Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis

May 18-19, 2017

Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD, 20993

Day 2 May 19, 2017
1:21 p.m. - 3:53 p.m.

TRANSCRIPT OF MEETING May 19, 2017

TRANSCRIBER: JANINE THOMAS
NOTARY PUBLIC

(Proceedings recorded by electronic sound recording, transcript produced by transcription service.)

VERITEXT NATIONAL COURT REPORTING COMPANY
MID-ATLANTIC REGION
1801 Market Street - Suite 1800
Philadelphia, Pennsylvania 19103
(888) 777-6690

I N D E X

John Hatcliff and Stephanie Domas

Discussions 69

DINESH PATWARDHAN: As you can see we've thinned a little bit, but I really appreciate, we really appreciate you staying through the readout session. I listened in on several sessions since yesterday and there were robust discussions in small and large groups.

What we're going to do today is to have a first readout by the session chairs. And this is going to be for five minutes each, so that we get a scope cross the entire two breakout session, one yesterday and one today. We will have time for discussions which will be after the break. Just so that we are all aware. This is again, the big room and we are being webcast.

So the -- what I'm going to do for the session chairs, I will call the session chairs and then we will have a readout of just the highlights in five minutes or so. Our goal is to have a discussion after the initial readout so that you can see across the sessions if there are common themes and then as a result of that maybe we can combine several common themes and that type of discussion we can have once we have all heard, because I also have not heard, I don't think anybody has heard what happened in sessions one through eight, yesterday

and one through six today.

So what we're going to do, I was just, we are doing this live is that as the session chairs read them out we are going to capture it on stickies. Try to capture the main sense, the main point of the readout on a sticky and we are going to do an affinity diagram as I will call it.

We will, so as we do the discussion maybe that affinity diagram makes a little bit more sense. I don't want to be here and keep on stretching this out. If somebody has a burning question I'm open, otherwise, we'll just get started. Okay.

Yesterday's session, breakout session one was Relationship Between Medical Device Security and Patient Safety and the moderators or session chairs were Ken Hoyme and Anura Fernando, so is -- I ask see Ken here. Oh, please come up to the front. So the -- you can stand at this table and say your few words.

RELATIONSHIP BETWEEN MEDICAL DEVICE SECURITY AND PATIENT SAFETY

ANURA FERNANDO: So, I'll start off. You know, we had the same topic in two of the session and so there

was quite a bit of overlap and so Ken and I will sort of, I think combine efforts here.

In the session that Kevin Fu and I were leading we really honed in on two key areas, you know, after going through a number of questions. One was asset management and not only from the individual device perspective and understanding, like the bill of materials, for example, on the components that comprise that product, but also from or of an HDO perspective understanding, you know, what assets are available, how those assets are effected by the kinds of events we've seen over the last several days and that type of thing.

And so understanding assets, understanding where vulnerabilities exist and complex systems whether they're systems that are themselves products or the health care system itself was one of the key topics.

Then another one that came up was education and workforce. And so making sure that individuals that are involved in cybersecurity understand the multidisciplinary nature of this and have both an understanding of the clinical domain and potential impact on safety as well as the technical domain

associated with understanding how vulnerabilities may play out and manifest and those were some of the key areas, you know, recognizing that there wasn't a sufficient workforce and that we needed to understand what disciplinary areas needed to be focused on to build that workforce and then once we have that workforce in place managing assets both at the product level and at the system level.

KEN HOYME: So we functioned slightly differently, but I probably I think touched some of the same kind of topics and we had split the group again into two and we started out with a set of questions that had been seated by the four of the moderators that had worked with this particular topic and then spent time brainstorming additional questions from the group and then did dot quoting to focus on which we were going to speak through and then we had, so we had four of winning questions that we each then spent about a half hour going through the post-it note, an affinity map so Eugene has all kinds of post-it note filled paper with the details and background to these four questions.

The four questions were that we ended up

discussing was how could we -- one secure an institutional ecosystem of devices ranging from legacy systems, state-of-the-art systems --

UNIDENTIFIED SPEAKER: Can you slow down, I actually do have to write these down?

KEN HOYME: I e-mailed these to you.

UNIDENTIFIED SPEAKER: I know.

KEN HOYME: Oh.

UNIDENTIFIED SPEAKER: I still need to write them down.

KEN HOYME: Okay. How --

UNIDENTIFIED SPEAKER: Thank you.

KEN HOYME: You're welcome. How can one secure an institutional ecosystem of devices ranging from legacy system, state-of-the-art systems and BYOD products? And so then we talked about the various different kinds of ways one would go about securing them, you know, dealing with some of the legacy issues. Whether or not there is a -- devices that could be used to insulate legacy devices to risk management to incentives, getting management aligned appropriately so that the finances and things are put in place necessary

to do the securing of it.

We also, I think in that, talked about what we would need to do for small manufacturers in terms of or small hospitals in terms of provides some profiles and things that might help a small hospital secure, given that they don't have the same kind of resources.

Second question we talked about is what are the requirements for a common reporting framework for medical device cyber-incidents, so how do we detect when something is incidents, so, yep so this is more real-time behavior of how does a hospital in their security operations center also get information about what's going on with devices so that they can track and manage and respond to devices and how might that information then be fed to the manufacturers of those devices so that the manufacturers can do the long-term trending, also can do the response for patch management if something like that is needed, so. But we ought to recognize that it's not probably, but I think as manufacturers we tend to do this is building something that sends information back to the manufacturer as part of our software deployment process, putting the

manufacturer in the loop for incident response is not the right thing if it's short-term and need to do something about what's going on on the floor right now it should be within the -- in the hospital.

Third question was what steps can we take that will improve the culture of security cross the ecosystem and this is where we got similar to what Anura just talked about in terms of a lot of things about training and education and how do you make people aware. How do you make day-in-the-life videos of what a nurse actually does on the floor so you can recognize how these devices are getting used? How do we improve things from an education and experience perspective?

Last question we tackled was what techniques can be used to create usable authentication in a wide range of clinical settings including homes. So this is that authentication problem and we talked about biometrics and talked about all the various different ways that you might consider authenticating devices. We recognize that if we solved the authentication problem in that context that we should patent it. I don't know that we came up with something unique yesterday that

solved the authentication problem, but we did generate some material to, I think that's, you know, an area that certainly would require some research.

UNIDENTIFIED SPEAKER: And you were setting incentives.

KEN HOYME: Yes. So.

ANURA FERNANDO: Just as a closing comment there. So it was kind of interesting to see that breaking two separate groups out and going through the same set of questions there were -- there was effectively only really one area of significant difference, you know, between those two, so people are identifying the different, right.

KEN HOYME: We all tend to agree that the big problems are the big problems.

DINESH PATWARDHAN: Thank you. Does there other -- Chuck or Kevin, do you have -- are they here? Kevin, do you have anything to add?

KEVIN FU: Yeah, I'll just add just a little more color to what Anura just said. The big problem with safety and security is really just figuring out how to select, you know, what are the methodologies do we

need to be able to figure out what part of security truly does affect a central clinical performance and all the questions that we prioritize those nine questions or so, really just drill down into that one little piece, but as we're not trying to solve the problems today I don't think I'll go into anymore detail, but we had good consensus around those questions. The details are in the scribe notes. The two scribes have sent them in. Okay.

UNIDENTIFIED SPEAKER: If you're a second chair or the scribe and I don't have the notes from your session, please be sure that I do.

KEVIN FU: I'll just repeat for Eugene. Scribes, send your stuff to Eugene if you haven't.

UNIDENTIFIED SPEAKER: Are you going to say everything I say?

KEVIN FU: I'm going to say anything Eugene says.

UNIDENTIFIED SPEAKER: Okay.

DINESH PATWARDHAN: Okay. Thank you. I'm going to move onto the second breakout session, second pair, because we had two. Unique Security and

Regulatory Science Challenges for Medical Devices and Bo and Michelle and Nick and Mike. So I don't know what, if they have -- okay. We can go with Michelle and --

UNIQUE SECURITY AND REGULATORY SCIENCE CHALLENGES FOR MEDICAL DEVICES

MICHELLE JUMP: Okay. So just to clarify, I can give you the topics that we kind of came up with in the big bucket discussion, but a lot of them had multiple questions that were associated with them. So do you want me to go through all of the questions, because that's all in the notes?

DINESH PATWARDHAN: Yeah.

MICHELLE JUMP: Or can I just give you the high level kind of --

DINESH PATWARDHAN: High level.

Unique Security and Regulatory Science Challenges for Medical Devices

MICHELLE JUMP: Okay. So it's really fruitful discussions in our group. A lot of it boiled down to, I think kind of four different areas that we focused on. The first was how do you determine a good base level

expectation around security. Those of you may have seen the IEEE building code for medical devices looking to expand on something like that were some good practices that should be considered foundational for medical device manufacturers, not mandatory, because every product, there's a lot of diversity of products, but looking at ways of getting a good idea of what's good enough, what's a good foundational practice for mitigating security and hardening devices.

The second one was around I guess I would just say responsibility agreements and whose responsible for what better defining that shared responsibility between all the different stakeholders and I guess I would say beyond just the manufacturers and the HDOs, because there's a lot of other people who are responsible in this space as well. So we talked about a variety of ways we might look at that.

The third bucket was around communication understanding two levels of communication. One, how could we get better communication between all those stakeholders so the right information gets passed along and two, how do we get a better awareness campaign for

what's expected from manufacturers and what resources are out there.

That was the third one and then fourth was really looking specifically at the home health area, we thought that was a space that we focus so much on health care delivery organizations that it would be really beneficial to get some better clarity around what's needed in the home health care situation.

UNIDENTIFIED SPEAKER: Yeah, there was more detail underneath that, but.

MICHELLE JUMP: All folks. Yeah.

UNIDENTIFIED SPEAKER: That's kind of what it rolled up to and we saw a lot of what was in here had overlap with what some of the other groups had and so when we came in here yesterday for the debrief we ended up putting a lot of this into some of the sessions that we did today, so if some of those themes sound familiar it's not by accident, it's because we worked on some of the output of that today.

DINESH PATWARDHAN: Thank you. Nick and Chuck.

UNIDENTIFIED SPEAKER: So there was a lot of overlap with essentially, with both last groups said,

but there were a couple sessions today that came up as a result of some of the topics that we talked about and I thought one of the biggest areas and really where the industry as a whole can probably benefit the most is around essentially having these example or sample threat models, a register that can be used when you're doing your risk assessment submitting to the FDA.

What specifically prompted that was a question around essentially manufacturer submits their device, the FDA gets a response in return saying did you consider this threat or this threat? And having some source of information to start with would be very helpful to the space. But inherently that is only what should you consider from a threat side, it doesn't talk about what good looks like. So that was one of the other areas that came up is and you know, it's nice to know what the all the risks are, but how do we know when we've put in the right things, or you know, we don't have the cybersecurity professionals to understand what good looks like and, you know, we're not going to necessarily hire a third party to tell us so having some document or something out there that really establishes

the sum of leading practices to build into security and have the security by design approach was important.

One other area that came up and whether it will be done or not is another story, but having someone like the FDA or some body provide real actionable security by design guidance, so the example that we walked through was essentially, you know, the FDA saying, you know, we approve these tools for use with static code analysis, because they do a thorough job and you can trust the results, so those are some good key areas and then lastly was the hospital versus home use, so unfortunately, we were very manufacturer centric in the room, we didn't have any hospitals, so it was a one-sided conversation, but having guidance around, you know, what you may be able to consider transferring to a hospital and that being inherently different than what you have to build in for a home network that you have to basically assume that they're not going to be putting those mechanisms in place.

