector today. It focuses on real stories that we reference of cyber attacks and incidents and why it is important. And you could give this to your physician or your dentist and they will understand what we are talking about.

Another thing in the main document is -- and this is because of the input we got from industry stakeholders, is we have these threat pages that you can actually just print out and put on your desk, put on your workstations and you have quick tips to remember to address the five threats that have been identified by the task group.

The other thing is the technical volumes, so you cannot have a cybersecurity document without a technical volume. So I think the task group did a good job with parsing that through and dividing it into a main document and technical volumes for small and then medium and large. I think there's a lot of information out there that exists, but I am confident to say that this one actually does a good job with addressing the whole spectrum of our sector, non-IT, non-security professionals who can actually talk together now because of this document.

MR. GARCIA: All right, thank you. All right, now let's turn to our second task group, 1B, which created the Medical Device and Health IT Joint Security Plan. This is co-chaired by Rob Suárez and Kevin McDonald along with Aftin Ross from FDA, and I think what's notable about this is, in fact, the co-chairs, the two major stakeholders in this challenge of medical device security, both the vendors and the hospital systems got together to co-chair this to find a common solution and I think it was a big success. So I'll turn it over to whichever one of you would like to start and take it away.

MR. SUÁREZ: I'll get it started. Thank you, Greg. So with Task Group 1B, let's start maybe 2 years ago, a year and a half, 2 years ago, there was a report called the Healthcare

Industry Cybersecurity Task Force Report which outlined a number of different challenges specific to the healthcare industry as it relates to cybersecurity recommendations, imperatives, for improving or addressing those challenges. One of them was Imperative 2, which described the need to improve cyber resilience for medical devices and healthcare IT. And so in Task Group 1B our group focused on building what is a voluntary framework and plan for, again, incrementally over time improving cybersecurity, not just as a medical device manufacturer or healthcare IT vendor but also as a healthcare provider and consumer of these technologies.

And so the idea actually, I think, blossomed also out of a small group of medical devices manufacturers that were exchanging ideas of, you know, how can we share some of our practices, open source our product security frameworks and perhaps come together with something that's even better than what we had before, and then also distilling a lot of the industry standards and best practices, again, into our own organizational practices and quality management systems.

And with that, an initial draft of the Joint Security Plan was put together, but then we realized we can't do this without healthcare providers and certainly can't do this without our regulators and policymakers, industry associations. And so we had a number of different healthcare providers contribute to the drafting process of the Joint Security Plan.

What is, I think, different about the Joint Security Plan is -- and makes it unique is that it's not a standard in itself, it's actually referencing a lot of industry standards, but really providing an overlay to those standards and it's demonstrating how it's applicable to medical technology. Whether it's static code analysis, vulnerability scanning, risk assessment, design requirements for security, what can a medical technology vendor do to adopt these best practices and almost copy/paste the Joint Security Plan into their respective quality management systems and also backbone and leverage existing traditional

pillars to quality management that exist today, for example, design control, complaint handling, and risk management. And so I think, through that effort, you'll see in the Joint Security Plan a number of different sections that show how you can incorporate these practices but also, an appendix with some helpful templates and also examples, again, of security documentation for your customers that you could use or even during market submissions. There's also sections that describe other types of authoritative sources for some of these best practices.

Yeah, and the last thing I'll mention is that it's a voluntary framework so you can choose to do this, you can choose not to do it and you might be asking yourself now, then, what's the point, no one's going to do it, right? Well, this is where the work starts in a plan, is that you take this document back home to your respective companies and you show your executive leadership that the majority of -- or I should say some of the largest medical technology companies and healthcare providers in the world have come together and actually agreed on something. They agreed on how to do security throughout the life cycle of medical technology. That's what happened in the Joint Security Plan. And healthcare providers will ask their manufacturers, their healthcare IT vendors, how are you doing against the Joint Security Plan and adopting these different practices? I'll ask my other co-chairs to chime in.

MR. McDONALD: So what was attractive to me as a -- from an HDO, is that it sort of includes the wish list of all the things that we have expectations of that vendors go through to be able to develop and produce a secure-by-design product. Back to, you know, it is a voluntary framework, but when you come calling at an HDO, these -- by following a lot of these processes, it makes it pretty doggone easy. I'm still going to send you that, you know, 4,442-question, you know, questionnaire and I'm still going to ask you to do the network diagram, but those are all things that are outputs of this, those are all things that will just

ease that journey to be able to do the right thing. And from what we've seen from the companies we've worked with, this just produces a more -- by following a lot of these processes, this allows you to produce a more secure and a better quality product and which we want, you guys, all the vendors in the room want, and it really will just help the whole ecosystem as we go forward.

MR. GARCIA: Great. And before I ask Aftin to discuss what's happening with FDA and their part in this, just to note the cross-fertilizing nature of these two resources, that we've been talking a lot about a software bill of materials over the past 2 days and for example, one of the things that the HICP best practices say is that hospitals should be asking for a software bill of materials from their vendors and the Joint Security Plan is saying manufacturers, you ought to be offering to your customers a software bill of materials. And so they're cross-referencing each other and I think that's really particularly important, it's a force multiplier effect in this cross-sectional effort.

MR. DECKER: Yeah, I'll jump in a little bit on that. I just wanted to pin that down as well. So the HICP has one of the practices about -- it's about medical device management from an HDO perspective and we worked with our partners on the JSP side and provided input on both sets of documents both ways, because what we're looking for here is the JSP to be sort of the manufacturer side of the house, the HICP side to be the provider side of the house, and the two married together around the shared responsibility about how we can manage medical device security and patient safety. So it's a great opportunity and it was a great collaboration.

MR. GARCIA: Yeah. Okay, and then I'd like to hear from Aftin and while she's talking, I'd like both Baxter and Johnson & Johnson to be thinking about how are you going to be actually implementing within your enterprises the Joint Security Plan? But Aftin, you've got some interesting things going on at FDA.

DR. ROSS: Right. I actually think it might be better if Ashley and Colin, since they were engaged in the JSP, to talk a little bit about that because it actually does feed in nicely to some of the things we want to talk about in terms of some international harmonization.

MS. WOYAK: So I think there are two huge benefits. I know I've purchased paid in this working group since early on, so I've been a part of working through it and integrating within our organization the key fundamentals of what came out of the document.

But I think one of the key takeaways is, one, a really good check so that everybody is working towards the same objectives, thinking about the same key things they should be doing within their organization. And I think of it almost like a toolkit because we all know that the people who are sitting in this room may have a varying level of maturity within their organization and if you're a less mature organization, this document provides a lot of great opportunities for you to know what -- what's the right way of going about doing certain things, procedures. It really is full of great content that any organization can leverage and make sure that they're doing the right things and on the right path.

MR. MORGAN: So from our perspective, as Rob talked about, this was, you know, a year's long effort, meaning you probably see it in the hallways here. A lot of us had been working together in this space for a number of years, working to improve cybersecurity across healthcare. We're constantly talking either here or on the phone or at other events, sharing what we're doing, sharing what we're building, and bouncing ideas off one another. And, really, a handful of us have been talking for a while about how do we get the work we're doing out into the public domain.

Obviously, we have our own legal considerations that we sometimes bump into and by doing something collaboratively under the industry -- you know, Healthcare Sector Coordinating Council, it made it, you know, just smart and honestly the best way to get this information out there. So rather than it being company A producing their materials and

company B producing theirs, it was a collaborative effort to share what we're doing. You know, some of the information in that document came, you know, straight from our organization, straight from other organizations. Some of our frameworks look very similar, some of our language in our software procedures might look similar. And really, you know, there is an infographic that went along with the JSP, which they call theirs HICP, we call ours JSP. I could hashtag -- JSP is what I like to tweet out there. Be at that training, that would be great.

But the infographic had some pretty interesting data on it, you know, it talks about the number of medical device manufacturers that exist, I think that might say somewhere upwards of 7,000, and how 80% of medical device companies are fewer than 50 employees. Some of them, three, four, five employees. Some of them working in a garage trying to create an amazing lifesaving technology and their job is to get that device to market. Not all of them had the opportunity or the ability to build security programs, to have dedicated security professionals to focus on this. And frankly, those small companies don't have any idea where to start and I know that because we acquire them and it can be quite a lot of security debt that we acquire and we have to figure out how to clean up.

So at the end of the day, the JSP is a mechanism to help move that needle in healthcare cybersecurity for medical technologies to start ensuring that all of these companies with brilliant ideas, that are going to create lifesaving technologies to enable better patient care, can be done from a safe and secure perspective. So for us, the JSP is really about getting information out there for people to be able to use in a format that's easy to follow and examples that people are using today that they can leverage.

MR. GARCIA: Exactly. And the same with HICP, to really target a lot of those smaller to mid-sized hospital systems that don't have the resources or expertise, this is a place for them to start. And now we've got, you know, two companies here on the JSP that are

global companies and Aftin, as you mentioned, this is a global enterprise and it's a global issue and you want to talk about the --

DR. ROSS: Yeah, so one of the things we hear a lot from regulated industry is that it's challenging for medical device cybersecurity because they operate in various jurisdictions and so was there a way to try to harmonize on what we're thinking about with regard to medical device cybersecurity globally. And so there is an organization called the International Medical Device Regulators Forum and really the purpose of this group is really trying to accelerate the harmonization and consensus building across regulators and across the globe.

And so one of the things that came up in this group was this topic of medical device cybersecurity and it was decided that they would start a workgroup, and though the management of the Regulators Forum is, as the name indicates, regulators, the workgroup can be -- have membership from a broad range of stakeholders including industry, healthcare providers, etc. And so within this particular workgroup, which FDA and Health Canada are the co-chairs for, we actually do have industry partners that are participating along with the regulators.

And really, what this group is looking to do is to come up with a consensus document that helps provide guidance globally as it relates to medical device cybersecurity and some of the different topics that would be of value for our stakeholders, so the ideas we've been talking about here with regard to, you know, the shared responsibility and even making sure we're all talking the same language, what are some of the common definitions that are important for all of us to have a baseline understanding so we can communicate across the various jurisdictions. And, of course, you know, information sharing, which we know is a key hurdle here.

So we'll work in the coming year on trying to come up with a document that tries to

reflect the learnings from across the globe as it relates to medical device cybersecurity and give a good starting place for medical device manufacturers and healthcare organizations, as appropriate, to have a good starting point and try to make things a little bit easier both for healthcare providers but also for medical device manufacturers who service various constituencies across the globe.

But I mentioned that we -- this is an international group, so we have international regulators and I thought it would be helpful, part of the reason we wanted to have Michelle here is because when we had the phone call, she brought up some of the things that are happening with some of the guidances that have come out recently from other countries. I know that both Australia and Canada have recently come out with some guidance and so we did want to just talk a little bit about how the conversation process is going to take that into account.

MR. GARCIA: Okay, I think we just --

(Off microphone comment.)

MR. GARCIA: What? Oh, I'm sorry, I didn't hear that.

MS. JUMP: That's okay, Greg. Thanks, Aftin. Yeah, so just real quickly, one of the things from a global perspective, many of the manufacturers in the room do try to look at the global environment and we've seen, as Aftin mentioned, Australia recently releasing a guidance for comment, as did Health Canada. We're seeing new expectations in China and Japan, across Asia, and it's very important to see IMDRF taking a leadership role in this space because what we don't want to do is have guidances that are asking for lots of different things. The good thing is, is that there does seem to be some harmonization in looking for SBOMs and looking for a risk-based approach from these other global guidance documents, but I think everyone would like to see one whole consistent approach to what's expected. One thing to look at there is the MDS2 revision. Some of the global

manufacturers have been trying to help circulate the understanding of how MDS2 revision can help harmonize the information that's being provided from the manufacturer to the healthcare organization and it looks like that's going to be a really great tool and so keeping an eye on MDS2 is not only for U.S. centric, but also looking at how Europe may be accepting that as a common vehicle of information exchange, and some other jurisdictions that are looking at that.

So those are great things to be seeing moving forward in a consistent amount of information because I think, from everyone's perspective, it's a lot of information to pull together and trying to get that information to be consistent, just looking at the U.S. and the number of information security agreements that are going through, and I'm sure the manufacturers can speak to that, is frustrating imagining, you know, cyber awareness increasing globally and asking for a whole other set of -- new and unique sets of document requirements. So I think that's a really important thing.

