Tom Kraus: All right. It looks like the numbers are picking up here. So, I'm just going to give folks another few seconds to dial on before we get started. Okay. Good afternoon. I'm Tom Kraus, vice-president of government relations at ASHP. As a former FDA associate commissioner and chief of staff, I'm proud to continue supporting the agency through the Alliance for a Stronger FDA. We are delighted to have you with us for today's webinar on cybersecurity and digital health with Dr. Suzanne Schwartz. This could be a meaty topic, and I want to thank all of the Alliance members, and guests, and media for joining us today.

Before we begin, I do want to put in a quick word about the Alliance for a Stronger FDA. The Alliance is a multi-stakeholder coalition of advocates for increased appropriated resources for the FDA. We have been an important force in the doubling of the FDA's budget authority funding from $1.6 billion to more than $3.3 billion. Our other mission is to educate policymakers, the American people, and media about the FDA's growing missions and responsibilities. We're the only advocacy organization focused on resources for both food safety and medical products as well as other components of the FDA mission.

Our members include consumer and patient groups, research advocates, health professional societies, trade groups, and industry. We have about 160 members, and we welcome new members to further strengthen our advocacy and educational efforts for the agency. Today's webinar format will follow a two-part approach that's worked well with other webinars. So, we'll start with Dr. Schwartz responding to questions that the Alliance has provided in advance. And we'll follow-up with ample time for her to answer some of your questions, which you may submit by clicking on the Q&A button at the bottom of your screen.

Our moderators for today's event are Nancy Myers and Zachary Rothstein. Nancy is the CEO of Catalyst Healthcare Consulting and is an expert on cutting edge biotechnology and med tech issues that should come up today. And Zach is the Senior Vice-President for Technology and Regulatory Affairs at AdvaMed. Before I introduce today's speaker, the Alliance would like to particularly thank Letise Williams for her help coordinating this event. So, I now have the privilege of introducing our speaker, Dr. Suzanne Schwartz. She is the Director of the Office of Strategic Partnerships and Technology Innovation at FDA's Center for Devices in Radiological Health.

Dr. Schwartz became Director in September of 2020. Her prior experience includes serving as a lead clinical reviewer in CDRH, and as the Associate Director for Science and Strategic Partnerships at CDRH. She chairs the CDRH Cybersecurity Working Group and co-chairs the Government Coordinating Council for the critical infrastructure sector focusing on healthcare and cybersecurity initiatives. She's a graduate of the Albert Einstein College of Medicine, trained in general surgery and burn trauma, received an MBA from NYU Stern, and completed Harvard's National Preparedness and Leadership Initiatives. So, Dr. Schwartz, thank you so much for joining us today and sharing your perspectives. The floor is yours.

Dr. Schwartz: Thank you so much, Tom. And I just want to say, it's with great privilege to speak with the Alliance today. And we really couldn't have wished for a better timing to showcase the important work that is happening within our office, OST. So, what I mean by that is I think that many of you already know that this month, October, is National Cybersecurity Awareness Month. What you may not know is that October is actually sandwiched in between two other really important months, and that is September being National Preparedness Month, and November, being Critical Infrastructure Security and Resilience Month.

And so, in essence, we have hit upon a trifecta, if you will, where OST shines in the efforts in the programmatic areas we currently work. Number 1, we know emergency preparedness in being able to not only be at the ready, but then, also be in responsive mode to matters of public health concern as they involve medical devices. Number 2, as we are in October right now, cybersecurity of medical devices. And Number 3, speaking to enhancement of resilience with respect to the healthcare and public health, or what's called HPH, critical infrastructure sector writ large.

And while we can view that through many different lenses, for the sake of today's self-interviewing discussion, I especially want to hit upon something that's very germane, which is on the supply chain side of medical devices. Now, while these programmatic areas are of high visibility, our portfolio is quite expansive and I think that Nancy might've even sent around on LinkedIn a link to OST's portfolio on the FDA website. And just to name a few areas, we've got: Standards and Conformity Assessment. We have Health of Women; Pediatrics and Special Populations.