UNKNOWN SPEAKER: So without trying to be -- not redundant at all, I guess we had a long open discussion that included a number of areas and I just

kind of jotted down some of the main -- some of the main themes which help sort of feed into today's, you know, topic generation and sessions.

I know we had a little bit of discussion, I said is, is just know it at a different, you know, requirements and needs for different environments of use. Certainly, some of the manufacturers brought up the either challenges of doing V and V and rolling out new software in an expeditious manner with respect to testing fixes related to cyber-threats and the demands of say the client or the hospital whom to get them out as fast as possible.

There was also, I guess with respect to the threat models, particularly, you know, some of the, you know, manufacturers in the room discussed, you know, just kind of, what kind of libraries they were talking about, like, you know, wireless in the hospital versus wireless versus home versus stationary and, you know, that kind of categorization.

There was also raised a need for possibly some well done, they cited some, I think, Mayo Clinic examples of empathy videos for education components for

the life folks in the hospital to help increase awareness and understanding of sort of, you know, of these kind of problems and what it means to them and last thing, at least on my --

UNIDENTIFIED SPEAKER: I'm sorry, I missed that.

UNKNOWN SPEAKER: What is that?

UNIDENTIFIED SPEAKER: Who's the audience for that? For that --

UNKNOWN SPEAKER: That was lay folks. They were thinking -- the thought was the lay folks, like the -- lay folks, meaning, not lay folks, like the patient, they were thinking like the nurses and as well as, I think the people that's worked in the hospital not the -- and the example was given, I think, I don't remember who gave the example, like the empathy that are, if you -- Mayo Clinic does, you may have seen them, they're actually quite well done.

UNIDENTIFIED SPEAKER: The Cleveland Clinic.

UNKNOWN SPEAKER: Oh, Cleveland Clinic. Oh, you brought it up, but somebody else I think brought it up in our too, as well. Yeah, but you mentioned that it

was Cleveland Clinic, right. Cleveland Clinic, sorry. Correct, thank you. Cleveland Clinic. But it was also -- it came up in our group, but I guess Bo, we discussed it later. And also the -- there was some discussion that was sort of, you know, at least highlighted in my notes regarding, you know, something similar to echoes, not echoes, Energy Star for like appliances, you know, like cyber-star or whatever you want to call it for certification of some sort of minimal set of requirements relative to cybersecurity for devices and I think that's it for me. All right. Thank you.

DINESH PATWARDHAN: Thank you. Next readout is Roles Intersection of IT Professionals and Bio Meds, Ray.

THE ROLES AND INTERSECTION OF INFORMATION TECHNOLOGY AND PROFESSIONALS AND BIOMEDICAL ENGINEERS

RICK HAMPTON: So for yesterday we had the breakout session three which was Roles and Intersection of Information Technology Professionals and Biomedical Engineers and the first thing we did is we did establish that there is a needed intersection.

UNIDENTIFIED SPEAKER: Please slow down.

RICK HAMPTON: I will. You didn't need to capture that. It was a horrible joke that no one laughed at, so.

UNIDENTIFIED SPEAKER: Reboot it and tell it again.

RICK HAMPTON: It never gets any better.

Okay. So basically, what we tried to do was to look at it at operations inside the hospital where you have the biomedical engineers maintaining the medical equipment. The IT and the security people maintaining the IT network, how those things merged and where that system, you know, where the tendrils of that system go.

Let me look at my notes here, because I am sleep deprived and I can't even remember my name right now. So part of the things that we came back to is and this is a big surprise to everyone even at that intersection there was an information shortage and we, you know, so we wound up talking about a lot about how do we share information between the IS Department, the Security Department and the Biomedical Engineering Department so that we can secure these things.

There is, forgive me, one of the questions that came up was, you know, for example, do we need a DHS type cert for medical devices? We've got the ICS cert, they go out and they look at things. They feed that back to, you know, the ICS folks. And while they're doing that now, for medical devices, you know, from the hospital perspective the stuff that they have doesn't necessarily work in the hospital environment neither for the biomedical engineering clinical engineer groups or the IT security people.

It's one of those close, but not quite things and so that was one of the question, you know, do we need to have some kind of a governmental agency who's looking at that to provide us better service in health care? We don't know. We kind of think that's an issue.

One of the questions that came up was, you know, the concept of certifications for equipment from device manufacturers, because when we get stuff in the hospital we have to, you know, look at it and see, you know, how are we going to put it in our network, you know, is it, you know, how do we know that it's fit to be put on our network? Well, we have some kind of

assurances from the FDA on the basic device itself. We don't have that on the software side. So one of the questions is we, you know, should we have some kind of software certification that we can look at together to determine whether or not the device is, you know, fit for consumption, if you will.

Then the question came up, what's the lifetime of that? What does the certification really mean, you know, how long is it good for, if, you know, once it expires? And that's important, because we've got these devices that, you know, even if they're brand new today they will be tomorrow's legacy devices. You know, so we're trying to solve this legacy problem today. We're trying to figure out a way of keeping the new devices we just -- everyone knows are going to be safe, are they going to become tomorrow's legacy device and repeat this mess all over again?

So those were some of the things that we needed or that we thought we needed to look at and I got a whole bunch of notes here I could ramble all day long. Is that fine for you right now? Okay.

DINESH PATWARDHAN: Thank you.

RICK HAMPTON: Can I make --

UNIDENTIFIED SPEAKER: Just send them over.

RICK HAMPTON: Okay. You got them last night. Can I make a personal plea? Is that the camera that's live? Okay. I'm going to assume it is. If you're in a hospital and you're watching this I want to know why you're not here, because there's like 12 of us in this group of 300 people and in all seriousness we try to do a good job to respect hospitals, but as someone pointed out you really don't want me representing your hospital. Come defend yourself.

DINESH PATWARDHAN: Thank you. Okay. We move to the next one, Potential Metrics and Evaluation Tools to Test and Quantify the Security of Medical Systems and Devices, John Hatcliff.

POTENTIAL METRICS AND EVALUATION TOOLS TO TEST AND QUANTIFY THE SECURITY OF MEDICAL SYSTEMS AND DEVICES

JOHN HATCLIFF: All right. Thank you. So we were trying to think about, well, what are all the different aspects involved in either coming up with metrics and tools or improving them and so forth? So we started to think about first of all, the need to have

reproducible aspects, you know, whether it's talking about reproducible testing methodologies and techniques, reproducible outcomes, reproducible metrics, so, we started, first of all, sort of identifying sort of the things that help us normalize testing activities and one of the first things you think of is appropriate standards. So the nice thing, you know, we heard yesterday Anura Fernando talking about the emergence of the 2900 family of standards and so we talked about the ability to sort of use that as an initial test case, if you will, to see the extent to which a standard like that could help us normalize testing for security issues and then that raised the issue, well, if you have such a standard how do you normalize across the different test houses that might be supporting that.

So there was one particular thing on the issue of getting repeatable testing methodologies. On the side of getting reproducible metrics, one of the things that a number of groups came up with is the need to have more of a standardized way of reporting the bill of materials on a device, so that fed into some of the discussions today. But one of the things that was kind

of a novel aspect of some of the discussions in our group since we were focusing on tools was can you imagine any sort of tooling that would be built into devices in the future that you would use to automatically report or generate that bill of materials and then once you get that automated bill of materials, how can you then automatically link that to your vulnerability assessments and so forth to create a profile that feeds into your inventory management. So those issues came up in a number of breakout groups which, you know, fed into the discussions today.

Just like the previous group we also identified the need for better sort of community-based organizations that focused on sharing, so the clearinghouse concepts and so forth, so I won't go into the details of that.

One of the things that came up for us is we tried to think about metrics. There was a discussion of the need to recognize that since the security space and challenges are so dynamic that we need to recognize that the metrics themselves might somehow be dynamic and we talked about in that context the need to distinguish

between metrics that are applied preproduction where you have sort of a static object, you know you're evaluating it, you release it and then metrics that are used in postproduction. So in particular, you know, the need to be able to rapidly and dynamically update sort of the metrics or the profile associated with the devices vulnerabilities.

So another issue that came up for us related to metrics and reporting was the fact that in the modern world when you have a thing in the medical space that you're interesting in reasoning about security it's not just the device anymore, you know, the device is connected to a network and there may be different modes of connecting whether it's peer-to-peer across some sort of hub and spoke out into LAN and into the broader area hospital. So we wanted to be able to score, create metrics based on the architecture, right, so be able to say, oh, we're talking about metrics or issues within this particular point or characteristic of an architecture so that require us being able to do both modeling of architectures and have a somewhat normalized way for discussing architectural issues as well as ways

of tracing vulnerabilities to particular points in the architecture.

So finally, we kind of concluded with some of -- some things that were roadblocks to what we were trying to do; right. Even the most basic things related to testing, penetration testing, scanning and so forth, we heard mention in some of the opening talks that it's very difficult to even approach some of these things because some of the devices that we're producing now are not robust with respect to scanning, you know, you scan a device it actually brings it down, so come up with sort of basic foundational issues to be addressed in the design of devices so that they're more amenable to this type of automated testing that we need to do.

We also talked about again, how metric obsolescence in the face of dynamically changing security context. And finally, the need to have better threat models that allow us to even justify trying to build a tool that would try to get us some sort of standard approach to threat characterization.

DINESH PATWARDHAN: Thank you. The next one is Automated and Manual Tools for Communicating Security

Information About Medical Device Design and Function, Stephanie Domas.

AUTOMATED AND MANUAL TOOLS FOR COMMUNICATING SECURITY INFORMATION ABOUT MEDICAL DEVICE DESIGN AND FUNCTION

STEPHANIE DOMAS: Hello, everyone. Stephanie Domas from Batell [ph]. So our group was talking about the automated and manual tools for sharing vulnerability information. So our discussion kind of focused around four main areas and the first one was kind of how do we share information, so what are the mechanisms that a manufacturer can use to disseminate information about a vulnerability?

So we talked about the ISACS [ph], we talked about individual websites for the manufacture, there's social media, there's mechanisms like ICS Cert and then there's trade organizations. So one of the gaps we identified in that was we felt like while that involves stakeholders like hospitals, purchasing groups, manufacturers, most of those weren't going to be a successful means of communicating with the individual patients, so if things like home care use devices they're probably not watching NH-ISACs website. They're

probably not looking at their manufacture's website to see is there a vulnerability that they need to be concerned about. So that was kind of one gap was that the information sharing mechanisms that are out there right now for vulnerabilities are overlooking getting information to patients.

So we talked about, well -- so we have mechanisms for disseminating information, but what kind of information do we share through those mechanisms? So some of the information we identified was, you know, is there an update? Should you be applying the update? And did the update work?

One of the other categories we talked about is in the information that you share there are so many mechanisms and possible ways that you can kind of rank the severity of a vulnerability that it becomes hard when manufacturers are sharing information to compare apples to apples. So if one manufacturer says they identify a vulnerability and they've ranked it internally as a low how would you know if that would rank as a low by your own manufacturing processes? So everyone using different ranking mechanisms makes it

hard for people who aren't cybersecurity experts to look at your criteria and say whether or not they agree with your ranking mechanism and then we also felt like there was a potential regulatory gap around guidance about what level of threats should be shared. So that we had a lot of discussions around if I get to the point as a manufacturer of if every single cybersecurity threat that comes to mind is something that I push out, it's just going to become alarm fatigue. If I push out all of thousands of different internal vulnerabilities and small things then I might become aware of it's too much information.