If I could have just one moment to give one example. Dr. Shuren and I had actually talked about this, before this IMDRF issue had come up, because I had mentioned that it's been great to see what FDA has done in the U.S. for understanding that oftentimes you need to allow manufacturers to get out and actually start patching vulnerabilities because patching is more important than perhaps putting in documentation that -- around going out and touching those devices. And it's been great to see FDA's understanding that getting out and patching is a critical part to this and providing guidance that you can go out and patch and you don't necessarily have to typically put in a 510(k) for vulnerability patching.

But as you start to go outside the U.S., you realize that some of those regulators have not had those conversations and trying to go out and patch devices out in the field in some of these other countries is extremely difficult because they haven't made those assessments and those allowances to be able to perform regular security updates on

products in the field versus here in the U.S. where those processes have been outlined pretty clearly in guidance for us. So I don't know if any of the other manufacturers want to speak about some of those challenges but I think, as we look at the harmonization, it's not just necessarily the communication of information but it's also the practice of getting those products patched in the field.

DR. ROSS: And I would just want to end by saying that that is part of the point of doing the guidance document from IMDRF is to try to address these main facts or challenges, so that is some of the discussion that we're actually having within the workgroup, what are the challenges, so that we make sure we produce a document that helps to address those.

MR. GARCIA: Okay, great. Thanks. And, Michelle, my apologies, I didn't mean to jump you, I was paying attention to the time and my next question and Aftin was done and I thought oh, it's my turn to talk.

(Off microphone response.)

MR. GARCIA: I have postprandial torpor, I guess, myself. How much time do we have now? Are we moving on to the next half?

(Off microphone response.)

MR. GARCIA: Okay, there's a question.

MR. TUGMAN: So hi, my name is Jason Tugman, Axio. So this is actually to Erik and Julia, it's more just a comment. I'm a chair of a working group for the Department of Energy to update this, the C2M2, cybersecurity capability and maturity model. And then, actually, my colleague here, she represents pipeline trade associations. She and I and others are leading the effort for updating the American Petroleum Institute's 1164 standard, which is -- we're are going to include an IoT component to that. One of the things that we have with the API standard that we're drafting is making it real to the people that are also working on

wellheads, on pipeline, right, they're OT operators. Two weeks ago in Houston and again, next week, we're working on the architecture, how we frame our standard, that standard and I just want to say publicly if anybody has not read the HICP, I read it with great joy. It was weird, I'm a standards nerd, but it, I think, set the model for how to make it real and I gave a whole demonstration of how we can apply the architecture of how you frame the pages into potentially the API 1164 standard. So I'm just saying if anybody's not read it, it really is impressive what you guys have done, so I just wanted to call that out publicly.

MS. CHUA: Thank you for that comment. So the format and the layout of the main document was done on purpose. We wanted to make sure that, essentially, our -- one of our key audiences for the main document were the medical practitioners, the physicians, and they are very keen on, you know, a journal type of look. So we got that positive feedback, too, and hopefully that carries on as we go.

MR. DECKER: I just want to take a quick thank you and I also want to say this is not a standard nor a baseline nor a --

(Off microphone comment.)

MR. DECKER: Right.

MS. CHUA: Yeah.

MR. DECKER: Yeah, we want to be very clear about that.

MS. CHUA: Yeah.

MR. DECKER: Thank you.

MS. CHUA: Thank you, Erik. So it is a resource, that's what we are calling it. It is voluntary, it is mandated to be voluntary, and it is no way --

(Laughter.)

MS. CHUA: So that's the first thing you need to know, it's already mandated, so HHS cannot make this is a requirement. Number two, the task group really wanted this to be

something of a resource so that everyone can get their foot on the ground and start ruling.

MR. GARCIA: What's next? How are you -- I mean, it's out there now, what do we do with it?

MS. CHUA: I knew you were going to ask that, of course. So there are some practical things that we are doing right now. We have a fireside chat between Erik and myself on February 6 and 8 and if you want to get on that distribution list, it is cisa405b@hhs.gov. So you can email that resource mailbox, we will make sure you are on that distribution list and any other updates to take up in 405(b) specifically.

The other thing is we do have a threat series all through March and April and essentially, we go through each of the five threats and we get into a deep dive into the 10 practices that the technical volumes address and put forth.

So those are two very immediate things that are happening. Erik and I and some of our partners in crime are also going out and speaking about this, raising the awareness and really pushing for the adoption and the implementation of this, because this is a great document but if no one hears about it, no one knows about it, then it will just sit in our inboxes. So we are trying not to do that and we are aware that that is a risk.

And we do thank, from an HHS perspective and representative, we want to thank the HSCC for all the pushing and all the awareness of the two documents, the HICP and the JSP, because without our industry partners and the association members who are a part of that, we would not be actually here today or we would not be speaking of these engagements where we are being invited to talk about the document.

The third next step is Version 2.0 and/or another resource that can be under the umbrella of the 405(b) mandate. So just to clarify that, 405(b) calls for aligning health industry security practices. That's a lot, and if you want to chunk it into different topics, I think the task group has that on their plate to decide on. So Erik can talk about --

MR. DECKER: We start tomorrow.

(Laughter.)

MS. CHUA: I know, we reconvene the old and the new members of the task group tomorrow, a virtual session. There is still time to sign up. I don't think there is a max in a Webex, so we do -- would like to welcome especially this community. We have had a few medical manufacturers and medical device representatives and we need more.

MR. MORGAN: Hey, Rob and Kevin, are you ready for JSP Version 2.0?

(Laughter.)

MR. SUÁREZ: Yes. So we do have, by the way, on the healthcaresectorcouncil.org webpage, there is -- you'll find there an email address where you can send your feedback on the Joint Security Plan. I believe it's jspfeedback@healthcaresectorcouncil.org. And certainly that will go into Version 2.0. Just like any roadmap that you may have in your respective organizations, the JSP is intended to evolve over time and to adapt. And so we expect -- here's a great thing that all of you could do, perhaps, even if you don't have a single person dedicated to cybersecurity today.

Take a look at the JSP, there's a section that's called Evaluating Maturity Against the Joint Security Plan, and it is a way to how to measure yourself against all these different practices in cybersecurity for medical technology and determine how you're doing, in general. It's using the CMMI as a scoring system really to rank yourself. It's not one single score, it's not -- so please don't hate the score. You know, it's a number of different metrics, okay? And also share that with your leadership. The reason why is because I'm almost positive, without even knowing them, I'd like to believe that your companies and your C-level -- you know, your C-suite are genuinely good people, good human beings, and they want to do the right thing. They might just not know how to focus their efforts and

prioritize things. The maturity evaluation allows you to focus on here are our deficiencies. It may be bad across the board and you know what, at least you know where you can focus your investment from a security perspective and whether or not it's building up risk assessment processes or it's incorporating static code analysis, vulnerability scanning, into your development and life cycle.

And, hey, you might even think all those things cost money as well. Well, actually, the way that the JSP outlines risk assessment you could do with no funding whatsoever, you don't need to hire, you know, a consultant to go do that for you. It's, in very simple terms, design requirements. It shows you how to prioritize those design requirements in your design input requirements as manufacturers, by the way, and healthcare IT companies, very relative terms to what you may already be doing today. And so I think those are some really good things that you could do immediately.

MR. GARCIA: Great. Okay, thank you, Rob.

And that ends this portion of the panel discussion, so I'll now ask Anura Fernando and Brian Fitzgerald to come on up and while they're doing that, just know, both of these major documents we've discussed, they are living documents and we're going to need your help in implementing them, getting the word out.

If you are not a member of the Health Sector Coordinating Council, you should be. Any medical device manufacturer, healthcare providers, it's your responsibility to be a part of this broad collaborative. If you're not a member of the Health-ISAC, likewise, we have a collective responsibility to secure our systems across the healthcare sector. So please see me if you're not a member of the Sector Council and we'll get you enrolled and get you active.

Now, for the second part of this panel discussion, we're going to be talking about the standards, standards in healthcare, and Michelle gave us a teaser on that, thank you. So

why don't we start with Anura, to just introduce yourselves, and of course, Brian has been here before, but go right ahead. So Anura.

MR. FERNANDO: Yeah, thanks. Anura Fernando, I'm with Underwriters Laboratories, I'm their chief innovation architect for medical system security and interoperability.

MR. FITZGERALD: Brian Fitzgerald, Office of Science and Engineering Labs here at CDRH.

MR. GARCIA: Okay. Well, this is pretty open-ended. I mean, standards can be the discussion of weeks of -- but, Anura, why don't we start with you and what are some of the activities UL is doing and where you sort of fit into the broader ecosystem.

MR. FERNANDO: Sure, definitely. So, you know, as both a standards development organization within UL as well as a certification, testing and certification organization, we really have two major divisions of our company. As a standards development organization, we don't just develop UL standards but we participate in international standards and we try to coordinate things. I think you can probably tell from the size of this panel just how popular standards are.

(Laughter.)

MR. FERNANDO: But one of the things we try to do to make your lives easier is you all have to comply with a core set of standards, typically, when you're dealing with safety and, you know, quality of your product and those kinds of things. And so by participating in international standards operations and even with other domestic standards developers like AAMI and DTSec and IEEE and, you know, a variety of others out there, we come up with a way to coordinate the requirements so that, as manufacturers and as consumers of these requirements, you can actually minimize the impact of, you know, what you might face when you see dozens and dozens of standards out there that you may be able to use. And

so with security, we took that same kind of approach. You know, we saw that in the world of IEC there was a whole body of work going on with the 80001 series of standards and now 81001 that Michelle is leading, and what that showed us was that from a risk management point of view, a network security related risk management point of view, that was sort of the user perspective of this. You know, what if this ends up in the hospital, how is the device integrated into the hospital?

Then we said if we can characterize that context of use and understand the risk considerations there, then it's a matter of again looking at what the medical device manufacturers are already using, so they have to have the quality management system for systematic defect reduction and software quality is sort of the overall tenet, you know, that security falls within.

And so if you look at how the quality management system encompasses the risk management process and the software development life cycle processes, then you start to build a set of requirements that integrate existing processes that manufacturers have that need to be extended to deal with, you now, some of the newer issues of security, but they fundamentally still align with a lot of the processes that manufacturers already have to make that delta sort of minimal.

And so combining the risk management processes, the software development life cycle processes, under a quality management system from a device manufacturer perspective and then putting that into the context of IT risk management and device integration considerations from the HDO perspective, you then have a good way to trace what are the risk considerations in the hospital, how do those relate down to what the device manufacturers are doing.

And then the next key is disclosure. So, first, you want to test your devices, you know, all the things that Rob mentioned on the previous panel, that expert code analysis,

binary analysis, using tools to help verify SBOMs and things like that, and when you take all of that test information and couple it with the things that you're already doing -- I made a comment earlier this morning about the fact that manufacturers have a lot of test data that just comes from their safety testing when you do EMC testing and things like that.

And so we wanted to look at how can you leverage that. You know, if you see an aberrant behavior of your product when you're doing a frequency sweep during electromagnetic compatibility testing, do you alert your security group that hey, there's some kind of weird behavior here, how does that relate to security? I won't ask for a show of hands, but I'm guessing that there probably aren't a whole lot of folks that are doing that right now.

And so testing was one of the biggest pieces that was missing when we looked at the landscape of security standards as part of the evolution of 2900 under the 2016 Cybersecurity National Action Plan. At that time the GSA, through DHS, drove some activities that looked at the landscape of standards and said what's missing, why do things like the OPM breach still happen? And part of that is that there weren't a lot of good verification mechanisms or testing mechanisms out there. And so those kinds of things have really factored in to the development and evolution of these standards, like 2900, that are tie-ins to IEC and ISO standards and so forth.