We have Digital Transformation. Of course, we have the Digital Health Center of Excellence. We have Patient Science and Engagement. To name just a smattering of the items within our portfolio.

Which, begs the question, as to how did OST come to have so many seemingly disparate elements? So, I want to share with you our, what I'll call our OST origin story. OST came into being in May 2019. It was a part of a more overarching CDRH reorganization. Our office is largely spun out of programs that initially existed within the Office of the Center Director but was also joined by programs that existed elsewhere within CDRH.

As you can probably imagine the challenges of undertaking this type of reorganization in bringing folks together, especially those who are uprooted from other places within the Center, where they have identified as belonging. So, first and foremost, for me in my role, initially as the Deputy and as the Acting Office Director was really to kind of create an identity - a set of values that would resonate with the staff across the board, and that would ultimately provide the type of inspiration that is so important for the work that we do across all of our highly valued staff members.

So, as an office, one of my first undertakings was working on, what is it that we, OST, stood for. What's our identity? Most holistically, how do we view ourselves? How do we brand ourselves? How do we even maximize? I'll take a step back, how do we identify and then, maximize the synergies that do exist across this programmatic kind of huge-huge expanse. And just to thread an example of that, where we have looked really maximized that in a very deliberate way is - you've got Patient Science and Engagement as one programmatic area. We have Cybersecurity of Medical Devices in another. Isn't it important for us to be thinking about the confluence of what the impact is of engaging with patients on advancing and enhancing cybersecurity of medical devices?

So, to continue with my little story here, rather than be known as OSPTI, which is our formal acronym, Office of Strategic Partnerships and Technology Innovation, if you would have to verbalize that, it comes out as "Ospeti" which is certainly not something that rolls off the tongue in a very favorable way. So, we shortened our acronym to OST.

And as we worked on really what our identity is and what we stand

for, we came up with the notion of what we aspire to be. And what we aspire to be as an Office is - Stewards of Transformation. Our values are Impact, Integrity, and Innovation. And we believe in embodying the principles of Inclusivity, Transparency, Rigor, and Agility in everything that we do and how we go about our behaviors, our work day-to-day, our interactions whether those interactions are internal, within the office, within CDRH, within the government, within the agency as well as being reflective in how we interact externally with partners across the entire ecosystem.

So, coming to Question 2, what are our key priorities over the next year? And I'll start with cybersecurity in a very, very tangible way, we are leaning forward and are intending on releasing the final guidance for cybersecurity of medical devices on the pre-market side. As many of you are probably aware, we issued the draft of that guidance in April of this past year, and we had been working very diligently and expeditiously in response to the public comment that has come in, very robust, and certainly, a large number of comments that have come in, (in order to address those) and to meet the moment appropriately of being able to finalize this guidance and get it out within this current fiscal year that we have just entered.

Secondly, on the cybersecurity front, we have been working closely and continuously with our partners across the ecosystem to really try to make a very strong and compelling case for FDA to receive authorities in the area of medical device cybersecurity. And what I mean by that are explicit authorities, authorities that will enable us to really very closely tie the importance of cybersecurity of medical devices to their safety, and their effectiveness in terms of their performance.

We know that this is critical. We've done everything we can in a more implicit manner to really make that bridge. But it is so important now to really be able to either take that to the end as far as needing additional authorities or specific requirements. Also, separate from cybersecurity, in terms of key priorities over this next year, we're further evolving and we're solidifying the work that we are doing in what was initially established earlier this year that is our supply chain resilience program.

And with that notion, resilience, of course we are talking about shortage mitigation. But ultimately, where we want to be able to get to in this more multiyear vision is prevention of shortages, being able to understand what the entirety of the landscape and the supply

chain looks like. And in order to be able to really build upon the idea of resilience. And I'll add parenthetically that the theme of resilience is one that really runs through so much of the work that we are doing, driving lessons learned from throughout the pandemic.