So is there a barrier where say, all right, well, if everything is ranked using for example CVSS version 3, is there a cut off that says, well, maybe everything ranked over a 5 should be shared and everything below a 5 maybe shouldn't. So we didn't have any resolution around that, but just we felt like that might be a potential gap and that there's not clear guidance on what you should be sharing and what you shouldn't be sharing so that stuff's gone through a little bit of vetting and that everyone is speaking the

same language with the information that's shared.

DINESH PATWARDHAN: Thank you. The last one for yesterday, Best Practices in Security Design, Deployment, and Post-Deployment Activities and Procedures, George Samaras.

BEST PRACTICES IN SECURITY DESIGN, DEPLOYMENT, AND POST-DEPLOYMENT ACTIVITIES AND PROCEDURES

GEORGE SAMARAS: One moment, please, he said. Oh, okay. I am George Samaras. Oh, okay. One more moment. Go ahead? So best practices arise from bad experiences. They get codified in textbooks. They get codified in national, international consensus standards and they get codified in regulations and guidance documents. And we have lots of best practices above and beyond those related to cybersecurity and not all of them are followed, so we need to keep in mind that best practices are nice to know and nice to have, but they may or may not solve a particular problem.

One of the big issues that seemed to be of importance to the group yesterday afternoon was who owns cybersecurity? A lot of emphasis in the group on manufacturers owning it. My personal opinion is I

disagree with that. I think it is a shared responsibility, it can't be anything but that and yet there was a great deal of concern that it was manufacturers' responsibility. It was manufacturers' -- under manufacturers' control. And another question that came up related to that was what role does the FDA play with that beyond manufactures? Because the FDA only regulates manufacturers not hospitals in the practice of medicine.

The central theme with regard to best practices was trying to reduce cyber risk and we were concerned both with premarket and postmarket, basically the whole life cycle which is development, deployment, clinical use, clinical servicing and then disposal.

On the postmarket side and especially with the emphasis on legacy devices when do you add cybersecurity if you don't already have it? Whether is it appropriate to retrofit existing devices? When to label or relabel. How to incorporate cybersecurity into service and one has to consider "patching, updating" and other modifications to be a service function. And then what are the minimum set of activities that one needs to do,

because remember we are dealing with a medical device manufacturing community and a health delivery organization community that range from very, very small to global multinationals.

The third point was a regulatory gap was identified and so I'm not quite sure how one approaches this because of the bar on talking about policy, but basically the question was what is the FDA going to do about requiring devices that are constructed in an interoperable manner. That means you've got ports. You've got connectivity to basically implement the requirements for cybersecurity. And I think that's a question that the FDA focus need to address.

The only other thing that I wanted to comment about is that in terms of legacy devices we had a nice definition this morning about legacy devices being those that haven't yet been addressed by the folks in the HDOs, but you have to remember that legacy devices are not just that are running DOS 3.1, they're also those devices that are still in the pipeline that have been under development for the past five or eight years and haven't yet hit the market. Thank you.

DINESH PATWARDHAN: Thank you. So we are going to switch over to day two and I just wanted to pause for a second. We heard from session chairs from yesterday at the end of the day yesterday the session chairs and the FDA team met and we did a quick similar session, what we heard today and today's sessions that -- those six sessions that were introduced by Brian were a synthesis of those discussions at the end of the day.

The second point I want to make is the note takers, the scribes in each and every discussion they did a really superb job and I want to thank them, because those are the -- those are the notes that will form the basis of the report that we are -- we would be working on, so I just wanted to make that note. Thank them and let's give them a round of applause. Thank you.

So I'm going to switch over to today's session in the morning and there, we have six of them and as we hear more I suspect that there may be some overlap from the comments made before, but that's just the nature of it.

The first session moderators were Chuck and

Anura Who Owns Cybersecurity? How Do We Understand Roles, Responsibilities and Accountability from the Supply Chain to Care Delivery.

HOW DO WE UNDERSTAND ROLES, RESPONSIBILITIES AND ACCOUNTABILITY FROM THE SUPPLY CHAIN TO CARE DELIVERY

CHARLES FARLOW: So Chuck Farlow, Medtronic. Again, this was kind of a carryover from the last topic discussed. I think just a caveat up front and this was mentioned by Rick. We only had two HDO representatives in our session, so as much as we tried, I think, you know, there really needs to be almost a 50/50 split of HDO and device manufacturers and so that was somewhat disappointing and, you know, the danger of only having two HDOs in the room is that it can become a bit of a group think with medical device manufacturers.

We actually kind of divided the topic into premarket and postmarket. I think in premarket there was general agreement that the device manufacturer is accountable for security, but has a responsibility to seek out that input from a wide variety of stakeholders, patients, clinicians, HDOs to name a few.

We discussed the quality of procured components

including software. And then we also discussed some unique challenges for small companies.

UNIDENTIFIED SPEAKER: Slow down just a little bit.

CHARLES FARLOW: Oh, okay.

UNIDENTIFIED SPEAKER: After manufacturers are accountable what was the second thing?

CHARLES FARLOW: We discussed the quality of procured components including software. And then we briefly discussed just small company challenges, you know, it's easy for larger companies to obtain that feedback from patients, clinicians and HDOs, but it's a little bit more challenging for smaller organizations.

Within the context of the premarket phase we also discussed developing security requirements early in the medical device design process as well as the fact that throughout industry and actually even in our regulators there needs to be an increased amount of security education. So do you want to cover the postmarket? Okay.

UNIDENTIFIED SPEAKER: Please do. I just came up.

CHARLES FARLOW: Postmarket, moving onto postmarket, a little bit different. In the postmarket phase the group really viewed security as a shared accountability between the medical device manufacturers and the HDO and we had a lot of discussions about intended use, as well as off-label use of medical devices. An issue that was identified was end of support for medical devices. Are manufacturers doing a good enough job communicating when a medical device will no longer be supported in the field?

And then finally we did discuss the latest attack, the WannaCry attack and we thought the communication of threat and vulnerability was good, I mean, there's a good exchange of information, but you know, our recurring HHS teleconference is really sustainable for a large number of events. You know, we did appreciate the HHS teleconferences held this last week, but again, is that really a sustainable model?

Anything you might add?

UNIDENTIFIED SPEAKER: No. Thank.

DINESH PATWARDHAN: Thank you. The second session for today, Information Sharing What to Share

with Whom and When, Mike Jaffe and Rick Hampton.

INFORMATION SHARING WHAT TO SHARE WITH WHOM AND WHEN

RICK HAMPTON: Okay. There was a common thread in all of these as I sat and listened to them and it basically boils down to, you know, what did you know? When did you know it and how did you get it to us? And we kind of tried to directly address that and we basically wound up splitting our talk into two different sections.

The first section this morning we tried to address, you know, what do device manufacturers need to provide to hospitals, the end users for that be the consumer hospitals, you know, what information does the manufacturers or do the manufacturers and regulators have to provide to the HDOs, the users in order to allow us to connect these devices in a safe and secure manner?

We didn't get nearly as far as where I had hoped we would get. Frankly, we got hung up on the fact that no one really knows what's required of manufacturers to hand people. You know, how much is too much information? Too much in terms of, you know, we hand you this bill of materials and all this other stuff

and a small hospital, the engineers and the technicians are now drowning in data they cannot possibly process.

The other question is how much data we put out there and how does it get to you in a way that, and this is my characterization, it's not anything that anyone else said, but I'm going to use some terms that I've heard in other places.

You know, how can we get this volume of information to you in a way that it's not weaponized by an opponent and/or turned into battle damage assessment by someone who can come back and attack us from a different direction.

So while I did not hear any of the device manufacturers say inherently we do not want to give you that information. The question is how much do we really need to impart to make this safe? And how do we do it so the information is not turned against us all? So let me just leave it at that point for the first one. And I think those are very valid things.

The second or in the afternoon we tried to address the issues of, you know, the last couple of days, so now we're in -- now we're responding to event.

What information needs to be shared? How does it get there and who needs to get it? That we had a little more clarity with. We didn't get into so much of a, well, we basically did a postmortem. Let me just put it that way. We did a postmortem on the last couple days and here's what we discovered.

The nice thing, people wanted to share information. The bad thing, they were sharing it in every venue known to man. It was not well coordinated. Is Susanne here by any chance? Oh, I was going to make her feel bad, because I found that Susanne had a call that she didn't personally call me about, so I feel hurt that I wasn't included in her call.

The problem was it was happening at the same time as two other calls were going on, one of which I was on. You know, so there is virtually, well, this is my characterization, so throw your shoes at me if it offends you. There's virtually no coordination in what's going on with the cyber response. There -- HHS was having a call NH-ISAC was having a call. FDA was having a call. DHS was having a call. No one knew when those calls were going on. There was no coordination at

all. If you managed to find out about one, good for you. You know, so that's -- that's one of the problems. There needs to be a coordinated activity between these organizations.

There was very little direction -- pardon.

UNIDENTIFIED SPEAKER: What were the organizations?

RICK HAMPTON: All the ones that are supposed to be in this room.

UNIDENTIFIED SPEAKER: Okay.

UNKNOWN SPEAKER: HHS.

RICK HAMPTON: HHS, DHS, FDA, NH-ISAC and I think there were one or two others that were going on.

UNIDENTIFIED SPEAKER: So you're calling for a national coordinator?

RICK HAMPTON: Well, you know, that was what someone said, isn't that part of we've got a national coordinator.

UNIDENTIFIED SPEAKER: Let's save that for the discussion.

RICK HAMPTON: Yeah. Yeah. So yeah, we kind of need a national coordinator for the national

coordinator, but, you know, the point of it is and all seriousness aside ONC is that, okay. Now you know I'm sleep deprived when I say something like that. Just shoot me and put me out of my misery.

All silliness aside is what I mend to see, you know, there needs to be a coordinated effort, because each of these departments has a separate distinct area of responsibility. In some places they overlap, in other places there's a wide gulf and they need to get together and figure out beforehand how they're going to do it. I think this was a good try for the first time out. It certainly, you know, exposed a lot of problems inherent in not having tested it before, but that was one of the issues. What was the other thing I was going to say?

Oh, we didn't really know what the information was supposed to be passed along and we didn't really know what direction that information was supposed to show. You know, so for example, I remember being on one of the calls, some of the other people did too. The government entities they were wanting to receive information, but when we in the hospitals and the device

manufacturers wanted to receive some of that intelligence back it was like it's a deep dark black hole information comes in and it never comes back out. That's not good for us, you know.

We understand the reasons why you don't want to give all of the details out that whole battle damage assessment thing. We understand that. One of the things I heard and this is where I'm going to do one challenge. I don't know who it was, but I hope he's listening or watching, because I'm talking to you. One of the -- on one of the calls I was on the -- one of the hospitals asked we need to have some idea of what's being affected, you know, if you can't give us the device manufacturers' name at least tell us what kind of device. Tell us where to look. The answer that came back was I will characterize as being an understatement extremely unhelpful. The answer that came back was we don't want to try and -- we don't want to tell you that because you'll just check that one device and ignore all the rest. Give me a break. We may be crazy, but we're not stupid. And I'll get off that soapbox now. But that was kind of, you know, that my personal take. Some

of my personal input and it was reflected in some of the other participants as well.