So in a nutshell, that's kind of where we are. You know, it's a voluntary standard just like, you know, other consortia-based documents and so forth are voluntary. They are FDA recognized consensus standards, so they do help the regulatory processes. They are tied to some of the next generation efforts that are going on with things like AAMI/UL 2800 and looking at interoperability and so forth. They're being leveraged internationally by other regulators like the MFDS, the -- I forget the name of the acronym now, the NMPA. In China it's the CFDA. Health Canada and a variety of other countries. Singapore is looking at using

them. And so this notion of having a single set of requirements that Michelle mentioned earlier, to get manufacturers into the market effectively is really what we were after.

MR. GARCIA: Thank you. Okay. And Brian, from FDA's perspective, how do you use standards?

MR. FITZGERALD: So let me start off with the idea that, as Anura mentioned, that when you have hundreds and hundreds and hundreds of really fine standards in a sector, guess what, you don't have any standards. We have too many standards, that's the problem.

And so not too long ago we decided to try and get ourselves -- finagle our way into the IEC central office for a forthcoming guide, 120, which was, if you like, how to put cybersecurity requirements into sector-specific standards and how not to, because at the same time as we had cybersecurity getting on everyone's plate in every sector everywhere, we ended up with these sectors approaching the cybersecurity perspectives quite differently. So trying to change the ship of state at IEC, which is, if you like, a rather large standardization organization in lots of different sectors, that became quite important.

So we participated in the development of Guide 120 and that is now out there and future standards developments, at least in the IEC, very probably also from ISO, they may take into account the considerations in that Guide 120 which will allow standards that are very sector specific to actually concentrate on the same types of things, security risk assessment rather than specific measures, leaving the specific measures on the standard, the criteria for the integrity of those measures, up to the expert subcommittees.

But from FDA's perspective as a regulator, we want to have standards that are available, that are attainable, that are verifiable, and we want them to be used as much as possible, but resources is a huge constraint on that. The more standards we have out there, the harder it is for us to get our own internal staff familiar with -- familiar enough with

these standards to be able to tell whether they've been complied with. So the proliferation of standards, some of which may not necessarily be aligned with each other, is leading to a process degradation where we may have to contemplate looking at third-party assessments in order to force leverage the resources we do possess. So I see, in the future, cybersecurity evaluations becoming part -- increasingly a part of third-party evaluations.

Then the question is well, what are the models that are suitable for verification that FDA can rely upon? Well, as you may know, I want to put in a little plug here for a program that, under MDUFMA V and MDUFMA IV, will bring third-party assessment increasingly to the fore as part of premarket evaluations. My ambition, I'm working assiduously to try and get cybersecurity somehow into that program. That program is called ASCA. It will be coming out, I think, here not too long, we have quite a bit of work done in it.

But cybersecurity is a system property and it's been largely ignored as a system property for 25 years and I see that the standards, the system standards that will lend themselves to third-party evaluation as that class of standards that will survive in the long run and at least as far as regulators are concerned. So that's a sort of strategic view of standards moving forward.

Right now, the tactical view is that we need security risk assessment to be highly standardized right from the premarket and the postmarket and by TIR57 and TIR96, which is coming along very nicely. We need standards for the disclosure of cybersecurity properties in an arbitrary device and that's where the MDS2 -- I'm grateful for Zach for turning up this week to -- grateful to him for chairing this effort. I think that's turning into an excellent document and it will be very, very useful for manufacturers and for industry and for the consumers of medical devices.

And then I think the renewed impetus of 80001 is not be underestimated. Eighty thousand and one started off way back in the day in 2005 as a means to establish how risk

could be communicated and transferred towards -- or rather from, if you like, the risk management approach of designers and producers of medical devices towards that user of that medical device. And remember that you shouldn't -- you shouldn't sort of think of medical devices as ending up in the hands of others to be deployed and maintained because even if you made implants and other things, that maintainer, that deployer is the future you, yourself. You must remember to design those devices so that you can maintain them.

So another, if you like, refinement of that system property we call now cybersecure-ability is that notion of the maintainability of that cybersecurity property, thinking of it as a secure-ability moving forward. These devices must now be designed with maintenance in mind. The reality, the physics, is that the standards must also now move towards a whole of life cycle approach with much less emphasis in the premarket. Even if the law is what it is, the physics are what they are.

MR. GARCIA: Okay.

DR. ROSS: A quick question for the panel. So can some of the panelists speak to some of the -- you mentioned, Brian, risk management -- speak to some of the efforts as it relates to TIR57 and 97, please?

MS. JUMP: I'll take that one.

MR. FITZGERALD: You go first.

MS. JUMP: Thanks. So maybe I'll build off a couple of the things that Brian said in answer to that question. Who's heard of TIR57? Wake up.

(Show of hands.)

MS. JUMP: Look at all of those hands. We love that. So one of the things, TIR57 was not only greatly received here in the U.S., actually internationally, they love it. The reason that they love it is because -- and I was on this group, so I love it, too. But the reason that they love it is we took 14971, so everyone knows the -- and we built a security risk

assessment structure on top of it. So we took something that people understand and know and we built security on it. Similar to what Brian was talking about, Guide 120, we're using that in 81001, by the way, yes, yes -- is that if you take structured standards that we understand today and you build security into it, then we find that the adoption rate, the understandability of that document, is much higher.

And so, by the way, if anyone is furiously writing down numbers from us standards geeks up here, there is a gift for you outside if you didn't get it this morning. I did write a list of a description of all of these pending standards that I'm going to talk about and Aftin has it too, so she should be posting it as well. So it's a list. So if everyone's trying to keep all of these numbers straight, they are listed with a short description of why they're security relevant.

Now, TIR57 is out there; however, there is SW96, which is a current effort under AAMI where we're taking TIR97 and turning it -- or, excuse me, 57 and turning it into a full standard versus just a technical information report. And then there is TIR97. So there's SW96 and TIR97. Sorry, I always have a hard time with those two. That's why they're on the paper. So the SW96, we're hoping to take TIR57 and turn it into an international standard eventually. But TIR97 -- there we go, yeah, thank you. It's been a long day. This is where we take -- so we did the risk management and this is for postmarket management and the nice thing about this is that it's looking at how to -- it's foundational in saying, you know, this is how you start to develop policy, this is how you start to design devices that can hold up in the postmarket space. And so we've talked a little bit about design here in the last couple of days, just a little bit, and that's really important when you're also thinking about the maintenance of those devices in the field. And if I could just also touch on one other international standard?

MR. GARCIA: Just a couple minutes left.

MS. JUMP: Yeah, thank you. 81001, as referenced a couple of times, one of the things that Brian was talking about is we have all of these different standards, right, and they're all going in different directions. 81001 is a very new and different kind of standard, that's why it's taking us so long to create it; it's a cradle-to-grave document.

And so there's a security element in it because we've considered that security should be an unbroken threat from the time you start to even conceive of a device to the time it gets retired or decommissioned in the hospital. The problem is, is this transfer of information that we've talked about so much in the last couple of days is currently not very standardized and so -- but it shouldn't just be security.

There's a lot of other risks that we consider when you're designing a device and then transferring those devices to new owners across the entire life cycle of the device. So 81001 is trying to address that by talking about some of these key foundational elements, security, privacy, risk management, quality management, all of those things and talking about how you start to transition information across that space.

But what we're also trying to do is align around a single set of terms that we're using. We find that people are using risk management terms in different ways, we're finding that even defining harm creates a lot of heartburn for us standards geeks because we define harm differently in different spaces, and risk differently in different spaces. And so that particular document, I think, is going to be really helpful in trying to bring together some of that harmonization.

The one last standard there -- I know we're probably well over time here -- is also on the list but it follows this model of 14971 and remember, TIR57 is really helpful because it goes on a 14971 framework. Well, greatly anticipated, at least for us standards geeks in the standard world, another greatly anticipated standard that is actually just kicking off next week is 80001-5-1, which takes -- again, this is on the paper, don't worry about writing it all

down -- 62304, your software life cycle mother standard and it is going to be reinvented from a security framework state of mind, right? It's really hard to add security into an existing standard like 62304 because everyone has it in their quality system; nobody wants to change it. So they're setting up a new one, a companion document, that would be 62304 but for standard-specific considerations, so those will be able to be used in conjunction.

So a lot of important stuff going on right now in this space, which is why I wrote it all down, because if you're not embedded in it like we do and rattle off these numbers off your tongue it can be really helpful to get a list of those, so that will be distributed.

MR. GARCIA: Right here. You've got a lot of challenges ahead of you, that's very daunting. Do we have time for just one question, one last question? Yes, sir.

MR. HAHTI: Manu Hahti, Stryker. It's a really good question for Michelle, so the last standard that you mentioned that's going to replace 6304 from a security perspective, is there a plan for it to be harmonized as yet or are you just developing it now and -- I was just curious if there's been discussions about that.

MS. JUMP: Harmonize with what?

MR. HAHTI: Harmonize from an international perspective, a European one and --

MS. JUMP: Well, fortunately for you, that's a really easy answer and because it's being done at the international level, it's being kicked off at the international level, so it will automatically be -- it will be an international standard, so it's under IEC and ISO.

MR. GARCIA: All right, we have run out of time, I'm sorry. This is a very interesting conversation but please, for the panel that proceeded them and this panel, please, let's all give them a warm thank you.

(Applause.)

DR. D'AMICO: Thank you, everyone. So next we'll invite our panelists and moderator up for our next panel, Information Sharing: An Evolving Journey.

(Pause.)

MR. ROTHSTEIN: I'm curious, should we have all the panelists together? Would that make for a little bit of a better conversation? John? John Gomez. Paging John.

(Pause.)

MR. ROTHSTEIN: Oh, see, now I get to stay far away from the panelists, I can take a more serious approach to this panel. Well, welcome to Session X, Information Sharing. I'm actually really excited for this panel for a number of reasons. We have a lot of really good speakers up here today and also, I think this is one of the panels where the rubber really hits the road in terms of implementing cybersecurity and working together as a community with respect to your cybersecurity practices.

So instead of just a quick introduction of your name and organization, I was actually hoping each of you could get into a little bit deeper information about what your organization is, as you introduce yourself so, you know, who you are and then what is your organization and what's its purpose for the sector that you participate in.

So, Denise, let's start with you.

MS. ANDERSON: How many people have heard of an information sharing and analysis center?

(Show of hands.)

MS. ANDERSON: Okay, good. So I've been in the ISAC world for quite a long time. I was employee number two at Financial Services ISAC and have been doing information sharing before that was even really a word. But, basically, the ISACs are the operational arms of the sectors, so they're responsible for the coordination and response during incidents whether they be cyber or physical, so we look at both sides of the equation and basically what we are, for lack of a better word, is a trusted community of stakeholders within healthcare. And then we also, of course, collaborate with all of our brother and

sister ISACs out there in critical infrastructure. So we have stakeholders that are, as you could see up there on the slide, within almost all of the subsectors in healthcare. And one of the things I'd like to say that I think we do pretty uniquely is bring both sides of the medical device equation to the table and that's the HDOs and the manufacturers together.

One of the things that we do that I want to highlight is we have a working group, a medical device information sharing cybersecurity council, where they're sharing -- where it's co-chaired by Ken Hoyme, who is here, and Shawn Anderson. So Ken is a manufacturer, obviously, and Shawn is with Intermountain, so that's an HDO. And we purposely did that so that we could make sure that the conversation is a dual conversation, so both interests, both perspectives are brought to the table so that, you know, when there is an issue or there is something to frame out we can get both sides really working together instead of, you know, pointing fingers at each other.

So as I think I heard in an earlier panel, we're all in this together and the quicker we can realize that we have to absolutely be on the same page and be teams, the better off everyone will be. We are also very international, obviously, within the manufacturing community, with pharmaceutical manufacturers as well as medical device manufacturers and now HDOs, too. There is a lot of work being done on a global scale and we're certainly trying to leverage what already exists and build that infrastructure out. So I think that's good for me.

MR. BEARD: Hi, I'm Daniel Beard. I'm director of MedISAO. We're an information sharing and analysis organization that is focused on the devices themselves and the manufacturers that make them with an even more intense focus on small to medium-sized manufacturers. Kind of like Colin said earlier on another panel, small manufacturers get acquired by large manufacturers, so small manufacturer problems become large manufacturer problems eventually. So we think that that's a place where we can do a lot of

good in getting the small to medium-sized manufacturers the appropriate vulnerability and threat information to make safer devices from the beginning.