And the recognition, really, as it comes back to supply chain, that over-reliance or over-dependence on certain sources of materials, component parts, manufacturers, other entities can wreak havoc in making us as a nation that much more vulnerable to supply chain disruptions. And what those vulnerabilities and those supply chain disruptions lead to ultimately is inability for patients and providers to have access to medical device products that they need.

Another key priority in the near-term is really in propping up the efforts of and the visibility of the Digital Health Center of Excellence so that it is certainly well-poised and well-resourced in order to meet the needs - and take on the challenges of - future, emerging technologies. And there is no doubt there is a lot of work to be done on this front, especially as we speak about policy development. We have been very heavily at work and the DHCOE has done so much great work in terms of putting out documents, guidance, reports, frameworks, and we're going to continue to do that. But to really ramp it up even more to obtain the type of visibility that is so necessary, especially during a time when we are seeing technologies that are emerging right and left, and that really warrant us thinking about what's around the corner, and how do we best meet those needs.

Now, as we look over the horizon, from this year into the next few years, I would be remiss if I didn't highlight the very important CDRH strategic priority of Advancing Health Equities which, OST is very honored to co-lead on behalf of the Center along with OPEQ. We have long envisioned the potential - the promise - for digital health technologies to be true enablers in addressing inequities in healthcare, and in being able to reach remote populations, underserved communities. So, kind of pulling on the thread that I mentioned a little bit earlier in terms of maximizing synergies across the office, this is another really good example of where we are working right now on laying out that blueprint across our patient science and engagement programmatic team along with Digital Health and the Digital Health Center of Excellence to create what would be, again, this blueprint or roadmap for work to be done over the next few years that truly leverages the innovative technologies of today and tomorrow in order to close the gaps that we're seeing

today with respect to health inequity.

So, speaking of Digital Health, you might be wondering how does the Digital Health Center of Excellence – I'll call it DHCOE for short, interact with other Centers? This is another example of really recognizing the criticality of collaboration across other parts of the agency on issues that are cross-cutting issues. We've established over the past, I would say, close to around one and a half years ago with the launch of the Digital Health Center of Excellence, we subsequently put in place what we call the DHAB, the Digital Health Advisory Board.

And the Digital Health Advisory Board, it's internal to the agency, and its intent is to really have that roundtable bring together leaders, subject matter experts, across the different product centers, across different offices within the agency to have a place, a forum to discuss common interests, current challenges. To really roll up sleeves and you can talk about workstreams and how we can, working together, achieve certain common goals.

And I think that while that effort was nascent about a year and a half ago, we're now seeing that pick up greater momentum by meeting more frequently, by the DHAB itself creating smaller work groups, if you will, that are populated by staff across the different product centers, and have different leads, with different tasks. We are in the process of actually establishing a new workstream on cybersecurity that would fit under the DHAB recognizing that while so much of the work that we've done at the agency for product cybersecurity has been within CDRH on the medical device front. Clearly, that needs to really be expanded and extended across other product domains, other product areas in terms of CDER and CBER. And so, this gives us the opportunity, again, leveraging the DHCOE and the DHAB as a mechanism to really bring the efforts together in greater alignment.

It's worth also, taking another moment to underscore that while we share common issues with other product centers, and it's important for us to have that kind of cross-visibility whether it's in cybersecurity, in supply chain, in fraudulent or counterfeit products, our approach in CDRH at times, will certainly differ from how the other product centers work.

I do want to underscore here the importance of us definitely having that cross-visibility because we do learn from one another. And

knowing best practices or knowing what's worked well and how we can borrow that at CDRH or how another Center can borrow what we've done is really critical to making the agency be really in the best place, in the best position to address some of these very, very difficult challenges.