So we think that there is a way to get that information out there. We're glad that people tried it needs more coordination and you really need to stop and think. You really need to ask and this is kind of a research thing. You need to go back out and ask more people than what's here. What is it that you need to know and how can we get that to you in a way that's secure so it can't be used against us later.

DINESH PATWARDHAN: Thank You. Working with Legacy Devices, George Samaras.

WORKING WITH LEGACY DEVICES

GEORGE SAMARAS: So one of the first things we did is try to define legacy devices. We had a number of definitions unfortunately, Phil hasn't e-mailed me the scribe notes yet, so I don't have them in front of me, but one of the definition s which I think was the broadest and all-encompassing was those devices that have not yet been managed. And when you stop and think about that rather glib statement it actually make a whole lot of sense and it's a moving target, because you

may have managed them today. Next week there unmanaged again.

I see personally, legacy devices in three categories. I see the devices that are already out there that have not yet exceeded their service life. I see the -- another set that have exceeded their service life, but they're still available hardware and software and expertise accessible to maintain them even though it's not done by the manufacturer necessarily.

And then there's that remaining set that DOS 3.one and the ones where you have to have -- get out your 3D printer to manufacturer the part to keep that device that has essential performance and clinical value still running in your organization since once again, like we said earlier, we've got a broad range of health deliver organizations from huge hospital systems down to the little rural hospitals that have the 25 or 35 beds and not big budgets.

We talked about different perspectives on legacy devices. The manufacturer's perspective. The health delivery perspective. We had an engineer who is also a patient who talked to us about his perspective

and all of this are in the notes. We got some input from regulatory perspective. We had both Dinesh and Sandy Winegar [ph], Dr. Winegar in there.

We talked about challenges for managing, maintaining and doing risk assessment for legacy devices. And we talked about various strategies for managing them and for remediating them, you know, bolt on compensating controls and avenues for segregation and separation and, you know, using private LANs and things like that.

It's a huge problem and while we were focused legacy devices the problem -- the devices that are coming out now the path forward are going to be producing more legacy devices, it's already been set up here before and so we need to come up with some best practices that actually will get followed to prevent us from revisiting this problem 10 or 15 years from now.

DINESH PATWARDHAN: Thank you. The next one is Software Bill of Materials and Resulting Considerations, Ken Hoyme and Michelle Jump.

SOFTWARE BILL OF MATERIALS AND RESULTING CONSIDERATIONS

KEN HOYME: So I'll make -- you've got the

better list of the research things. I'll make sure you cover that.

MICHELLE JUMP: Okay. You want to just start?

KEN HOYME: We started talking about software bill of materials and realized that that might be a misleading term, because it isn't quite the same thing as the hardware bill of materials, so we spent a considerable time coming up with other acronyms like SWILL.

I think when we entered the room we were kind of thinking that the purpose of a software bill of materials is vulnerability management. It was kind of that request of hospitals want to know what's inside the devices that are on their network so that when something breaks in the world they understand the risk profile.

As we worked our way through the day we kept coming up with other uses and values for what this could be done for which could potentially drive how it's captured and how it's exchanged. We found it could be used for purchasing decisions that the risk profile of how much of this kind of software and at what level is inside the device might be part of your purchasing

decision. Yes, vulnerability management, incidence response, we did have to go and recruit some HDO people to come in for a while and what he talked about when a particular device is being hit they would like to know what other software -- what other devices share that same software if that happens to be going around the hospital right now, so it's a very short-term incident response.

Supply chain management service contract management, when they're negotiating service contracts understanding the quality of what is being updated with that. For a company or a hospital to obtain cyber insurance it might be that the insurance companies will start wanting to know how much risk is still in that software based on its -- emerging acquisition activities, if you are a medical device company acquiring a smaller company having that as part of your due diligence might be a valuable piece of information.

We talked about certification of software, whether or not the part of that certification process the certifiers would want to understand the software bill of materials and some of its risk profile. And we

have not to speculate about whether or not if we had a large database of this would that allow a national assessment of health care system risk as part of a critical infrastructure assessment that it might go up to, so.

We spent time brainstorming challenges and I've captured a lot of some of the challenges related to that. I think challenges that we saw were the concern that there's intellectual property released in this and whether or not competitors would use the state of somebody else's software bill of material as a competitive argument so how do you secure it? How do you -- when do you exchange it? Are there -- should a service be created that would allow small hospitals to be able to query this database without having to manage it themselves? So is the thing centralized? Is it distributed? A lot of different issues that can affect the overall design.

I think that was -- talked a little bit about liability issues. How this database might vary based on class of device anywhere from small embedded systems up to cloud-based medical services. I think that was --

MICHELLE JUMP: I guess I would add to that conversation, you know, as Ken mentioned we talked about use cases of how you might utilize an S-BOMB [ph] or a SWILL or however we want to call it. We'll call it S-BOMB for right now. We had a lot of fun with the acronyms though. And one of the things that we dug into a bill both before we went and collected some HDOs to come back in and afterwards is how they're using if we do release software bombs to customers how are those being utilized and is that really the best way to get this information, so understanding how the S-BOMBs are used helps us understand what kind of information could potentially be standardized so that everyone is providing the same information the same way; right. And make it a little bit more and expected. And coming back to it, you know, we're looking at vulnerability management, but if there's sufficient interest that the company is taking care of this can some of that burden be relieved from the HDO and the manufacturer is expected and has a process in place where the communication is regularly established where vulnerabilities are monitored, assessed and communicated

back to the HDO on a regular basis.

So we talked about having options there so companies with maybe less advanced processes for managing vulnerabilities will still give their S-BOMBs and look to the hospital to kind of look at that themselves, but then other hospitals or other manufacturers who might have more advanced ways of managing vulnerabilities making sure that they just don't tell the hospitals when they have found something that needs patching, but rather they've found something that's very low risk and it will be patched on the next go-round or they've looked at it and it's not exploitable and it will not be patched.

So just because you haven't heard from an HDO doesn't always -- or from a manufacturer doesn't always mean that nothing's happened, but I think the consistency and the trust of the communication that's happening both when something needs to happen on the HDO side and when it doesn't plays into this role.

The other part that we talked about here which is our first question is the consistency and the way people are managing their S-BOMBs from the

manufacturer's side, right. So the way manufacturers currently are managing S-BOMBs may have been established. That process may have been established well before they were using this for security purposes and so one of the questions for research is is there -- would there be an S-BOMB management methodology that might be beneficial to kind of standardize and put out there as an operationalized example for medical device manufacturers.

Something that would be useful to both large manufacturers and small manufacturers also dealing with how you're going to deal with legacy issues and kind of defer categories of devices. Some devices may have different needs for the S-BOMB. The other -- one of the other issues here was what kind of content might be valuable to standardize for a template of S-BOMBs that would go to HDOs and understanding how they use it, making sure that it's accurate and looking whether a database might be the better way of managing it was another research question that we had.

One other thing that had come up in the conversation around research questions was is there

potentially a benefit for looking at the need for something like a third-party white listing tool? It would forgo the need for patching when disaster strikes for legacy products that aren't going to be patched any longer, things like that. So looking at this idea of a third-party white listing process.

We have quite a few questions and not all of them kind of bubble up to the need to be shared openly in the -- do you have anything?

KEN HOYME: One last thing I would add was one of the things we also talked about I think what Michelle was kind of implying is you could expand the use of the software bomb to a vulnerability communication tool, so if when you have a version of software listed in your bomb and a now CVE is published in the national database you could tag that with this response of where are we in the response, you know, are we still in analysis? Are we that? So we could make this a more efficient automated tool to communicate where there's a one-stop place you put that information in and everyone who needs it gets access to it rather than you having to send letters out to every customer, some of the overheads

that manufacturers have now.

MICHELLE JUMP: Yeah, so I think in a nutshell we talked a lot about how can we standardize the way this information is shared, how it's used, make sure that it fits that model and also dealing with this overload of information that could be overwhelming and trying to centralize that more of in a database that could be updated on a regular basis rather than getting an S-BOMB when you purchase the product and then never seeing another now one when you know it's going to be updated, so. But really good conversation I think we had folks come in and out throughout the morning and different folks came in and added their thoughts and so appreciate all the participation this morning. It was very good.

KEN HOYME: And the last note. Someone in the group whose name shall remain, Brian Fitzgerald, introduced the concept of a software smorgasbord so that might be what becomes coined.

DINESH PATWARDHAN: Thank you.

KEN HOYME: It's got the dots over the O.

DINESH PATWARDHAN: The next one is Nick and

Bo Woods [ph], Generalized Threat Modeling One Liability Profile for Medical Devices.

GENERALIZED THREAT MODELING ONE LIABILITY PROFILE FOR MEDICAL DEVICES

NICK SIKORSKI: Yes and this session kind of originated out of what I was talking about earlier, really both of our sessions had brought it up of essentially having a need for understanding what good looks like. What are the attributes? What are the different threats we should consider and, you know, the unique intricacies of this being the medical device world.

How it came up though is a little different Bo can describe how it came up in his, but in mine it was more an a sense of not just wanting to generally, you know, what is a list of threats, but for a specific type of device, say an implantable or a diagnostic device, what are some of the specific threats that face those, so rather than one list you would have different threat models based on, you know, category of device.

UNIDENTIFIED SPEAKER: Yeah and session it came up a little bit differently as nick mentioned. We were

really thinking about how can we have some way to equip medical device makers to do some of the threat modeling to define buckets or classes or categories in which they could have different threat models for different devices, but where there might be some guidance or examples that could be pulled from, so the one that I've used quite a lot the last couple of days is, you know, you might have a wireless communication bucket and then within that obviously you could do near field, you could do Bluetooth, you could do 4GLTE. Each of those would have unique considerations, no device or very few devices would have all 3 of those, but if there's something to give guidance and to provide the things within that to think about it would be really, really helpful.

So we tried to generate something that was like a call to action statement or the defining characteristic of what we're trying to put this research topic out there for and it's the -- the industry needs a way to improve health care cybersecurity through improved threat modeling which is comprehensive, usable, broadly adoptable and not derivative of what is

available today. So there's a lot in that and I'll unpack some of those things.

UNKNOWN SPEAKER: So is this is a direct quote? I need to get it right. Call to action, the industry needs a way to improve industry cybersecurity through approved threat modeling.

NICK SIKORSKI: It's in the notes sent to you as well.

UNIDENTIFIED SPEAKER: Yeah, it's in the notes. I'll repeat it for you so that you can correct. The industry needs a way to improve health care cybersecurity through improved threat modeling which is comprehensive, usable, broadly acceptable and not a derivative of what's available today. And that's a draft statement. It's probably not going to be final. There's some tweaking that I'm sure could be done. But some of the things that are packed into that are, you know, some way to dampen the variability of threat modeling use and acceptance. So if a medical device maker is doing a threat model one of the outputs from that is going to inform their internal teams, right.

One of the outputs from that could go to the

FDA. One of the outputs from that could go to customers who are buying things. One of the outputs could go to insurers. So there's multiple different steak holder groups that could benefit from this type of activity and the documented self would look different; right. You're not going to provide all the information to your buyers that you would to the FDA, so you might have different audiences and different documents, but to dampen some of the variability or to improve consistency and we chose those words deliberately rather than something like come up with a standard, because a standard would move really slowly in comparison to the threat modeling that needs to be done, but something like a framework could be flexible enough to be used for years without having to be updated even if the information that an individual device maker is using to put into that process changes.