MS. GAGLIOSTRO: And I trust at this point we're sufficiently out of order. I'm Rebecca Gagliostro. I'm with the Interstate Natural Gas Association of America. It's a lot of words. We usually refer to ourselves as INGAA. For those of you that don't know who we are, we are a trade association that represents 28 of the interstate natural gas operators in the U.S.

And full disclosure, I don't operate an ISAC. I don't, you know, run an ISAC, but -- so my comments today will be more focused on some of my experience working directly with the ISACs in the energy sector. And I think similar to what you deal with in healthcare when you have to work with different sectors and segments of healthcare, we do that in energy because there's a lot of interdependence between energy infrastructure. You have reliance on things like electricity for natural gas operations. Telecom. So there's a lot of cross-coordination, communication and sharing of information within our ISAC community.

DR. SCHWARTZ: Hello, good afternoon. Suzanne Schwartz, Associate Director for Science and Strategic Partnerships at FDA's Center for Devices and Radiological Health, and our mission is to protect and advance the public health. So from CDRH's perspective, that applies to the medical devices that we regulate, that we have oversight of, in terms of providing that kind of reasonable assurance around safety and effectiveness, and as cybersecurity is an emerging and evolving area with respect to patient safety as well, that falls within and under our remit.

MR. GOMEZ: Hi, John Gomez. I'm with Sensato ISAO. Before I tell you what that is, it's probably best to give you a little bit of history of how we became an ISAO. At the last workshop that was held here, after that we created the medical device cybersecurity task force. That task force was really focused on being extremely tactical in terms of best

practices for securing both medical devices from the medical device manufacturer's perspective and also from the provider, the hospital organization. That's grown to about 83 different members and continuing to grow. It's a free membership, we don't charge for membership in it. It's a combination of medical device manufacturers, hospitals, consultancies, and others.

That's now evolved into an ISAO and so as the ISAO continues, we probably will continue to focus more on the tactical side versus the long-term strategic. By tactical we mean that as issues or intelligence evolves, we try to respond to it very quickly, typically within 24 to 48 hours and establish at least a foundational set of directions. We also look at best practices that can be deployed rather quickly, especially from the provider's perspective. So that's kind of the background of how we evolved and where we're at now.

MR. ROTHSTEIN: Yeah, really good overviews. So maybe, Suzanne, I can ask you to explain to the audience what FDA's expectations are with respect to device manufacturers and their participation in information-sharing bodies.

DR. SCHWARTZ: Yeah, absolutely. And if it's okay with you, Zach, what I'd like to do is provide that in a little bit of historic context here that would be helpful for the audience.

So we can go back, actually, to 2014. I think it was 2014 when the FDA actually entered into a memorandum of understanding, our first MOU, which was with what was called then the NH-ISAC, now the H-ISAC, and what that was, was really conceptually a handshake with the recognition that the Agency had of the importance of there being a mechanism for sharing of information around vulnerabilities and threats as they pertain to medical devices and healthcare. And this followed also within the space and context of, at the time, the prior administration executive orders and the real importance of there being a trusted place, a trusted space for owners and operators to share information.

So we established that initial MOU with the understanding that this was going to

have to take on a bit more structure and certain specific objectives as well, and over the ensuing couple of years between 2014 and 2016, that is when we also -- we executed, we put forward our postmarket guidance, first as draft and then as final, and recognizing the space of cybersecurity of medical devices and being warned that would warrant an accelerated type of action by manufacturers, particularly around those types of vulnerabilities that are identified that could have the potential for patient harm, that do raise concerns for safety, that there would need to be some mechanisms from a policy perspective that the FDA would look to entertain, that would incentivize industry to move in a more expeditious manner.

So what does that mean for a regulator? Often what that means is trying to identify what are, first of all, the impediments, what are the barriers, whether they're perceived or real barriers that generally slow the process down as far as industry being able to address a matter, an issue, a malfunction, a safety concern. And in so doing, as we went through that process of thinking of how can we remove ourselves, how can we remove barriers from addressing issues that need to be addressed in a more timely manner with respect to cybersecurity, we had come up with this construct that I know that industry is well familiar with and that is this construct of controlled versus uncontrolled vulnerabilities, controlled risk versus uncontrolled risk.

And so what I'm going to do now is particularly focus on the uncontrolled risk of vulnerabilities, those being ones which have, by the manufacturer's assessment, an unacceptable residual risk regarding patients potentially being harmed if those vulnerabilities were to be exploited. Normally, for that type of a concern, in traditional FDA parlance for that kind of a safety concern, the manufacturer would engage with the Agency from the standpoint of what's called Part 806 corrections and removals. It's a process, there's paperwork, administrative pieces to that. It entails multiple steps. It isn't what I

would call agile, okay, and what we wanted to do is move to a place, again, that would provide incentives to manufacturers to act faster when these kinds of vulnerabilities are identified and then assessed as being indeed of concern for patient impact.

And so we described in the postmarket guidance three criteria, that as long as those three criteria are appropriately met that the manufacturer would not need to undergo the Part 806 corrections and removals. Those criteria, just again for purposes of repeating and making sure that everybody's aware of them are, number one, that there have been actually no adverse events, no injuries, no deaths related to that vulnerability; in essence, that the vulnerability, to anyone's knowledge, has not been exploited.

Secondly, there's a time component to it and that's the 30/60-day rule that you heard people talking about over the course of the past 2 days, that from the time that the vulnerability is initially identified, brought forward to the manufacturer, to the time that an initial assessment and communication out to customers with respect to then also including mitigations that are going to reduce the concerns for safety to an acceptable level, has to be undertaken within 30 days and then a more permanent or definitive type of remediation would occur within 60 days. So that's criterion number two.

And then the third criterion, which is the one that we're talking really kind of about here as far as the development of the ISAO concept for medical devices, is that manufacturers participate actively in an information sharing analysis organization that was created for medical device vulnerability information sharing. And the notion of this kind of goes back to the very principle of transparency and information sharing and creating a trusted space for that with the idea then of being able to use the ISAO also as that force multiplier in terms of getting that information out beyond in a more expeditious type of a manner. So that is the history there as far as the relevance of medical device ISAOs. Our vision for how, then, we operationalize that was that utilizing the healthcare ISAC,

leveraging the H-ISAC as really that central place for the healthcare sector at large.

And this goes back to the hub-and-spoke model that medical device ISAOs that could emerge based upon the interests, the needs, of different parts of the medical device community would then be able to also share information to the H-ISAC, which could then be distributed out broadly to the ecosystem, to the community at large so that there is a small community of like manufacturers who might have the same types of challenges, who might want to develop best practices and share amongst them in addition to the vulnerability information sharing components or there may be other value propositions that an individual medical device ISAO might have and this would enable manufacturers to determine potentially where the best fit is for them to allow that kind of information sharing so that, number one, it's suiting FDA's needs from the -- and allowing manufacturers to take advantage of the incentive in the guidance and at the same time it's providing additional value add to manufacturers to find that smaller community that they find is going to be most of value to them and that information then would also, from a vulnerability perspective, be more broadly available and distributed through the healthcare ISAC as its mission to the ecosystem at large.

MR. ROTHSTEIN: So a lot to peel back there, but maybe we can start with, for John and Daniel, one thing Suzanne mentioned which is in the postmarket guidance is to take advantage of that Part 806 provision, a manufacturer has to "actively" participate in an ISAO. So both of you operate ISAOs right now that medical device manufacturers can participate in. Do you have definitions or otherwise expectations around what active participation looks like?

MR. BEARD: Yes, for MedISAO, we want members to be part of our coordinated vulnerability disclosure program and we feel that that's an important part of being an active member and also to contribute to the community. We have internal discussions about

vulnerabilities and how to remediate them. So by doing those two things we feel you're an active member.

MR. GOMEZ: So it's very similar, it's disclosure of the vulnerabilities through a formal process and scoring the impact to that vulnerability on potential patient safety. The second area, though, is also -- and this may also be something that an ISAO is doing as well, is looking at overall risk management and how can that contribute to getting ahead of the vulnerabilities that we're looking at and providing practices around writing secure code and secure by design and deployment and really looking at, from a medical devices perspective, how they are detecting for security, not just with what they have but as they go forward.

MR. BEARD: It was part of the postmarket guidance, but this is a premarket workshop and I feel like even premarket it makes a lot of sense to join an ISAO because that's where you get the most benefit from this information is while you're designing the device.

MR. ROTHSTEIN: And so, Denise, can you then maybe explain, from the ISAC level, how this all functions together, you know, from the ISAOs, from the ISAC and then even your coordination with other ISACs and even the federal government?

MS. ANDERSON: So I don't know that we've had an actual case test yet come bubbling up from the ISAOs, but we do have what -- I don't think we mentioned, we do have MOUs in place with both ISAOs so that, you know, when something does bubble up through that channel then we would be able to take it and incorporate it into a process that we've already worked out and one is the fact that we've developed relationships not only, of course, with FDA but also with ISC/CERT at DHS and of course, the manufacturers, so that when something comes and it's disclosed we're able to all work together and coordinate how the message will get out appropriately to the right stakeholders. So we, of course, use our channels to get the word out as broadly as possible and that's not just the ISAC but also

the Sector Coordinating Council and using -- you know, leveraging all the trade associations that are a part of that to get word out to the appropriate stakeholders. I would love to see us dive deeper down into some of that process, actually, and have some ideas and that, you know, bringing more stakeholders together in a collaborative fashion even before the disclosure comes out and so that everyone is on the same page.

MR. ROTHSTEIN: Could you elaborate on that?

MS. ANDERSON: Well, I think, you know, like we've heard some conversations today just pop, you know, some things that were bubbling in my head were the fact that having the communication of the actual vulnerability is confusing to many healthcare delivery organizations. Sometimes it's not helping them understand well, how do I build whatever I've got already in my compensating controls in line with this vulnerability? So being able to talk beforehand about the message that comes out, that would be appropriate and meaningful to everyone that's involved. I think it would save a lot of angst. So being able to be proactive versus reactive, I think, would be a great path forward.

MR. ROTHSTEIN: Rebecca, maybe I can bring you into the conversation from your angle. What has been the experience on your end for setting up an ISAC and maybe some of the lessons learned that you have that you could share with another industry like ours?

MS. GAGLIOSTRO: Yeah. So one thing that strikes me as very interesting in listening to this panel talk so far, I represent a segment of the energy industry, we're almost like end users of what you guys do. So you're providing the manufacturing of devices. We're the end users of devices in our own right and I think this conversation around disclosing vulnerabilities, in particular, kind of strikes a note with me because I know when we -- we are building our ISAC for looking for things such as vulnerabilities and products that we're using. We're also looking for information on active threats and campaigns and mitigative measures and easy ways to digest that information so we know what we need to do. I think

if you take a step back from those differences, one kind of fundamental theme across any sort of information sharing community is the need -- Suzanne said this in her open remarks, it's building a community of trust.

So when you keep that in mind, you have to know a little bit of who your user base is and recognize that you're dealing with individual organizations with very distinct cultures and modes of operation and it's going to take time to really foster and grow that maturity, but it's -- you know, it's kind of a crawl/walk/run thing. So just because we all agree that this is something that we need to do, how do you get to that next step of truly being able to implement it?

And so some of the conversations so far have hit on -- one of the key drivers, I think, is finding the right ways to incentivize the proactive sharing of information because I think most organizations tend to prefer to be consumers of information. In my experience, there's a couple reasons why that might be the case. In the energy sector in particular, it might just be bandwidth issues, that they don't really have the bandwidth to be both taking in the information, dealing with what they find through that information and pushing stuff out. They're more interested in dealing with the now, so how do you incentivize them to be more proactive?

Beyond that, there is also oftentimes legal concerns that we come across where, especially if you're dealing with an incident yourself, you don't want to be too proactive because you might be exposing yourself and you're afraid of what the repercussions are for that. So I think a good first step in getting over the hurdle really comes down to education. We've had a lot of conversations with our members about protections provided by the Cybersecurity Information Sharing Act, in particular, and the protections that that provides for information sharing to get folks more comfortable with the idea of you're not going to get yourselves so much into trouble. And I think those conversations in particular, because

they've looped in a lot of the legal departments within the member organizations, that's really a significant hurdle to jump through first is getting through the legal side of.

Beyond that, when we talk about building a community of trust, I think you have to find ways of establishing familiarity with the community so it's not just as much as okay, we've got a cool technological platform, we've got a couple of analysts, they're putting stuff out there, you need to actually get the community to know each other. Some of the ways that we've been successful in doing that in the energy sector, I think, are having other touch points and actually logging on to a portal, so having kind of more regularly scheduled calls and face-to-face meetings so you start to learn who that community is, be familiar with the faces and get comfortable with them.

And I think it often rolls the ISAOs -- by taking kind of smaller chunks of that, you can have almost little -- you can form little trust cohorts, so to speak, of being able to be really familiar because I can tell you with INGAA representing 28 member companies, our biggest benefit in that space is the fact that we are so small, so it's really easy for me to get on the phone with my members and just have really open and candid conversations. But it didn't happen overnight, it kind of happened gradually.

MR. ROTHSTEIN: So can we maybe talk a bit more about this concept of building trust, right? It's something both Denise and Rebecca have mentioned. I'm wondering, John and Daniel, can you talk about how you've built trust in your community and maybe some of the challenges that you had in doing so?

MR. BEARD: Sure. So because we're targeting small and medium-sized companies, a lot of them were new to cybersecurity in general, so we put out a lot of documentation and best practices guides to help them specifically and generated a lot of conversation, both over the phone and in our online portal, about how to bootstrap up a cybersecurity program and what to do with this information that you're getting, and I think just that

constant conversation is -- builds trust.

MR. GOMEZ: So the tactic we've been using is probably not -- I guess would be a little bit more unorthodox or more education focused, like Rebecca stated. What we do is we really focus on the medical device manufacturer's revenue and sales pipeline of all things and what we talk to them about is how to use security and the postmarket and premarket guidance as differentiators in your marketing and sales.

So what we've been finding is the reaction to security is a lot driven by, ultimately, the clients. Hospitals are coming to medical device manufacturers and saying we need you to fill out this risk assessment, we're not going to buy your product until you disclose these, how does -- what's the internal architecture, which slows down the sales process.

So what we've been really working on is working with product managers and program managers and executives at medical device manufacturers, helping them understand that if you embrace security, you -- in many cases, especially where we are right now in the maturity of the industry, you can use that as a differentiator. You can also help kind of push forward your sales pipeline. Suddenly, you have their attention and some of the things we talk about is join an ISAO or, you know, work on your disclosure and that should all be part of your differentiators.

I think for us it's been really pushing that side of the equation versus focusing on whatever is considered traditional trust and there are some things we do around traditional trust, which would be assuring that anybody that is part of the ISAO is vetted and we talk through how we do that and that you're not just sharing information, you know, broadly across the world and things of that nature. But what we've been really trying to do is focus on what are the pain points that security creates for the management teams at the medical device manufacturers and then using kind of what we all know in this room to be the right answers as the way for them to kind of start deciding maybe it's not just trust, but it's a

good business practice and so what we need to be doing. Ultimately, the ends justify the means, I think, is kind of how we look at it.

MR. ROTHSTEIN: Denise, I'm curious, from the H-ISAC perspective, how you build trust within your community, how that's overseen. And, in particular, maybe if you could talk a bit about the dynamic that you have, unlike for John and Daniel, but in your case you have customers and the manufacturers fitting together because it's the broader ISAC. And so how does that dynamic work and how do you deal with those situations?

MS. ANDERSON: I look at them as all customers, so interesting, but -- so I think there's a couple things. One is there's some legal instruments that are in place, right, so we have the MDAs within the ISAC so that people feel comfortable knowing that they're going to be held by the MDA to share information appropriately.

We also have the traffic light protocol, so that's a protocol where the originator of the information that gets shared and marks it as to how they want to get it disseminated, so a risk-based group like stop light, red, green, amber and white with red being restricted to a certain group, amber being open to a broader group, green being with trusted partners, and white open source subject to copyright. So there's some constructs there that kind of build that foundation for trust.

But then it's all about the relationships. I mean, I know I heard that earlier. It is about the relationships, building relationships across sectors, within the sector, across the subsectors, so that when you are talking to someone you know who they are, you know you can trust them, you know you're willing to help each other out because one person's defense is going to become everybody else's offense, that's what it's all about. And so, you know, doing face-to-face meetings, you know, or having -- we have summits where we do a lot of networking and create a lot of networking opportunities.

But even something as simple as a list server. When I was with the Financial Services

ISAC and we started sharing information with each other it was anonymous at the time because people were uncomfortable about sharing or didn't feel that their legal counsel would let them share, so they did it anonymously. And what we found was that when we moved to list servers where there was attribution, the sharing actually multiplied enormously because what happened was people started building relationships, they saw who was sharing, they saw what they were sharing, they saw that everybody wanted to help each other out because, guess what, they were all in it together.

And one of the things I think, you know, if you're a parent or maybe not a parent but you have kids, you think that you're the only one in the world that suffers from the things that your kids do and then you talk to somebody else and they're like no, my kid does that, too, and you're like, oh my God, everyone -- you know, it's like everyone has the same problems and when you start understanding and talking to each other about it, then you realize we are all in this together, we all need to help each other out.

MR. ROTHSTEIN: That's great. And maybe now switching gears just a little bit, we've talked a lot about information sharing services that are being provided. What other services, though, are organizations like yours providing that members get to take advantage of?

MS. ANDERSON: Do you want -- go ahead, go ahead.

MR. BEARD: Well, I just wanted to reiterate that the traffic light protocol, before we go on, that is a really easy way of communicating. Everyone gets it. We at MedISAO, too. So if you're having trouble getting that trust, I don't know if it's going to get disseminated and who is it going to get -- who's going to get told the traffic light protocol is a great tool. So as far as services go, we have the coordinated vulnerability disclosure service, we're looking at ways in the next year of filtering vulnerability information to more closely target individual manufacturers, and I think CBOM or SBOM or whatever you want to call it is a

great tool for that. We have documentation, best practices guides, and again, the community. It's all sorts of information, not just vulnerability information.

MS. ANDERSON: Okay, I'll jump in. I'm not going to -- we actually offer a lot of stuff that I'm actually very proud of and a lot of that free to our members. One of the two really valuable ones are domain monitoring and also credential parsing. So we've had over six billion credentials parsed and about one billion of them were true credentials that were discovered. So we're doing some amazing work there.

The sharing that we do, we have sharing capabilities through our list servers, of course, and then also automated sharing. So we have a number of automated ways that members can share with each other and we also have a chat platform where the sharing has been phenomenal. What we did when Petya and NotPetya broke was amazing work from a collaborative standpoint amongst the member organizations.

We also do a lot of education, so we have summits, workshops, webinars, exercises, etc., and then we have a number of other tools that we offer to our members and some of them free and some of them have a -- you know, at a low group cost. So like, we have a third-party risk assessment program and stuff like that.

MR. GOMEZ: Similar to the other constituents, there's a variety of workshops, educational programs that we do. Some of the ones that are most popular for us are tabletop simulations, we do a variety of those to kind of help drive awareness. We also do a lot of threat intelligence briefings specific to medical devices. We've just adopted C2M2, which you may or may not be familiar with, which came out of the Department of Energy for quickly and rapidly assessing risk to medical devices and healthcare, so that's something else we do. We also do a writing secure code program. All of those are pretty much free. We also do coordinated incident response and the way we look at that is on an ability to pay. If you can't pay, we'll still manage and help you within certain responses if you do

have a situation that arises and help coordinate that, but -- yeah, so there's a variety of different surfaces beyond just the vulnerability disclosure that we do.

MR. ROTHSTEIN: Suzanne, you've mentioned how FDA fits in. Could you talk a bit about how other aspects of the federal government, and maybe to the extent you're aware of local and state governments interact with respect to information sharing and addressing potential cybersecurity issues?

DR. SCHWARTZ: So there has been an effort that was established back in 2014 for independent and executive branch regulators to get together around cybersecurity of critical infrastructure for purposes of sharing experiences, sharing best practices, understanding what each other's policies were, whether these were existing policies or policies in formation, primarily to try to get to a place of if not kind of a harmonized approach, one of making sure that if there is a need for deconflicting, it would be important for the different agencies through government to really understand exactly what each other's approaches are.

That initiative, again, which started back in around June or so of 2014 lent itself to a series of workshops that were hosted by different agencies on a voluntary basis to try to tackle different areas that have been challenging for, again, different regulators. Some were on the supply chain or on information sharing or on "are additional regulations necessary." The dialogue that would happen within those workshops, which would also include bringing in from industry specific subject matter experts also to educate the agencies on new evolving areas was very useful, was very beneficial. I think that there's been a little bit of a lull as far as that activity goes recently, but I think that there may be -- we've been rotating, different agencies taking responsibility to kind of be at the helm of organizing this particular forum, again, called the Independent Executive Branch Regulators Forum for Cybersecurity. It started off with the nuclear regulatory side taking the lead on

that and working together with the executive branch with the White House National Security Council and then moved on to FCC taking a role and FTC has taken a role as well.

So that is one avenue for, on the federal government side, certainly discussions and information sharing that allows for some of what we're talking about, you know, within the private sector of being able to understand what best practices or what's working and what's not working to really bring that to the fore.

As far as liaisons or working together with state and local, I think that that's an area of opportunity. I don't know that that is really well established or structured at this point. I would say that -- and I know, I think perhaps our last panel is going to talk about this a bit. Certainly in the area of response or preparedness and response, there there's not only a need but there are already some nascent efforts to bridge between federal, state, local, private sector because really, all of those entities have critical roles to play with respect to the response to an incident, an incident that may go well beyond local to -- you know, to a regional area and assuring that among the different jurisdictions, first of all, where you can get areas into a lot of conflict, obviously, that people -- agencies are not tripping over each other but that really we're working, we got this unity of mission, unity of effort towards dealing with the potential for a public safety concern.

MS. GAGLIOSTRO: If I could just make a quick comment because you're making so many good points. A lesson learned from the energy sector, one way that we've kind of addressed that is through coordinated exercises. You may have heard of the North American Electric Reliability Corporation's GridEx, grid security exercise. That's a national-level exercise that uses the ISAC as kind of the platform for pushing the simulation out, but it provides a great opportunity to practice in real time how the state and federal and regional entities come into play to coordinate in the real-time response to an incident.

MR. ROTHSTEIN: So we're coming up to the end of our time. Are there any

questions from the audience that anybody would like to ask? Otherwise, maybe I'll wrap up with a question for all of you and I guess maybe I should've given you a heads-up on this one, but let's see how it goes. Let's say 3, 5 years out from now, where do you want to see information sharing to be from where it is today? What does that look like? What should be our goal as a sector, as an industry? In any order.

DR. SCHWARTZ: All right, I'll give it a first stab. So one thing I did not mention at the beginning is that we were pretty silent -- we were silent in the postmarket guidance with regard to controlled vulnerabilities as far as stating anything about information sharing. We went right for the uncontrolled risk because, of course, those were of gravest concern to the Agency from a patient safety perspective.

But, ideally, what that vision was for us when we wrote it is that the trust would build to such an extent also among organizations that it would become routine and just this is the way it is, information sharing is happening around all vulnerabilities and that a regulator doesn't need to necessarily provide that incentive there, but by the very nature of creating those kinds of small communities of trust and the members of those communities recognizing what value they get out of information sharing that it becomes, of course, it's a given. You know, this is the way we do business.

MS. ANDERSON: So you know that Coke commercial, I think it was where everyone had their arms arranged together and said I'd like to teach the world to sing, and I think instead of sing we put share information. But seriously, I think, you know, the more people are comfortable with sharing and understanding that it's actually a business imperative to share because, you know, again, one person's defense is going to become everyone else's offense and if we don't do that, then shame on us.

MR. BEARD: I have kind of a similar sentiment, I'd like to see more sharing going on and more -- the more information we have, the better and then we can have discussions on

more and better tools to filter that information and make it actually actionable.