NICK SIKORSKI: And kind of one other thing to add onto that that kind of came up several times throughout the morning. What was really that while it would be good to have something that doesn't necessarily need updating everything, you know, few months, you also don't want to sacrifice the level of detail that could

be provided in such a document because at the end of the day the more detail in it the more actionable it is for most manufacturers and consumers of that document.

UNIDENTIFIED SPEAKER: Yeah, and we realize that there could be a split too. There could be a framework and then there could be something that's more not like a threat intelligence feed, but something that updates more frequently than the framework that could accompany it and there were a number of companion or partner documents that we had ideas for that are certainly in the notes, but we don't have to talk about all of those now. It's just, you know, we realize going through this process that there are going to be some dependencies and some assumptions in any research project that the success or failure of the ultimate output is going to depend on that. So how well and how widely adopted and used this is going to be is going to depend on for instance the level of detail that manufacturers might have access to within different threat model or different threat scenarios.

NICK SIKORSKI: And then on the topic of the partnering documents, right, what you don't want this to

do is just create more questions, right. So it's great we know what these threats are, but if we still don't know how to mitigate them we're in the same issue we were in before. So that's where this partner document, separate research effort, whatever it end up being is important which is what does leading practice look like to secure connected medical devices.

UNIDENTIFIED SPEAKER: Right. And there's a set of those that will be already excitant, right, like Microsoft's Stride Methodology could be a companion document that helps a manufacturer understand how to go through and do this, but there could be other companion documents that would need to be generated that might generate a new research project. So we allowed for both of those in our discussion and in our conversations.

To the -- we also realized that the critical dependency of this is going to be how well adopted the output of the research effort is. So if it's like, you know, for the record, for the camera I love the OWASP Group. They put out a lot of really, really good material, but they haven't been nearly as effective in communicating and getting outreach to developers. So if

the research project generates a beautiful, magnificent, perfect document, but particularly somewhat HDOs and medical device makers have never heard of it then I think that that would hit a failure criteria rather than a success criteria, so something needs to be built into the -- the considerations of the research project of how this is going to raise awareness among the stakeholders and the constituents that need to know it so that it will be successful and the -- I used this example yesterday. I'll recycle it today, because I'm green, but the idea of having something like a Smokey the Bear for a threat modeling, just something that's easily accessible that has an outreach component that also has an education and awareness component and ultimately if we can drive adoption of whatever comes out of this process then it increases, it improves communication between all the different stakeholders and it becomes a vehicle to set expectations.

One of the problems that we realized yesterday and today is that manufacturers make a device with certain expectations about the environment it's going to be housed in and if those expectations are violated by

the HDO then of course you'll have security breakdowns and one of the ones that we've already seen and talked about yesterday was a medical device maker that put several layers of high quality security on the device, but when it went into the -- the environment they striped some of those layers away that were protecting it in order to do a different security mechanism, in order to put a different security measure in place. So we want to avoid that and this could be a mechanism to actually improve those communications, to set expectations all the way around.

And then this is more of a global statement, but this type of a document can build and improve market confidence in the reliability of the devices. And it can actually reduce commercial friction and commercial burden. So you're already going through the process to do threat modeling this makes it easier or it can make it easier to make sure that, you know, all manufacturers are doing the same process and then it can also make it a lot easier to communicate to out external organizations so that they know what you've done and they know how it fits into what they want to buy. So

there's a potential commercial aspect to this that makes it both cheaper to do and improves the market confidence.

And one last point to unpack the very end of our guiding statement is that this must be new and valuable to our stakeholders. It can't just be, oh, yeah, here's something else to think about and from what we've heard around the room and we can investigate this more in the research project is is there any kind of a standard threat modeling idea for the health care domain and if there is, certainly some of the folks in the room didn't know about it. I didn't know about it. And that could be a valuable contribution to this community. Hopefully we can go beyond just having a customized stride for health care, but if we start with the idea that we need to generate something very new and very valuable for this group then I think it would be a success.

NICK SIKORSKI: And then just one other note is while this is mostly going to be digestible by manufacturers this is another tool for hospitals during procurement similar to how they might currently use an

MDS2 form, they might be able to use a, you know, one of the these threat profiles to essentially hold the manufacturer more accountable. All right. Thanks.

DINESH PATWARDHAN: Thank you. Okay. The last one is V&V Under Security Related Time Pressures, John Hatcliff and Stephanie Domas.

V&V UNDER SECURITY RELATED TIME PRESSURES

JOHN HATCLIFF: Show of hands, how many are aware of a standardized threat model for medical devices?

UNIDENTIFIED SPEAKER: Exactly what was said, exactly what was said just now. Is there any kind of standard threat modeling idea out there? Is anyone aware of one?

- - -

(Background Conversation)

- - -

DINESH PATWARDHAN: Please.

JOHN HATCLIFF: Right. So to kind of summarize the issues that we are trying to address. The issue is everyone sort of understands the main idea of V&V, right. So the question is when you're in a context of

trying to rapidly incorporate the security patches how should the notion of V&V change?

So imagine, you know, we all know the V diagram, we know where V&V occurs and that life cycle development process, you know, how would you redraw the V diagram; right? To focus on the particular issue of responding to patches. The same thing if you opened up the annex of 14971 there's a risk management flow diagram, risk management process. How are you going to redo, rejigger that diagram to address what needs to be a risk-based approach to doing this patch management V&V sort of activity. So these are the main things that we were trying to sort of address from a variety of perspectives.

So one of the things that came up for us is I think we all kind of understand that there's needs to be some sort of phasing. Often you need to apply a quick fix, right, but you don't want that quick fix to be a permanent solution. So there was a -- we recognized a need to sort of explicitly design a process that was phased where you could roll out a quick fix in response to a security threat, justify that in some way with your

risk management approach but then later on have a required, you know, again justified by risk management follow on phase where you did a more thorough V&V to substantiate the fact that, you know, what you did at first was either good enough or you've now rolled in additional risk controls that you need to fulfill your V&V objectives.

Yes, so a crucial aspect in this --

STEPHANIE DOMAS: Go ahead.

JOHN HATCLIFF: A crucial aspect in this was addressing issues surrounding liability. So if you want to encourage people to push a patch out quickly to address what are certainly valid concerns they need to somehow have some sort of protection from liability issues to make sure that that is indeed a recognized sort of process or best practices in the regulatory context that doesn't leave them open to liability issues. So that was a significant challenge in that space.

Kind of similar to what the previous group said, we also need to understand that our risk management practices need to take into account of where

the device may be placed in context when it's deployed. So the ideas that our risk management processes in this context can't simply be oh, I've, you know, I'm looking at my device and yeah, this is a low criticality device in some sense and so I'm not going to patch it immediately, because that device may be placed in context and when it's in the context of a larger network it could be used as a pivot point when you can then, you know, get into that device and use it as a launch pad to launch additional attacks.

So the issue then was, okay. We can do research, produce technical results on this. How do we then flow these into the regulatory context? And a lot of vendors were very concerned about the need for increased clarity around this particular issue in the regulatory context and one of the specific needs for research that came up was if you're going to make an argument to the FDA in either of these phases about I've done enough or I need to do more and I've done what I said I was going to do and we're now what needs to be done, how do you substantiate that with maybe not a complete assurance case, but at least some sort of

structured argument. What's the arguments in evidence that you need to produce in that context?

So another technical issue surrounding this topic is the whole idea of making a change in a device and then figuring out what you need to do, what might be sort of effected by that change is related to a technical concept called impact analysis.

So in the past, you know, many organizations are aware of these concepts and they apply them, but since we're now getting into the state of the world where changes are going to be much more rapid and we need to more rapidly respond, we felt that it was important to elevate the notion of impact analysis providing training on that highlighting exactly how that gets carried out when you're in particular addressing both safety and security concerns. And we had a number of issue that we laid out for that.

STEPHANIE DOMAS: Okay. So one of the areas that we also branched out in conversation was talking about the need for maybe a meds cert, so people are generally familiar with ICS Cert, but ICS Cert is specifically Industrial Control Systems. The purpose of

it was to share vulnerability information that it's hitting the industrial control systems industry and disseminate that to the public with information about the vulnerability potential fixes and potential impacts.

So we discussed was there a potential need for a med cert, so a way for us to publicly disclose information about medical products, but another piece of the ICS Cert Division is that they have what they call go teams, so teams that are specifically trained to help in the security and industrial control systems see those are go teams that if an industrial control system is having an issue they can call in those go teams to help them, so would having a med cert with basically go teams specifically trained to help in medical cybersecurity incidents is that something that our industry needs? So it was generally favorable in our room, but that's a discussion.

And another piece of the sort of sharing of information there's the ICS Certs or a Med Cert that is run by the government, it's funded by the government and on the flip side you have the ISOWs [ph] so things like NH-ISAC which is meant to the industry driven so we had

some government representation in our room and they said they feed information into ISACs, but they don't participate in them they want that to be a sharing experience amongst the industry stakeholders so while they will feed information in to disseminate vulnerability information they're aware of they are not consuming that information they want it to be industry driven where something like a Med Cert would be government driven.

Yeah, so a part of having a flexible or agile V&V was a topic we talked about was consistency and repeatability of testing. So if I need to scale my testing in some way I need to have a consistent and repeatable way that I can conduct testing to still give myself the confidence that the patch that I'm issuing isn't going to have a safety impact.

So one of the things we talked about from a couple other industries the things that they use, so things like hackathon s, so in the automotive space there are industry-run hackathons that will allow people to come in. They all sign NDAs. Will come in and allow them to essentially hack on automobiles on manufacturers

who have agreed to participate and use that information to help bring all of that industry up. So all of the manufacturers participating learn all of the information about the people who have participated in the hackathons.

And there's also in the oil and gas industry there's some consortium efforts to help share vulnerability information amongst the oil and gas industry so that was another one that came up is, you know, is the health care consortium something that will work and one of the issues that was discussed is that in oil and gas industry you have maybe 10 big players and if you get those 10 players you've got 90% of the market, but medical's not like that. If we got the big players, the couple dozen big players you've actually still got a small subset of the market, so it's a lot hardening to have a consortium driven group because the med device industry is so fragmented.

JOHN HATCLIFF: So another one of the things we talked about as far as achieving solutions, community-based solutions that would scale. So we talked about the notions of developing test beds or test

context where we could use to test devices. A manufacturer could come in and at a relatively low cost instead of having to build all their own testing infrastructure they could work within the context of this test bed to have their devices sort of evaluated in context in a realistic context.

Some of the challenges there were there's tremendous variability in the medical space and so even the need to sort of design a test bed means that you really have to analyze the domain space to understand what are the different attributes that I need to consider in a test bed so that I'm getting appropriate coverage of different types of issues. So --

STEPHANIE DOMAS: So just briefly on that one. So the challenge there was that even if you've done some like quick fix in a small scale down version of your own V&V to release this patch, how do you know that it doesn't affect the ecosystem of medical devices that it plugs into? It passed your tiny smaller V&V, but you're part of a larger system.