MR. GOMEZ: Yeah, I'm not sure I can improve upon what was said. I think it would hopefully be that sharing information is just business as usual, right, it's just what we do, we've gotten past the trust issues and hopefully we've automated most of it by that time, right? That's probably the other big piece of it, is just making it really, really simple to do.

MS. GAGLIOSTRO: And the last point I'll make is that I think what we're all saying is that we want this to be the next level of maturity. So it's the maturity walk that we're taking right now in information sharing and if it's more proactive and ingrained in our culture, we'll be at that next step.

MR. ROTHSTEIN: And I'll make one point since I haven't really said anything interesting while I've stood up here. I think at some point it would be good, and I know the H-ISAC, just changing your name is already reflecting that there's an international component, too, especially in this space where, you know, these risks are not confined to geographic borders, so looking at collaborating beyond just the domestic side, I think, will also be important for our sector and for others as well.

So we are out of time. Thank you, everyone, for paying attention and thank you to the panel for a great discussion.

(Applause.)

DR. D'AMICO: Thanks, everyone. So we'll take a quick break, and we'll shoot to get started -- I know we're running behind, so a little bit after 3:35. So feel free to stretch your legs and use the restroom.

(Off the record at 3:33 p.m.)

(On the record at 3:44 p.m.)

MS. ZUK: I think we're going to get started. Can everybody hear me? Good. I'm Margie Zuk from MITRE. Our final panel of the workshop is on preparedness and response,

and I'm very fortunate to have so many participants here with me representing many parts of the sector and we're wanting to end on a good note with offering a lot of resources and activities that are available, you know, to help with preparedness and response. So we're going to start with just a quick introduction. Maybe Christian, could you start? Just name and organization so we get through that first.

DR. DAMEFF: Sure. My name is Christian Dameff. I'm at the University of California San Diego.

MS. ALFREDO: Good afternoon, I'm Laura Alfredo. I'm with the Greater New York Hospital Association.

MR. WATERS: Chad Waters with ECRI Institute.

MS. TAMARI: Nastassia Tamari with Becton Dickinson, and I do the incident response and coordinated vulnerability disclosure for BD, a medical device manufacturer.

MR. GARCIA: Hello, again. Greg Garcia with the Health Sector Coordinating Council.

MR. ROTHSTEIN: Zach Rothstein with AdvaMed.

MS. ANDERSON: Denise Anderson, Health-ISAC.

MR. BASTANI: Rob Bastani, Assistant Secretary for Preparedness and Response.

MS. CHASE: Penny Chase, MITRE.

MS. WOYAK: Ashley Woyak from Baxter.

MR. GOMEZ: John Gomez with Sensato.

MS. ZUK: Great. So as you can see, we have a wide variety of perspectives on the panel today representing associations, hospitals, manufacturers, and what we wanted to start with, since the name of our panel is about WannaCry and what will we do if WannaCry Again, we want to begin by talking about, from each organization's perspective, how did WannaCry shape preparedness and response activities?

I know for us up in the Boston area, we happened to have a regional resiliency

meeting the day before WannaCry with 75 hospital participants and discussed what would happen if there was a widespread malware or attack affecting hospitals and it was so interesting to hear the debates on that day about whether you would invoke a national system that was used for other types of disasters or create a different one for cyber, for example, and you know, the next day everything took shape. So I think it's really interesting to get these different perspectives about what happened on that day and since. So I think we're going to start with Christian, from the hospital perspective.

DR. DAMEFF: So I was at a drill preparing for ransomware attacks when WannaCry hit. No, I was working clinically, so I'm an emergency medicine physician. So I was working in the emergency department. I did not find out about WannaCry until the next day partially because of how busy clinical practice is and partially because it just wasn't even communicated to us. Maybe many of you out there say well, should it be, it wasn't affecting you, why would we tell people about this, but I just wanted to communicate that there's huge swaths of clinicians that probably don't know what WannaCry is, yet they take care of patients using infrastructure, very sick patients, using infrastructure that was vulnerable.

And what I'd like to communicate is since WannaCry, how is it -- the second part of the question is how has it kind of shaped? Well, in order for hospitals to be hospitals, they have to be accredited. Part of that accreditation is having an emergency manager, incident response plan, etc. And please, out there in the audience, raise your hand if you think cybersecurity is a required point of preparation for hospital accreditation.

(Show of hands.)

DR. DAMEFF: To my knowledge, you're right, you're correct. It isn't the case. The most they have to do is a tabletop exercise that says something about technical failure, it doesn't even have to be cyber related. And perhaps they do a tabletop once a year and that

can be a tabletop simulating a hurricane, it can be a tabletop simulating an earthquake, it doesn't even have to be a technical failure, that's just one of the things on the list. So then since WannaCry, how has it impacted me? Well, raise your hand again if you think the physicians were taught anything about ransomware and how it impacted their care of patients since WannaCry.

(Show of hands.)

DR. DAMEFF: Wow, you guys are just as pessimistic as I am. None. There is none. And perhaps there was a drill done at one of the hospitals I worked at, I wouldn't know actually that the individuals involved probably totaled less than 20 and those are high-level managers, emergency managers, etc. So we really have a lack of information sharing with the ground-level clinicians, the nurses, the physicians that would actually take care of these patients and I think that lack of communication is startling and potentially dangerous.

MS. ZUK: Great. Not great, but -- thank you.

MS. ALFREDO: We're going to end on an uplifting note, I think we were told.

(Laughter.)

MS. ALFREDO: So I may have my timeline wrong but I don't think I do. So in our hospital association, we represent about 160 hospitals and health systems primarily in New York State but also in some surrounding states, and we had done our first cyber exercise with DHS a couple of months before WannaCry. About a week after that there was a major ransomware attack upstate, in upstate New York, that we all learned a lot from but we were pleased, to use a weird word, that we had done this exercise, we had invited regulators including the Department of Health and so people had at least started thinking about this stuff. When WannaCry hit, I think I was speaking at a compliance association meeting and learned about it that night and then really, what we did as an association is, you know, exactly what we do with all kinds of things, including other types of emergencies, which is

sort of fielding questions from members, trying to connect members to resources, disseminating information. I can't say that it was pursuant to any plan or that it was particularly systematic, but we served the function that we always serve for our members, which is to get information out and try to help them through it.

We have since then done a lot of thinking about what our role should be in cyber and what it shouldn't be, as well, and we've done additional exercises and we've partnered with state, local and also federal resources which we could talk about more later. But we had already been thinking about it, I think WannaCry sort of fast-forwarded that thinking to another stage and we're still, you know, very much in the process of continuing to evolve how we think about cyber as a hospital association.

MS. ZUK: Great. Chad, do you want to go next? I believe we'll just go down.

MR. WATERS: All right. At ECRI Institute, we fielded a lot of emails and phone calls from our member providers asking us if we could help identify what devices were affected by this. At the time, I don't think we were prepared for it but since then we have some initiatives to help field those questions in the future. I was actually working at an HDO myself as a network engineer and I was scrambling to identify things on our network that were affected and we did pretty well. We had probably compliance within the 90% and then we had to identify all the outliers. There's a manual process to do that.

MS. ZUK: Nastassia.

MS. TAMARI: So I think our ability -- can you hear me? Our ability to respond is really based proportionately on our ability for preparedness, so BD had a lot of the information that our customers wanted, who is impacted, right? From an HDO perspective you want to know am I impacted, are the devices I have impacted and then what can I do about it. So we were able to quickly gather that information and then work with ICSR and FDA to release that information through a security bulletin to customers for that type of

information and I think what we learned from that is we really needed to formalize that process of gathering that information.

And as, you know, security manufacturers, we have all the information, you know, what type of third-party products are in our devices, so things like SBOM, right, how do we kind of formalize that information and provide it to customers? So we formalized our product security white papers from that and so all of our products have a product security white paper that has that information. We have our policy and procedures, our incident vulnerability management plans and training that we routinely do on a routine basis.

MS. ZUK: Great.

MS. REKIK: Excuse me, can you please speak up? We can't really hear you in the back.

MS. TAMARI: Okay.

MS. ZUK: Thank you.

MS. TAMARI: I'll get closer.

MR. GARCIA: Okay, from a sector-wide perspective, I think WannaCry really was a -- it was a clarion call for the full sector and by that I mean HDOs and medical device companies, pharmaceutical, plans and payers, health IT, public health, they all came together really understanding that there are a number of approaches to preventing another WannaCry from happening and those are a lot of the things we've been talking about here and in the previous panel that I moderated, the health industry cybersecurity practices and the Joint Security Plan, we have efforts on workforce development, on intellectual property data protection in the cyber realm, on telehealth security, supply chain security, a whole range of things that, taken together, we hope it would sort of galvanize us, as a sector, to deal with that kind of ransomware in future attacks. And I think just the -- it was a clarion call, it was a wakeup call, we went from about 60 organizational members in October

shortly after WannaCry to more than triple that number now in a very short period of time because of a collective understanding that this is everyone's problem. So in that respect, WannaCry was a galvanizing event that brought us together in a cross-sector perspective.

MS. ZUK: All right.

MR. ROTHSTEIN: I had a much different participation as WannaCry came out. So AdvaMed is a trade association and we represent over 400 medical device companies. We are the largest, I think, by numbers, probably in the world now and that put us in a particularly, I think, unique position as this occurred.

So one of my responsibilities at AdvaMed is I manage the day-to-day work of our digital health efforts which includes our cybersecurity working group, and fairly quickly into the outbreak, HHS actually set up a task force, I would call it a task force, that's not really the right name, but a group that had daily calls every morning to walk through intelligence that anybody was hearing and compare notes and it was then our jobs, on the association side, to then disseminate whatever we learned from those calls down to our members.

I believe FDA was participating in those calls and HHS was doing a really nice job putting them together. That was before Greg came around, right, so that was kind of the way the associations within the healthcare space were trying to come together and disseminate information to their members during, you know, what might be this first, you know, real issue that we had to deal with as a whole industry.

The other piece that I found interesting on my side was I would've expected Congress to call HHS or FDA. They were calling our government affairs people. So we were getting calls from congressional staffers saying, you know, not only what is WannaCry but how are medical devices being impacted by it. So our GA team was not prepared for that.

And then the other space would be our public relations or PA side, public affairs. Being a large association, many press outlets and media individuals reached out for

statements, for information, from us. And it's not that I would say we were not prepared, as an organization, it's just that it was the first time we had to go through a process like that where there really was -- we needed a war room, basically, to be able to manage all the incoming issues. And so we have, you know, worked internally so, you know, if this type of issue does come up again we'll be in a better position to more rapidly respond.

But I think the other piece of what WannaCry did that I saw, from my perspective, working with our members, is that there's a much larger focus now around preparedness and response plans and anything from tabletop exercises to other simulated, you know, plans, we're seeing more and more of our members engage in those types of activities so that when they experience some type of issue they'll be in a position where it's more, you know, something that they've trained on and that they're just ready to enact whatever systems they have in place to do so.

MS. ANDERSON: So we had just finished our summit, our spring summit, and I was looking forward to having a day off and WannaCry broke and immediately our chat rooms and all the servers lit up. But I took away three things and I'll put a little spin on something you said, Zach, so three things that I took away with. One was it was a global incident but we didn't focus on it, initially. One of the agencies, not here in the room, but they did -- they thought that this was something happening over there and they didn't really start monitoring it until HHS actually said hey, this is something that's impacting and we need to watch it. Well, in the private sector side, we have -- I mean, cyber has no borders, so we were watching it from the beginning. So I think that was a wakeup call, one, is that global means everybody, right?

Number two was there was a lot of -- on your spin with the press, when the incident was breaking, there was a lot of false information out there. There was a similar campaign going on with -- called JAFF (ph.) at the time, and their indicators were being pushed out as

WannaCry indicators, so there was a lot of erroneous information that got spilled out, pushed out broadly in the press and among the security vendors in the rush to be the first to get the news out and it led people down wrong paths. So that's another thing from that incident.

The third was yes, FDA did eventually come to the table but they weren't on the first calls that HHS stood up and so medical device was brought in a little bit later in the loop, it wasn't first and foremost when that was happening, which caused a lot of confusion because there were people that were curious about medical devices and the impacts to the end users and so that was something that, you know, again, I think we learned from it and, you know, future calls have been really good about incorporating that but on that first call that HHS stood up and it was a good call, but they weren't part of that call. And so that was another lesson learned, I think, from that. So those are my three big takeaways.

MR. BASTANI: And so, first of all, I said I'm Assistant Secretary for -- I'm not Assistant Secretary for Preparedness and Response. I'm from the organization that's called Assistant Secretary for Preparedness and Response, just to make sure.

(Laughter.)

MR. BASTANI: Our organization is really structured, is responsible for preparing and responding to disasters, all hazards, pandemics, influenza-like germs, things that are going on, we get involved in there, or natural disasters, to make sure that the critical healthcare infrastructure is intact and it's available, the patient care is really safe. So when this campaign took place, we -- very quickly we realized that we need to deal with this just like any other hazard and we repositioned our -- we have a software that really mostly deals with these type of events, we repositioned it to deal with this attack and we brought in a lot of our internal experts to look at this to see what it is and disseminate information.

We learned a lot from that and to be honest with you, initially there was a lot of

confusion. There was a lot of misinformation, there was a lot of confusion, we were really concerned about the material impact it has on the availability of the critical infrastructure and we wanted to really do an assessment of what is the impact of this cyber incident on supply chain, for example, and what drug companies are getting affected. Would it affect the supply chain of availability of certain drugs? And at the same time we were also dealing with helping the community to recover from this.

The role that we played was really we played initially a conduit for sharing information, for -- a clearinghouse for information. We wanted to make sure that the information that gets disseminated are the correct information, that we distinguish that from all the other type of attack that was going on, like you said. And the lessons, one of the -- we learned a lot from there.

One of the most important things that Greg brought up is the value of information sharing and reaching out. There's just absolutely -- I can't -- you can't put a price on that. The people that got on the phone and shared their experiences, they shared their signature of the attacks, what they saw in their environment and they shared it with their colleagues and that -- really, there's a certain level of protectionism in the community. First of all, they don't want to share information about their environment and they don't really want to share this information about how -- what the impact is. But very quickly everyone realized that the more information they shared, the better off everybody is and that was very helpful. And that incident really increased that information sharing and that's what Greg brought up. And it also reshaped the way we develop exercises. We look at exercise and we execute exercises and the stakeholders that need to be involved.

MS. CHASE: Okay, so the first personal -- for me, personally, the first impact was during that regional -- workshop. I had a lot of distracted members in my breakout session because things were starting to happen and they just kind of wandered away, so -- but the

impact that really happened for -- you know, for MITRE was, you know, as FDA got pulled into either the ASPR calls and trying to help HDOs understand what was going on with devices, they realized that they didn't -- there weren't a lot of good processes in place for responding to a widespread cyber incident like this.

And so FDA asked MITRE to develop a playbook on medical device cybersecurity, a regional incident preparedness and response playbook, and the reason why it's regional is all those -- Denise said cyber is global, response tends to be local because you need your local law enforcement, you know, state departments and city departments of health, you know, your local fusion centers, they're the people who are going -- your peers, if you have to do searching, you know, your response is actually going to be local, so that's why the emphasis on the playbook was regional. And the playbook, it's preparedness and response, so it was really important to help people understand how they should get ready, a lot of it had to do with building up those relationships ahead of time so you would know who to go to, doing things like asset management and, you know, the things that you need to do to prepare.

And then for the response, we really wanted to look at existing, you know, standards for incident response, for emergency preparedness and outline how hospitals could go and create this response into their regular emergency response. And as Julian Goldman pointed out this morning, one of the first things we did as part of this effort was convene the workshop at the medical device plug-and-play lab that brought together people from the Boston, Massachusetts area to share lessons learned and a lot of those lessons helped inform the playbook.

MS. WOYAK: So I think one of the terms consistent is the idea of a wakeup call and I think about -- the cybersecurity professionals were very much aware prior to WannaCry of what could happen from cybersecurity. I think there were a lot of people who were

unaware and maybe clinicians or quality postmarket surveillance, all of the different areas within this space that didn't have a lot of visibility into what could happen from a cybersecurity perspective. So I think, for those people, it was definitely a wakeup call.

And for me, I know when I went to the ASPR and the HHS workshop or simulation that they did at the end of last year, it was really eye opening how much there is around the national perspective of how we would respond to a more global cybersecurity incident like this and I think that there's been a lot that's been done up until then and still is being done after doing that exercise in October of last year.

MR. GOMEZ: So this is probably going to sound weird, but for us WannaCry was an absolute blast and we had a ton of fun with it. The reason for that is we run something called a cybersecurity tactical operation center, which is kind of like a security operation center on steroids.

And so we started seeing activity of WannaCry around 2:30 in the morning Eastern time coming out of Asia and as it continued to move globally, as was stated, across the world, we opened up three war rooms. One was an interagency war room for government agencies, one was a constituent war room and one is what we call our inbound war room where people want to share information. You can go to that war room and say this is what I'm seeing, this is what I'm hearing, and that's usually a lot of FUD, but we take it inbound anyway just to figure out what's going on. But one of the things we -- because of that FUD, one of the things we really focused on early on was separating the FUD from the reality and one of the biggest questions, if you think back to that time was, is this a targeted attack against healthcare because we had seen what happened with NHS out in UK and there were a number of hospitals hit and so we worked with the intelligence community in the UK to figure out is this real, you know, is this a targeted attack, is it a target against any industry and the answer quickly came back that no, it's not, you just have a lot of old technology

because you have poor economics when it comes to your infrastructure in healthcare.

And so we were able to kind of communicate that out, so I think, from our perspective, it was a lot more calm than I think what a lot of people experienced, but I think it goes to really still illustrate, you know, the concept of preparedness and understanding that there needs to be a lot of preplanning, a lot of things which I'm sure we'll touch on as the panel evolves.

If there was any scary/funny moment during the entire thing, it was -- I was on a ferry between New York and -- sorry, New Jersey and New York and we had a conference call with three or four different agencies, I won't name who they are, but the lead agency, who was a federal agency, said to me well, what do you think is going on and it was a scary moment because -- and I think this probably played out in several different calls throughout the day was well, you're supposed to know what's going on, we're just -- we're private sector, we're guessing at it and if you don't know, then that's a bigger issue.

So I think it caught a lot of people off -- you know, a lot of people were surprised by it, unfortunately, because we all knew it could happen, I just don't think we were expecting it to happen when it did and I know we all believe it's going to happen again, so maybe hopefully the information we share here can help you not have -- maybe have a good time with it versus a scary time with it.

(Laughter.)

MS. ZUK: That's a positive thought. So we've heard a lot about the different perspectives from the different organizations. I think some of the common themes that came out were the different stakeholders not being effectively integrated, so this is really a topic that we want to move to next. And the role of exercises, we heard about a lot of different types of exercises that happened as a result of that, so I wanted to dig a little deeper into how those are happening because if they're not happening in your organization

you might want to, you know, reach out and learn from that.

So, unfortunately, Christian had to leave but we have some people at this table that have participated in Christian's exercises that he has built from that time. He was very concerned about the clinician knowledge and experience with this type of attack and has done some very effective clinical simulations as a result, so I know, Nastassia, you participated in some of Christian's so may be you could give your experience with that.

MS. TAMARI: Yeah, so we went to the summit in Arizona in December and, you know, we always talk about how, at the end of our medical devices, right, it's really patient safety that's the most important and during these simulations, you know, we saw ransomware on a computer that really needed to be functional in order to let the physician know what avenue to take, right, medically.

And so that was something that was, you know, really eye opening and we take a lot of that information back and incorporate some of it into our training, so we do mock incident response training as well. And so, you know, we gather our stakeholders in a room, at least in our organization, you know, from privacy to quality to clinical to even, you know, people on the phones who intake that very first call and we make sure that we test our policy and procedures in a cross-communication functional way so that when these things do happen we're better prepared for it.

MS. ZUK: Great. Josh, do you want to comment on that cyber --

MR. CORMAN: Yeah. Christian was sad he had to leave, but -- a few of you were there. But I think one key thing is there's a lot of people in this room that are parts of that ecosystem, but the way we phrase that entire CyberMed, too, was the last mile in that clinicians and hospital organizations haven't been doing the preparedness drills.

Just a tiny anecdote. The day that WannaCry hit, the number of exposed open SMB clients on the Internet measured by the cheap data scientists -- of seven, was like 100,000

or 500,000. A year later it was 500,000, it hadn't really changed. So these impoverished health delivery organizations, the economics we mentioned, really haven't made much modification and it's not like they automatically got new staff.

My call to this group isn't so much that we need to do more CyberMeds, which we do, we want to do more of them in more cities at your hospitals to get that visceral passionate experiential fail small/fail fast in a simulation instead of in a real-world kind of experience. It's also that I think we've got to give them collective nudges to lean into this topic before they burn their hand on the stove. So far every single simulation we've done has led to pretty catastrophic failures. The problem is we're teaching a dozen people at a time instead of hundreds or leadership figures at a time.

MS. ZUK: Great, thank you. So Laura, from your association perspective you're trying to address this in a broader sense, right?

MS. ALFREDO: Yeah. And I agree with what Christian said earlier and what Josh just said and we partnered with I Am The Cavalry and one of our members, Northwell Health, and a couple of other organizations about a year ago to do something that we billed as cyber at the bedside and, you know, through live simulations it was a very interesting -- a very interesting event, more than just raise awareness and to really dive deeply into what an attack on a medical device would really look like, and I think the clinicians that attended really got a lot out of it, including thinking differently about malfunctions and, you know, getting cyber kind of in their minds. But I'll be frank, it was not standing room only and it's very hard to get clinicians who, you know, work doing patient care to come to events like that, so we're thinking about ways of packaging that and getting the word out more.

In terms of more traditional exercises, I mentioned we did one in early 2017 that was really, you know, at the time -- I look back on it and think wow, we've come quite far, we need to go much further but at the time I don't remember thinking wow, we're really, like,

at sub-zero level, but we were and including sort of the interplay with the regulatory agencies in New York, so it was an enlightening exercise that we did with DHS back then.

We also, a year ago -- well, a little bit less than a year ago teamed up with John and Sensato to do an exercise, a two-day exercise, with members designed to get them to really figure out what the gaps are in their incident response plans. And I would say, based on that and based on what we and our members learned about the gaps, we've spent the last eight or so months really trying to help them build out incident response plans or beef them up depending on where they are and this issue of low resource institutions, we certainly have many of them in New York State. We also have very well-resourced institutions, particularly in New York City, and just getting them to learn from each other and getting the playing field somewhat leveled is an ongoing challenge.

We have another exercise with DHS coming up in May where we'll really be looking toward helping to develop a template for members, you know, particularly the smaller ones that need a little bit more handholding.

So I feel like we've been working on incident response and building cyber incident response for well over a year and still have a lot more to do and in the medical device space, we probably have even more to do. But one thing that we're very interested in is trying to continue to improve the relationship between the device manufacturer community and the hospital community and you know, clearly, it has improved but we have to do a lot more on that front.

MS. ZUK: Great. Denise, do you want to comment on -- you've had a lot of exercises on the ISACs.

MS. ANDERSON: Sure, yeah, we do. We do a lot of workshops and exercises, both tabletop, we've done capture the flag, and the other piece of it was the physical and cyber, so the blended threat series that we did last year where we did six tabletop exercises across

the country to get feedback on different issues, you know, looking at the physical impacting cyber and cyber impacting physical, so we've done, you know, quite a bit of work in that.

MS. ZUK: Great. John, do you want to comment? I know you worked with --

MR. GOMEZ: Yeah.

MS. ZUK: -- Laura but you've done more.

MR. GOMEZ: Yeah. So I mean I would tell you to do them even if you've never done them before and you just do them on your own. They're easy to do, there is a lot of material out there that you can download, and scripts and we'll do them. If you need help, we provide guidance on it.

A few things I would give you as guiding principles as you put these together, one is don't rationalize. We find a lot of people will rationalize oh, that will never happen, that could never occur. Don't rationalize, don't underestimate the audacity of an attacker and so the psychology or psychological component.