JOHN HATCLIFF: So we finally addressed issues related to partitioning and separation issues and we

discussed that in a number of context here, so I won't go in-depth, but mainly the idea is that there are solution strategies out there for partitioning which can help you more easily roll patches in without and making sure that you're not impacting the rest of the system among many other things. And so a lot of our discussion centered around how can we raise awareness of these technologies? How can we provide tools that help people use these types of technologies? And what sort of analysis or design workflows go into using these technologies?

DINESH PATWARDHAN: Thank you. Thank you very much. I want to take this opportunity and on the behalf of the FDA team let all the session chairs did a very fantastic job and big round of applause to them.

A couple of housekeeping items, many of you have to catch a flight and all of us have to leave here. The readout part of the session is complete. What we are thinking is to have a five minute in place stretch out session, meaning we'll start real quick and then have our discussion. That discussion will be open and it will -- you may come up here and look at these,

please don't touch them, we haven't captured the notes quite yet, we are trying to do so.

So we will start in -- it's 2:48, we'll start at 3:00 and then we'll have a discussion. I was asked to repeat this. There is a group meeting outside going to at some point going to an airport, so if somebody's going to which Dulles, I believe, so just look for people outside going to the airport. I will start at 3:00. Thank you.

So we are going to start the discussion phase here and there is no -- there are very few rules, let me just put it that way.

- - -

DISCUSSIONS

- - -

PAT BAIRD: If I knew that, ah, man. So anyway, thank you for letting me go first. I got a bolt to the airport after this, but after the discussion of V&V and did we lose Stephanie? Two thoughts that I had that I thought might fold into the scope of the V&V work would be, you know, one --

UNIDENTIFIED SPEAKER: Could you hold those

thoughts literally for 30 seconds?

PAT BAIRD: Sure.

UNIDENTIFIED SPEAKER: Tell us a joke.

PAT BAIRD: I don't have any slides. You do not want me to sing. My wife will attest, you do not want me to sing.

UNIDENTIFIED SPEAKER: Okay.

PAT BAIRD: All right. Okay. Fair enough. It's done by now. So one thing that I thought and one of the themes that I had on the first day, right, was gee, there's a lot of SOUP. Gee, we need to have more consideration for design for patchability, you know, how can we take and upgrade these things? And have that as one of the design constraints you build in is make things easy to upgrade and one thing that hadn't occurred to me until we were talking about V&V wasn't just make it easy to swap out this part of the executable in that part of the executable, but also let's carry over that concept of segmentation into the testing itself, right. And so if you have -- if you've designed your tests so that you have to do a bizillion [ph] regression tests every time you change something

that worked fine for the initial launch, but if we're going to be patching this thing and need the patches to go out, so I was thinking that as we are developing or considering whatever kinds of guidances researches into V&V let's also talk about how to lower the cost of change when it comes to testing.

The other one that had occurred to me and maybe other folks are doing this already, but something that had popped up in a couple different conversation was people in the hospital don't want to take the machines down to do these upgrades. They want to be able to get upgrades done quickly and get them back up and running, because some of these they're income producing and they really need this are vital pieces of equipment to that hospital.

I wanted to make sure that because doing the upgrades is so important and doing them in a timely manner and people are in a rush both on our side and HDO side, are we doing a process FMEA for the upgrade process itself? So are we taking and consider what kind of risk can go in? Are we grabbing the wrong patch? Is it -- how long is the device down for? What kind of

risks does it take and introduce during that risk? So I was thinking that sort of as part of this suite of tools that would be really, really useful, I thought an installation process FMEA considerations for process FMEA something along those lines would be useful. Okay.

UNIDENTIFIED SPEAKER: Thank you.

PAT BAIRD: Okay. Thank you, sir.

DINESH PATWARDHAN: Thank you. I don't want to moderate the session. I want to have -- I don't want to pick volunteers. I want to -- please. Well, I want to be very careful.

KEVIN FU: So my car, I have this problem, now, it make a sound like -- no, so I want to talk about, we had the session with Michelle and Ken on bill of materials and I wanted to add a couple extra thoughts on that. The first, the cynical one and then sort of the real one. So the cynical way of looking at it is that there are two kinds of software. There's unmaintained software. That's where, you know, you might blame an HDO for not maintaining something and then there's unmaintainable software where the hospital no matter what they do are going to, they're just never going to

be able to keep it secure, because of some problems during manufacturing or choices in the default of the OEM.

But one -- there was a discussion that went on, on this related to inventory and it, in my view it basically boils down to, I'm sure if Gavin's here, but the cybersecurity framework sort of step one, know, your assets. Step two, controlling the risks and then step three, checking if your controls are working all the time. But it's sort of obvious, you can't protect what you don't know you have and we're seeing that problem in two different circles and they kind of, they relate to each other. So in our discussion we were talking about the SOUP, again, the SOUP that keeps coming up at the manufacturers where not all manufacturers have a good understanding of all their third-party software inside their projects and so they have an inventory problem. And then that trickles down into the HDOs, because when the HDOs start asking questions like what's on the inside the manufacturers might not have a great answer, but even if they do, the HDOs might be adding little bits of their own, you know, it will come in sort of

default OEM, but then it gets modified, customized to whatever that hospital's networking policies are.

The final thought would be there's a little bit of, I think, discussion/argument on, you know, should we give away this information, these bombs, this bill of materials, because doesn't that help the bad guys? And I offered the following counterargument.

The counterargument is, you know, let's not put our heads in the sand, so look, the bad guys already know what's out there. Just look at WannaCry. They're able to get in because they know those clinical networks better than the good guys.

What we're trying to say is, hey, you know, manufacturers, we would really appreciate it if you would share bombs such that the very busy HDOs who aren't just trying to hack into everybody and do have to worry about safety can know that too. The bad guys don't care about safety. They can just do anything they want to try to figure out what's on the inside. Take things apart, even cause harm to live clinical care and disabling HDOs.

UNIDENTIFIED SPEAKER: Kevin, I've heard that

phrase quite elegantly as the bad guys are already scanning your network, shouldn't you?

KEVIN FU: Okay. Eugene says that this has been coined as the bad guys are already scanning your network, so shouldn't you be? The counter-counterargument is that well, nobody wants to admit this on camera, but if you work in a hospital and you scan your hospital chances are you're going to knock something over and the clinical engineers are not going to give you, you know, the end of it.

UNIDENTIFIED SPEAKER: So sky quote.

KEVIN FU: It's a blue sky quote. But anyhow, I just, I think once we can start getting toward better bill of materials both in manufacturing and in the HDOs and they're going to be different approaches for those two things, I think we're going to be able to have much better grips on how to control these risks rather than focusing so much on post-market. Post-market is great, but wouldn't it be nice to get it, you know, cleaned up before you ship it. Those are my comments.

DINESH PATWARDHAN: Thank you.

TODD CARPENTER: Todd Carpenter, Adventium

Labs. On the bill of materials issue people might not be aware there are commercial tools you can purchase and throw a binary blob at it and it will tell you what's in there. It's not perfect, but it's a good starting point and so it shouldn't be surprised to any of the companies here. And the bad guys can buy these same tools.

UNIDENTIFIED SPEAKER: Are you saying there are SOUP extraction tools?

TODD CARPENTER: There are SOUP extraction tools.

UNIDENTIFIED SPEAKER: I just --

TODD CARPENTER: Go for it.

UNIDENTIFIED SPEAKER: I just want to add onto that there's also the NIST software reference library. NIST software reference library, so it's a collection of hashes, of lots of common systems that are out there. They're also including other kinds of information going back to some of the profile stuff we've been talking about. They're linking the entities and the library to SWIDS which were software I.D.s which are things that can be generated automatically when software installs.

So we might want to go and take a look at that

also as a way to help provide automated way to extract some of that information.

RICK HAMPTON: Since I seem to be the sole representative for every hospital in the world.

UNIDENTIFIED SPEAKER: Just the new ones -- standards.

RICK HAMPTON: So the -- what?

UNIDENTIFIED SPEAKER: Saint Rick's Hospital.

RICK HAMPTON: Yeah, Saint Rick's Hospital. I like that. So the concept of what to do with all this information, bill of materials and stuff, you know, someone when we were talking about this someone asked me what do you want. I want everything. I'm greedy. I want every piece of documentation. I want to be able to pick your engineer's brain. I want to know everything there is.

The thing of it is, I work at a place that's big enough I can handle all that information. So when we start looking to providing, you know, bombs and everything else to every hospital in the world, keep in mind that the interesting thing about hospitals is I may have 100,000 devices in my hospital, those 100,000

devices may represent 1,000 different makes and models. The hospital that's 18 beds, they don't have 100,000 devices, but they still have 1,000 or 100,000 devices total, but they may -- they will still have 100,000 or 1,000 makes and models.

So if you look at each make and model requiring a separate bill of material you're going to provide that little 18-bed hospital with the same stat -- with the same truckload of documentation that you're going to give me. I may have the staff to deal with that. That 18-bed hospital is not.

So bill of materials are great, but you got to be -- you got to take into consideration that are going to use it. Are they going to have the wherewithal to deal with it?

UNIDENTIFIED SPEAKER: Aren't you producing two different --

RICK HAMPTON: I'm sorry.

UNKNOWN SPEAKER: We're in the same direction.

EUGENE VASSERMAN: If you're producing two different ones anyway as a manufacturer, one for the small facility, one for the large facility it seems then

it makes sense to distribute them both. There's the S-BOMB which the summary software bomb. So it seems if you're producing at least two anyway, the small one and the big one two versions of the bill of material one --

RICK HAMPTON: Why would you have two versions of a bill of material?

EUGENE VASSERMAN: So as not to cause information overload from one of them that is a condense one that may include every single version number, simply the software packages.

RICK HAMPTON: Why would the little hospital need any less information?

EUGENE VASSERMAN: They -- I thought the point you were making is they may not be able to handle it.

RICK HAMPTON: Well, what I'm saying is the volume of material they may not be able to handle. So if you -- the volume of material they may not be able to handle, but they may need exactly the same material. So that's the question, how do we do that? Okay. And as soon as you get done --

EUGENE VASSERMAN: So I'm suggesting that you may produce a small one and a big one if we're calling

them S-BOMBs then it would be ES-BOMB that is the executive summary bomb along with the -- literally all of the information. And if you have the wherewithal to use it then you use the -- you use it, but if you, I mean, literally, if you don't have the time and you need to glance at it then at least there's something that doesn't cause information overload and that may be an overall win.

UNIDENTIFIED SPEAKER: From my perspective this is a standard human factors problem and it's already been solved. It's called the difference between push and pull information. Instead of dumping the truckload on them, put it somewhere where they can access it when they need it.

If you're worried about bad guys or competitors accessing it instead of giving them the truckload you just give them some way to authenticate that they deserve to access it.

RICK HAMPTON: I like the concept, but you used the one word that drives me nuts and that's assume. Don't assume anything, because if -- remember we're dealing with 18-bed hospitals, 100-bed hospitals, people

that don't have the time to deal with that stuff anyway.

Your assumption would work assuming we have funding to train those people how to use it. We don't --

UNIDENTIFIED SPEAKER: Well, if there's a third party that comes into play.

RICK HAMPTON: Assuming --

UNIDENTIFIED SPEAKER: Already --

RICK HAMPTON: Assuming the hospital has the money to pay to have their people trained or has enough money to pay for a third party to come in. That's the assumption that's bad. I like the idea and God knows and hate saying that, you know, we have to worry about money in health care, but we have to worry about money in health care.