And the last thing is they don't have to be super sophisticated, you don't have to have scripts and networks and you can just sit around a table and do a "what if." One of the best practices we've seen in working with medical device manufacturers is that on a quarterly basis they just kind of have a roundtable with pizza and talk about what-if scenarios, if they were to happen, against their devices. And it could be as simple as that or much, much more formal, kind of the things that we're talking about up here. I'll give you one simple scenario you can take home with you is you have a medical device returned to your organization, it's usually returned to some type of support group in your organization. One of the first things they typically will do is connect that device to see what's going on and we will, nine times out of 10, when we're going through a simulation use that as a point of compromise, that the device was actually compromised at the hospital, comes back, now it's on your network because that network is very rarely, within the medical device

manufacturer, segregated. So play out that scenario and see what happens within your organization is a simple little thing you can do.

MS. WOYAK: If I could add to that.

MS. ZUK: Oh, sure.

MS. WOYAK: I think one more guiding principle would be to make sure that when you're doing your tabletops or your simulations that you have the right people at the table. So I think there's a way in which you could have the wrong people at the table, maybe the people who wouldn't actually be involved in a simulation or an actual scenario, whether it's the wrong level or the wrong functional area being represented, but I think if you don't have the right representation at those types of exercises you're -- you might be missing a really valuable opportunity.

MR. GARCIA: And that's a hard thing to control for, I mean, taking Denise's cross-country cyber impact on physical and physical impact on cyber, who are the right people. The Sector Council last October had a blended incident exercise, a ransomware that occurred during pandemic flu, and we had physical security people -- sorry, physical healthcare people involved in supply chain or emergency response but they were not cyber people, but they nevertheless had to be part of this and I think the takeaway on that one was, you know, there was a line. Somebody came into a breakout session on cyber and she was not cyber and she said why didn't we get, like, a Cyber 101 on this? Well, that's a good takeaway, that's the gap with what Laura was talking about, was -- a successful exercise is when you find failure because if somebody does need to be part of a cyber response and it's not part of their job normally, then that's a gap. That's a gap in your process and in your incident response. So I think that was one of the big takeaways for me, that failure can be success in an exercise, that's what you're looking for.

MS. CHASE: And just to build on that, having had the privilege of witnessing the

exercise that John put together for Greater Hospital Association of New York, they brought -- these hospitals brought representatives from everybody that you would want. If you read through our playbook, you know, they'll say, you know, you need to have legal, compliance, regulatory, your IT people, your security people, and the hospitals actually brought all those people together, it was just amazing to see them kind of interact with each other and, you know -- and you really needed all those people together to do that decision making.

MS. ZUK: And I think Christian's point was you don't often see the clinicians in those tabletop exercises and that's what he's really trying to address with his clinical simulations.

Yes, Bob.

MR. BASTANI: If I could add something, just an observation. I think the exercises, I see a need for exercises to become more complex to be valuable. For example, this is a really, really good forum because I -- just the exchange of information, it has, at least for me, exposed me to a lot of different possibilities.

There was some talk here about virtual hospital and the ability to -- you can -- having that kind of environment would allow you to design certain type of exercises that would mimic the real event and I can see possibilities with having -- you know, if you have a virtual reality type hospital and you can really design very complicated, complex exercise, it's difficult to do, but those kind of things, I think, in the future, if I look at it future-wise, those are the things that would add a lot of value to these exercises.

MS. ZUK: So one thing we had not addressed yet was what we might learn from other sectors. Does anyone want to comment on activities that they know about in other sectors?

MS. ANDERSON: Like in exercises?

MS. ZUK: Yeah. Or preparedness and response in general.

MS. ANDERSON: I think there's a lot of lessons learned across -- you know, definitely

from the financial sector in the DDoS attacks of 2012-2013. There was a lot of lessons learned and they weren't all technical, you know, it's getting the right stakeholders in the room, you know, simple things like establish one person to make a decision that, you know, had the trust and the authority to do that on behalf of the organization because a lot of times you didn't have time to react or do things by consensus, right, which was the typical practice before that. And then you know, making sure that there was a bridge for your technical people and then a bridge for everybody else. And then bringing in the right teams, like business teams and communication teams and that kind of thing because a lot of times, in responding to the incident, they just brought the technical people to the table and that was a lesson learned for them.

There's certainly a number of exercises. I know that, you know, GridEx was mentioned before, so a lot of the ISACs will open up their exercises to other ISACs and allow for cross-sector participation, so there's certainly any number of events. And I would encourage you to go to any one of the ISACs. If you go to the National Council of ISACs website you can see all the various ISAC members there and you could go to their site and they'll have their various exercises up there.

MR. GARCIA: There was something I experienced in the financial sector, I was also previously executive director of the Financial Services Council and there was an incident that happened and the impact -- well, this was a matter of incident response and information sharing that this particular organization was not able to get details, certain details, out to the broader community so that the rest of the financial sector could take protective actions and the reason was, was that the organization, when it was hacked, pretty much immediately went to law enforcement for investigation and once you're in law enforcement, you are -- you know, you are constrained from sharing information when it is a matter subject to investigation.

So, you know, as a sector we talked about how do we stop -- you know, how do we deal with this and then I think there was a general agreement that let the sector know first, then go to law enforcement because you really need to ensure that the rest of the community has an ability to take protective action before it gets out of hand.

MS. ZUK: Axel.

MR. WIRTH: So as we're talking about a blueprint for preparedness and response, which would be a sensible exercise to develop basic categorizations of time of attacks and incidents, right? I mean, Christian's example of a patient with a pacemaker that is being attacked is very different from WannaCry impacting care delivery, it's very different from Petya impacting availability of drugs and vaccines. So there should be, in my opinion, a basic structure which says okay, this type of incident, therefore we need these stakeholders and these are the key decisions and key steps you undergo. But I think we shouldn't assume that they're all the same, they're actually all quite different.

MS. ZUK: Right. Good point. So I think --

MR. BASTANI: Can I make a follow-up point? That's an excellent point and the incident responses that we have generally are based on network incident response management. Those are the playbooks that people pull although it's a cyber incident, but the impact of a cyber incident to medical devices is different, much different, and the response needs to be different and the response also needs to be different depending on what the attack targets. So that is something that we need to mature on, to develop a specific incident response plan.

MS. ANDERSON: And one more thing, just here's a scenario and this is real, from Petya. The organization, within 90 seconds, lost all communication, so -- and all of the contacts lists are where? In your computer. So phone, email, all that was gone.

MS. ZUK: So, unfortunately, we have to wrap up. I think the goal we all have --

we've heard here a lot of positive steps that have been taken since WannaCry. I think what the sector needs to do is make those learnings available to everyone else, you know, and I think we've had a lot of suggestions today, so I think people will all take it upon themselves here, in their different parts of the sector, to share with everyone else. So thank you very much, I think we're done.

(Applause.)

DR. ROSS: Hi. Good afternoon, everyone. We are getting ready to end the workshop but before we do, we just wanted to give a quick highlight of some of the things we got out of the CYMSAB discussions that we had today. We were very happy to see people so highly engaged in the various breakout groups both here in the room as well as online and so we wanted to share a couple of those highlights as well as give some parting remarks.

So there are a couple of things that came across the different groups both in the room as well as those who participated online and there were a lot of -- there was a lot of discussion about, you know, what the vision is for the CYMSAB, you know, what is it, what is the value add, what are we looking to get out of it. And part of the reason we were purposely somewhat vague with regard to that at the beginning of the session is because we really wanted to hear from our stakeholders what would be of value as it relates to trying to address challenge areas that you have and trying to quickly address vulnerabilities that are potentially high-impact, high-consequence vulnerabilities. We got some good feedback from that that we'll be going through, but we did want to make sure that people understood that once again we didn't want to do anything that would not potentially be value add and that we also can't move forward with this unless we get some additional congressional appropriations; this is really still in the formative stage and that's why it's a good time to get in and get feedback from all of you.

We also heard about, you know, well, what types of stakeholders should be involved in the discussion and I think we heard resoundingly that it should be a cross-cutting group of stakeholders and, for us, one of the new things that we heard was that it would be important to include patients here.

And this is kind of also related to some of the input/output discussion people were having, so they were asking what actually would be the inputs to the CYMSAB and what will be coming out of it. And some of the things that came up as far as inputs had to do with maybe some of the risk scoring systems being inputs into it, threat models being input into the system, but what about what comes out?

And so we heard things about potential things related to communications, webinars, after action reports and things like that and that's where I think people thought that having the patient voice would potentially be of value to have with some of that communication back to that particular stakeholder group.

One of the key things I think that wraps up everything that we were talking about with regard to CYMSAB was really trying to make sure, even though this is a postmarket, if you will, response type of an activity, to really take a holistic look at it. So we talked a lot about total product life cycle and how the things that we learn from our postmarket activities should feed back into the premarket activities as well. And so that's why one of the suggestions we heard in a couple of different groups had to do with how do we share some of those lessons learned with the broader industry such that we're able to then pour that back into the premarket activities and that was a good suggestion as well.

So we wanted to thank everyone for taking the time to go through the breakouts with us, to be engaged, because it was very helpful for us to hear some of the different concepts that were coming up as a result of these discussions.

Over the last 2 days we have had a lot of great dialogue, and it's really because

we've had a lot of active participation from those that are physically present, as well as those online, and we really wanted to thank everyone for that. We have found these workshops to be highly valuable because of your active participation. We wanted this to be a two-way communication so we didn't just want it to be FDA speaking to industry, but we also wanted to get feedback from industry, as well, on our premarket guidance draft. And even though we had a condensed scheduling for some of those discussions yesterday, we still got a really -- a lot of fruitful discussion that came out of that and we really want to thank you for that. It will help us as we go through next steps as it relates to trying to update the guidance.

I also, though, would be remiss if I do not thank the FDA staff that have helped to make this event possible. I want to thank both -- a lot of the staff that came out of the Office of Center Director, in terms of helping us with a lot of the meeting logistics that happened here as well as planning some of the content for the workshop, from the cyber team, so I really wanted to thank everyone for all that effort. Yes.

(Applause.)

DR. ROSS: And then we wanted to -- we wanted to also make sure that we thanked our panelists and our moderators. We could not have had the rich discussion that we had today if we did not have their engagement early on and coming to some of the pre-meetings for this particular workshop such that we could make sure that we hit some of the high notes, to help to inform some of the breakout discussions that were had, so we really want to thank all of them. And then a lot of you also helped us because you were facilitators for these breakout groups and we could not have done that without having active attendees who said yes, I'll answer the call, I'll be a facilitator for those groups. We really, really want to thank you for that because that is -- allows us to get more content, more feedback then we could get if we just allowed for, you know, folks to come up to the

microphone. So let's please give all of those folks a hand of applause as well.

(Applause.)

DR. ROSS: So again we want to thank all of you for coming to the meeting, for making it a fruitful discussion. We wish you safe travels back to wherever you are coming from and I will allow for Suzanne to give a couple of remarks as well.

DR. SCHWARTZ: I just wanted to make sure that everybody who's in the room here as well as those as who are still listening online give a round of applause to Aftin Ross and Reid D'Amico from our team here who -- you can't imagine the amount of work that has gone into putting this workshop together, particularly because it was during the shutdown. Even if you would've taken that part of it away, it's still an enormous amount of heavy lifting and there was so much going on behind the scenes prior to these two days as well as while this workshop was on the continuum.

So I want to recognize these efforts. This workshop would not happen, certainly would not be a success, it would not happen without their direction and their leadership and I am very, very fortunate and very blessed to have them on my team here as colleagues and really, as advisors in how we proceed, so thank you. And I really want everybody to applaud them. Standing ovation, please.

(Applause.)

DR. ROSS: Okay. Thank you. And with that, we'll adjourn. Safe travels, everyone.

(Whereupon, at 4:37 p.m., the meeting was adjourned.)

C E R T I F I C A T E

This is to certify that the attached proceedings in the matter of:

PUBLIC WORKSHOP - CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES

January 30, 2019

Silver Spring, Maryland

were held as herein appears, and that this is the original transcription thereof for the files of the Food and Drug Administration, Center for Devices and Radiological Health.

_____

TOM BOWMAN

Official Reporter