UNIDENTIFIED SPEAKER: But that doesn't directly go to the issue of whether you're going to dump the documents on them and overload them. That thought doesn't go directly to the issue of whether you're going to dump the documents on them or go and overload them or just make it available to them. I think, I don't need all the documents all the time. I need the documents

that I want right now. I know how to find it. I would think that anybody in the hospital that's actually going to be doing something like this would know what they're working on.

RICK HAMPTON: Please provide your contact information, I got 100,000 hospitals that are going to want to come and have you volunteer for them. It's a nice idea. I'm not -- it's the scalability, you know, we've talked about human factors, you're right on the human factors part, it's the scalability issue.

UNIDENTIFIED SPEAKER: I can fix that.

UNKNOWN SPEAKER: He's going to fix it though.

EUGENE VASSERMAN: So I started immediately thinking, so how do you authenticate when you, when you request these? So the natural authentication is you're authenticated because you have the device that for which you're requesting the bomb, so someone said why, I mean, you should be able to scan your network and get the bombs from every device, well, what about scanning your network and asking the devices to nicely query their manufacturer and get the bomb for you, so you don't have to store it on the device and you use the device as a

proxy which solves both the authentication problem and the push pull problem.

UNIDENTIFIED SPEAKER: So this is just engineering, of course.

RICK HAMPTON: You know and the point that George brought up and I'll be happy to sit down or I can stand up here and you can throw shoes at me if you want. I can be the moderator again, because I don't know how to do that enough, you know, because I'm so moderate, exactly.

So the and I have to admit, when I was thinking about this I was thinking in terms of the last three days where we're working through an event and we need to know everything right now. In formal times, you're right, we could -- in normal times when you can access that stuff on a more reasonable basis where you can take the time to read one bomb a day or week or whatever, that, all of that makes sense. So whether it's delivered in a truckload or whether we go and pull it as we need it, under normal circumstances that's fine. Where I think that breaks down, where I think it's going to be challenged to the breakdown point and where we

have an event that we're trying to work through and if we really don't know, you know, if it's a targeted attack on one device that's easy, but in case like WannaCry where we have no ideal what's and we have to look at everything right now, that's where we're going to have a problem.

UNIDENTIFIED SPEAKER: Well, we're not going to look at everything right now simultaneously. We're only going to look at everything right now --

UNKNOWN SPEAKER: So I think there's a possibility here of these ISALES [ph] actually finding this as a core process. The manufacturers who generate the information, the ISALES who distribute it and the health care facilities, not just hospitals, by the way, it's your dentists, it's your orthopedic whatever, these are consumers of that information, they should have at their disposition a readily available service for this if they need it.

I'm not sure, however, how useful a one-size-fits-all bomb would be to the vast majority of people in the world who would like to consume a bill of materials. We discussed earlier that there were needs

for a bill of materials that exceed the need to manage vulnerability that for configuration management purposes, for intrusion purposes, for M&A, for due diligence, for certification purposes, for JCO [ph] maybe. There could be lots and lots of reasons to have different configurations of bombs. In any case, if this turns into some kind of service that ISO could manage on a subscription basis manufacturers could feed into it and they would have some level of trust that it wasn't being abused by their competition. At least it would be traceable if they found their competition going looking up their bill of materials.

RICK HAMPTON: I'm being sleep deprived. I'm mention that again. I'm running slow, but, you know, it's like Brian said, yeah, we do have other things beside, you know, we've got doctor's offices, dentist, hospitals. And I've look at that stuff and if you, you know, if you look at, I mean, we looked today at some of the regulatory things that hospitals have to do and in those standalone offices have even less that they're required to do, you know, we may be short on IT staff, they don't have IT staff, you know. So, yeah, it's a

kind of an interesting thing.

UNIDENTIFIED SPEAKER: IT staff, cybersecurity expertise thing, we've already got a model in the health care industry, in the health care delivery organization for this and that's medical physicists. Most hospitals don't have their own medical physicists. It's a third-party group that's brought in and they do what's necessary and they go to multiple hospital and they have high levels of expertise and it is gotten to the point where you go and you get trained as a specific medical physicist, not a biomedical engineer or an IT person that then does medical physics. And we -- it's conceivable we can do the same thing in cybersecurity.

RICK HAMPTON: Well, we have third-party drug companies in the medical devices.

UNIDENTIFIED SPEAKER: Right.

RICK HAMPTON: And that model is there --

UNIDENTIFIED SPEAKER: Right.

RICK HAMPTON: But what I was getting at is we still don't have -- we still don't have the regulatory drivers to make people spend the money if they do or they don't have the money.

UNIDENTIFIED SPEAKER: And that's --

- - -

(Speakers speaking off of the microphone.)

- - -

DINESH PATWARDHAN: I'm looking for the next one here. There were a couple people who came up to me and wanted to say something.

UNKNOWN SPEAKER: They're all asleep.

DINESH PATWARDHAN: I don't know how to take -- we are looking for a -- we had a discussion earlier. We had a recap and you were looking for discussions based on that recap and a number of people have left for flights and they'll be [indiscernible]. There was a raised hand back there.

EUGENE VASSERMAN: Let me ask this. Are -- from the audience who I realize I have my back to, are there -- are there things on this board if you had to pick one, the most important one and you feel very strongly about it, would you speak up and just say which one it is, because we have more topics than we -- I think we have audience member s by this point. So I'm fairly curious if you had to pick one for each audience

member what would they be?

UNIDENTIFIED SPEAKER: Some of them are difficult to read.

EUGENE VASSERMAN: Oh, you have to remember, no.

UNIDENTIFIED SPEAKER: I don't think that would be helpful.

EUGENE VASSERMAN: If it's that important to you, you would remember it. Okay. Anyone? That might have been [indiscernible].

UNIDENTIFIED SPEAKER: I'm going to actually kind of merge two and I'm thinking education and awareness, communication that kind of stuff, because I don't think you can do any of the other things without getting a lot more stakeholders engaged and aware. So if you don't educate people and you don't communicate what's going on then we'll never get the right bodies in place to even, if you create a tool only a few of us will use it, because we'll be the only ones that know about it.

UNKNOWN SPEAKER: So are you talking about only tools or other things?

UNIDENTIFIED SPEAKER: No. I'm just saying education and awareness to all of the stuff. What is cybersecurity? What's going on? Where are these hospitals [indiscernible].

UNKNOWN SPEAKER: And do you list some of those? Do you -- you do start it, sorry.

- - -

(Speakers speaking off of the microphone.)

- - -

UNIDENTIFIED SPEAKER: Okay. I'll do my homework.

DINESH PATWARDHAN: Anymore comments?

UNIDENTIFIED SPEAKER: What about this regulatory class? [Indiscernible].

DINESH PATWARDHAN: I -- I wanted to first finish education and training piece. Anymore comments of that? Okay. Yeah, you have -- there is.

- - -

(Speakers speaking off of the microphone.)

- - -

DINESH PATWARDHAN: Brian, can you hold just for a second, let him finish his comment? I'll bring

the mic.

UNIDENTIFIED SPEAKER: Yeah, okay. So the number of the commonalty of terms meaning of words, perhaps common understanding of evolution of relationship model, premarket versus postmarket versus legacy versus oh, God, who's going to fix it? That sort of thing would fit in with the education.

EUGENE VASSERMAN: So this is the education; right? So the other comment with education is, I think it has to be sort of a multiway street or a two-way street, I think. If you think of it as the cybersecurity experts just going out there and educating all the people who don't know what's going on that's not going to work. I think everybody needs to learn about each other's domain and come up with something that works for the whole group.

- - -

(Speakers speaking off of the microphone.)

- - -

UNIDENTIFIED SPEAKER: Yeah, just to add an additional comment to the normalizing the nomenclature in that the -- I suspect that there will be a tremendous

amount of name space collisions when you look at the three legs of the stools they were talking about. So you've got cyber-usability and then of course safety and so those are all that are to be covered even though we're talking primarily about cybersecurity, so I think that starting in that normalization is going to be tremendously helpful not only to everybody here, but everybody else in the industry and et cetera. Thanks.

UNKNOWN SPEAKER: So, for some time I've been quite concern about the lack of a formal ontological approach to definitions and terminology and if you go to the standards development organizations they'll tell you, well, we have got a set of definitions in the front of our standard and you go onto the next standard and they've got another set of definitions and we've got about 600 standards in this sector.

And if you have 600 standards in any sector you've got no standards in this sector. So, you know, we've got a significant problem in the world of cybersecurity and the ecosystem of sub-security and being able to community our ideas in a consistent and ontologically correct manner. This is actually, I think

a potential research topic itself. Just being able to get that done it may not linguistically anyway, it's the sort of thing that helps a sector be able to reframe its ideas and to have those ideas mapped to other sectors and to other languages. This is an international business, medical devices. A lot of other sectors have taken this approach and we should too.

I have to confess though that I was unsuccessful talking at the standards organizations about this. Maybe this is something we can do in the U.S. and maybe it's something that we can have done for us, you know, paid for by someone like Homeland Security who would have an interest perhaps in doing this.

- - -

(Speakers speaking off of the microphone.)

- - -

UNKNOWN SPEAKER: Yeah, the -- I'm being honest for an example of how this worked in another sector. So in the food and agriculture sector many years ago the FAO which is actually based out of Rome in Italy noticed that the a lot of farming was not being done very efficiently and it was because it was a lot of

mistranslation and lack of interest because no effective translation being done from languages to languages from countries to countries. Like environments could grow like things et cetera, but they didn't know how, so one of the things they approached that overarching problem with was to begin a study in of all things the ontology of farming and agriculture. They built not dictionaries, because that's a degenerate form of ontological map, they actually built the ontology and they published it. It gave rise to in the W3C consortium of an ability to therefore to go out there and look at and sort of distributed knowledge, use search engines to cross language boundaries, geographical boundaries and the like. And knowledge began to emerge by those who sought it rather than those who needed to be taught it. So that's the way that I come at this that when you have a common set of problems you've got to start off with a common semantic framework and get it is another matter, but when you've got it you can make use of it in the modern day and age with information technology.

DINESH PATWARDHAN: Any other comments? I

don't want to stretch this out. Any further unless we have comments. Okay.

- - -

(Speakers speaking off of the microphone.)

- - -

UNKNOWN SPEAKER: Yeah, we've got a limited amount of ability to discuss the regulatory hooks, but I for one as part of the FDA team want to thank you all for coming. I want to say that what I got out of this was some inclination of where the edge cases are. What we can do in the areas that we can affect and who are the people and where they reside to help us manage the other edge cases in this ecosystem so thank you very much for educating me.

UNIDENTIFIED SPEAKER: See like a concluding remark, Brian. So in terms of the regulatory hook here's -- I was having a conversation last night. He's one of the issues that I have. Hard coded credentials are bad; right? So how do you teach a biologist to ask questions that would provide evidentiary basis on premarket that no hard coded credentials have been used? There's a -- help me.

UNKNOWN SPEAKER: I not we stopped at the FDA having a microbiologist doing software reviews.

UNIDENTIFIED SPEAKER: Well, the reality of the situation is that from class one and class two devices that come to the center biologists will do software reviews.

- - -

(Speakers speaking off of the microphone.)

- - -

UNIDENTIFIED SPEAKER: Well, that's the reality of the situation. Class three devices are shopped out to OSSA [ph] I'll sure they'll comment there.

You can't make everybody a security expert that's the gist of what I'm getting at. So how do we adjust that?

UNKNOWN SPEAKER: Do you have microbiologists doing human factor reviews as well.

UNIDENTIFIED SPEAKER: Probably not, but somewhat -- I don't remember doing human factors review in my review days. Anyway, so what are the artifacts of that? So it's a paper based review too so you can't do certain tests that you may do.

UNKNOWN SPEAKER: Sure, it's an administrative review. I -- what I was after was what regulatory looks he was asking for. His name is Rick.

UNIDENTIFIED SPEAKER: I know Rick.

UNKNOWN SPEAKER: Yes.

UNIDENTIFIED SPEAKER: There are many economic drivers to attain a reasonable security. FDA can play a part. I'm asking for help there, yeah.

EUGENE VASSERMAN: I would ask a counterquestion. Given -- let's take it as a given that there's a limited amount of resources and a limited number of people which can be hired to do this would you want a security expert doing a biocompatibility review?

UNIDENTIFIED SPEAKER: Repeat your question.

EUGENE VASSERMAN: Good contributions, Seth. Would you want a security expert doing a biocompatibility review?

UNIDENTIFIED SPEAKER: Actually 10993 is really easy to understand so I'm not sure.

- - -

(Speakers speaking off of the microphone.)

- - -

UNIDENTIFIED SPEAKER: It depends. I had done a biocompatibility review. I'm not a biocompatibility expert, but I think you can be brought up to speed. But, I mean, the reality is that you have to bring reviewers up to a certain level of competence. What level that is, I don't know, but.

UNKNOWN SPEAKER: So we've given up on team reviews. I haven't worked here in a while, so the team reviews are gone.

DINESH PATWARDHAN: I think we are going off topic just a little bit.

UNIDENTIFIED SPEAKER: Fantastic. Sounds heated though and interesting.

UNKNOWN SPEAKER: I'm not sure how off topic that is. The way I heard it is we need to make the security information, security architecture, the security approach understandable by humans and that's not an easy challenge.

DINESH PATWARDHAN: That's right.

UNKNOWN SPEAKER: And that is an open research project.

DINESH PATWARDHAN: Yes.

UNKNOWN SPEAKER: So that is a gap that we could address.

EUGENE VASSERMAN: This time I'm going to be constructive. Whose responsibility -- Todd, who's responsibility would that be. So for example, knowing that there's limited reviewer power, is it up to the manufacturer to make their security architecture understandable by the lay reviewer for very creative values of lay?

TODD CARPENTER: If I'd like my device to get through review quickly, if I'm the medical manufacturer I would say the more easily understandable I make it the higher chance I'm going to get through review. So there's an economic business security benefit in making that.

- - -

(Speakers speaking off of the microphone.)

- - -

TODD CARPENTER: Omission will be -- that's not going to last for long. They will learn enough.

UNIDENTIFIED SPEAKER: Or you could get a third party to certify it.

UNKNOWN SPEAKER: That would be a form of evidence.

DINESH PATWARDHAN: Kevin you had a comment.

UNIDENTIFIED SPEAKER: Certified for what?

- - -

(Speakers speaking off of the microphone.)

- - -

KEVIN FU: Less a comment than a question. I'm just curious within the FDA campus, I'm not sure what the right term would be, but I'll just say computer scientists, but how is the growth of computer science representation been with the growth of computing problems? What does it look like? No, I mean, it's a serious question.

UNIDENTIFIED SPEAKER: I know and you want to withdrawal it.

KEVIN FU: I don't know if I --

- - -

(Speakers speaking off of the microphone.)

- - -

KEVIN FU: I'll leave it at that.

DINESH PATWARDHAN: Somebody had a comment. I

don't know. Yeah.

UNIDENTIFIED SPEAKER: I always thought that if you needed additional help during a review can't they request that and somebody could come in and help them. In other words, if a biologist didn't feel like they had the expertise could they request some additional help?

- - -

(Speakers speaking off of the microphone.)

- - -

DINESH PATWARDHAN: Yeah.

UNIDENTIFIED SPEAKER: So I just this goes back to why the education piece is really important, because if this is going to be a normal part of medical devices we can't be sort of waiting on limited expertise to deal with that widespread issue; right. Somehow the whole industry has to be brought up to speed both on the manufacturer the review side and all of the other users in order for this to work, but if it's so complex a problem and it's in every medical device and we need, you know, only the 10 people in the world who know how to do this to do it then we're not going to get any traction; right. So I think that's what makes the

education piece a very, very, very important piece and education on all fronts to make that happen. Yeah.

KEVIN FU: I like that framing the question. Let me rephrase that too. What should universities be doing in terms of, you know, what's missing in terms of the students coming out of our program? So I'm at the University of Michigan. We teach computer security as well as programming. Only about a third of the students take the security course, so two thirds of them are making the problems, the other third fix those two thirds.

So what kinds of students should we be producing in the future, both from manufacturers, hospitals, regulators, what's missing?

DINESH PATWARDHAN: Thank you. That's -- I'm trying.

- - -

(Speakers speaking off of the microphone.)

- - -

DINESH PATWARDHAN: Yes. And that's why that question was extremely important.

KEN HOYME: So I'll offer an answer in terms of

what I think the security focus that tends to come out of a lot of the schools is IT security which really focuses a lot on privacy and privacy protection. What we're dealing with in the medical device space is embedded systems and the safety security, the integrity availability side of things. There isn't a lot of programs that combine the knowledge of interacting with the physical world and interact -- and securing it against potential threats. The National Academy has just produced a report on a degree program in cyber physical systems and in there they were looking at ways that you -- given that with the Internet of things is going to be producing more and more of these cyber physical systems. It was kind of a curriculum for a four year program and a master's program, I believe in cyber physical systems and I don't know if there's, I guess there's a couple of schools that are starting to think about implementing that type of a program, but I think the medical device world could use cyber physical system security more than IT security.

DINESH PATWARDHAN: So Brian mentioned an important thing which is NSF is our partner and we will

try to include that having training at the university level will certainly help in this area.

UNIDENTIFIED SPEAKER: So Kevin, because you touched on the workforce problem a little bit you're absolutely right, you know and your school is one of the better ones, so if one third of the engineers coming out have had one security course I would say that that's probably a societal failure, you know, we're generating the problem faster than we're able to fix it. Which is not a ding on your school, right. Or on anybody in here who's a professor in the academic community.

I'd also say that in the universities it's -- there is some IT security stuff, there's also some very theoretical things that are really neat and interesting, but that aren't, you know, don't help us today, so we'll need those. We'll need all of those down the road, all right.

I saw something the other day that said we have about a six million person skills gap globally and whether it's actually six million or I've heard closer to one million, still seven figures; right. So it -- I don't care whether it's either one of those, but if we

take and Kevin, you've quoted a number to me of about how many years does it take to make a secure developer of study, like?

KEVIN FU: Oh, from an undergraduate?

UNIDENTIFIED SPEAKER: Yeah. Like.

KEVIN FU: You can make a pretty good hacker in three years. You could make a pretty good engineer after that and a lot of experience in the field.

UNIDENTIFIED SPEAKER: Right. So three years minimum bar to getting the people we need if we start today. So how do we get six million people started on this journey to become security professionals?

UNKNOWN SPEAKER: There's an addendum.

UNIDENTIFIED SPEAKER: Okay.

UNKNOWN SPEAKER: If you're going to design protocols so the underlying communication structures not necessarily with a patient, I would put another four years.

UNIDENTIFIED SPEAKER: Okay. So --

- - -

(Speakers speaking off of the microphone.)

- - -

UNKNOWN SPEAKER: I can rephrase it.

UNIDENTIFIED SPEAKER: For a hacker. Let's -- if it happens it happens.

- - -

(Speakers speaking off of the microphone.)

- - -

UNIDENTIFIED SPEAKER: Okay. So I don't want to get bike shedded on how many years it takes to make a security person. The point is it takes longer than we've got and we don't have the time to start and by the time we get there we'll need more than we started needing. This is a long-term problem that we've got to solve. There's a short-term problem that we have though, as well. And just like when we walked in here we didn't walk in to find a giant exoskeleton of protection keeping the building up, right, it just stood up on its own.

The way that we've done this in other disciplines is we cut out the specialty or cut down the need for the specialty of someone who's doing security or safety or those types of things. And so I think the answer is we've got to do the same thing or similar

thing in IT security which is we've got to cut out problem space faster than we're generating it. And that takes new architectures. That takes not just better coding, but better ways of implementing and we've got a lot of those things, we know how to do them, right. I said yesterday, I said today, if you're familiar with OWASP, they do a great job of generating information. They don't do a great job of distributing the information and William Gibson said the future is here, it's just unevenly distributed. The point is, maybe it's not that we need more knowledge. Maybe it's that we need a better way to distribute that information and get it into people's work flows which can be an educational thing. It can also be an incentive thing, so if you only pay engineers when they're software passes pen tests you'll get a very different product then if you pay them for the number of lines of code they write and the number of time they spend writing it.

So this is a broader issue than just education, but that's part of it. We've also got to realign some of the incentives that we've got. We've got to realign some of the processes so if it's as easy to review a

security package or a cyber safety package in a 5, 10k then maybe you don't need security people to do it. Maybe it could be a biomechanical engineer or whoever else you've got, but it takes a look cross all of the processes that we have and all the systems that we've got to fix it and some of that can be generated in NSF or DHS grants. Some of it can be generated just inside the FDA with some of the mechanisms that you're using, but it takes a lot of us working together is what I would say.

UNKNOWN SPEAKER: Let's not forget that the building stands up. There's a lot of building that fell down, because there's a building code, because there's no building inspectors, because there's lots and lots of bad experiences that have resulted in best practices that don't always get followed.

UNIDENTIFIED SPEAKER: Yeah, there's a whole process around build ing codes. I absolutely agree and I'm not trying to make a direct correlation.

UNKNOWN SPEAKER: No. I'm not criticizing, I'm --

UNIDENTIFIED SPEAKER: Yeah.

UNKNOWN SPEAKER: -- just saying that the problem are there's a lot of complexity.

UNIDENTIFIED SPEAKER: There is. Yeah.

UNKNOWN SPEAKER: And it's easy to overlook the complexity because we've lived with it for so long.

- - -

(Speakers speaking off of the microphone.)

- - -

DINESH PATWARDHAN: It is 3:50, that's according to my watch. I want to personally thank you for sticking to the end. We will not call it the bitter end, because it was a very great discussion.

UNIDENTIFIED SPEAKER: The sweet end.

DINESH PATWARDHAN: With this I call the end of the workshop. If you want to have individual discussions please stay around. Thank you.

- - -

(Whereupon, the proceeding was concluded at 3:53 p.m.)

- - -

CERTIFICATE OF NOTARY PUBLIC

I, Michael Farkas, the officer before whom the foregoing proceeding was taken, do hereby certify that the proceedings were recorded by me and thereafter reduced to typewriting under my direction; that said proceedings are a true and accurate record to the best of my knowledge, skills, and ability; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this was taken; and, further, that I am not a relative or employee of any counsel or attorney employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Michael Farkas
Notary Public in and for the
State of Maryland

C E R T I F I C A T E

I do hereby certify that the aforesaid hearing was transcribed by me from an audio recording to the best of my ability; and that I am neither of counsel nor kin to any party in said action, nor interested in the outcome thereof.

WITNESS my hand and official seal this _____ day of _____, 2017.

_____

Janine Thomas

Notary Public