And I think for CDRH, one of the ways that we've been different is, well, we've had to really be creative and out-of-the-box thinkers for a number of these, given the history of absence of resources, absence of appropriations, absence of authorities and really looking, recognizing that these are issues that have to be dealt with, and we have to figure out a way to do what we need to do with what we have. And so, that really provides a playground, if you will, for innovation: for innovating around what we do and how we do it so that, as a Center, we're not only working towards approving and clearing, getting marketing authorizations out there for innovative products, but that we are really constantly iterating, evolving, and innovating in how we look at different challenge areas, and how we think about them, and how we deal with them. I would say that certainly, in the supply chain area - - to take one example - - I think folks, probably from the Alliance recognize that pre-pandemic, CDRH had no dedicated resources for shortages at all; No resources nor any particular authorities.

And we have a history of having had to deal with a shortage or a crisis literally as it was unfolding which of course, puts our Center in very much a reactive mode and really required making the most out of folks who are working in other areas like our Emergency Preparedness or All Hazards Response team in order to wear multiple, different hats. We've learned a lot, from CDER over the past several years and the pandemic, in terms of the shortage program that they have established that is quite mature in terms of what they have accomplished. So that as we received our initial authorities through the CARES Act in 2020, in March 2020 - which we're so grateful for - the funding on the COVID side in order to be able to put a program together, we recognized for us, that what would be critical is being anticipatory. Being able to lean forward. Being able to understand and have a visual into supply chain, more end-to-end, to understand what's happening before we're on the heels of an actual crisis of products not being available on the shelf, of pediatric patients not having available tracheostomy tubes, etc., etc. How do we position ourselves? What should our posture be?

And how do we setup a program with the resources that we were

given that really seeks to do a better job at envisioning the future, and being, again, anticipatory? And that's been, I think, a distinct feature that we're very proud of in terms of what we have established thus far, again, very early and very nascent in what we have done. We did just convene a public workshop as well back in June of this past year.

And I couldn't be, first of all, more delighted to have as Associate Director and program lead, Dr. Tammy Beckham, who is just extraordinarily visionary, and who has really brought together and mobilized the subject matter experts from various disciplines in order for us to be better positioned to undertake this effort. But really key to that is – obviously, not only having the resources and the authorities. But recognizing the criticality of the engagement with our stakeholders, the collaborative piece, the community piece.

And that tends to be a running theme through a lot of what we have built. We can take cybersecurity as another example of that. And that goes to the question that was asked of me: how has the FDA built a cyber team and increased its expertise in the field? Our team has very few people on it at present. We are on a shoestring budget, if you will. But what we did from the very beginning is this notion of we've got to really immerse ourselves in understanding this space, leaning forward, really collaborating with the community, what I call, 'whole of community'- at – large, meaning: the medical device industry; the security industry; security researchers; healthcare delivery organizations; other government entities; patients; providers; really across the board. And through this effort of collaboration-building and understanding what are the challenges; what are the pain points; how do we move this ecosystem; how do we move the needle to a better place. That has been the foundational efforts that we undertook over the initial years. And to this day, we have very little, by the way, in the way of appropriations for cybersecurity.

We do have an ask on the table. That is public. With regards to being able to do more and bring in more FTEs for cybersecurity. But I think it speaks to – our work is really looking to be creative, out-of-the-box, and to be collaborative in everything that we have done.

Let me turn to one of the next questions that was asked of me. I mean, you might wonder how does our work in cybersecurity align with that of, you know, the work happening with other Centers at FDA as well as Digital Health.

So, on the Digital Health side, I think I spoke to it a little bit earlier. Again, I mentioned the fact that with the Digital Health Center of Excellence standing up this DHAB, the Digital Health Advisory Board, really allows us that level of being able to engage and to have this ability in what's happening with respect to the other Centers, and how we come to places of alignment. Cybersecurity is interesting, again, because while there has been so much emphasis, so much focus placed on medical devices themselves, we recognize that cybersecurity across the healthcare writ large ecosystem goes well beyond medical devices.

But we can talk about its impact in drug manufacturing. We could talk about its impact on the food side, as well, impact on biologics. And so, what's been important to us and what we have been undertaking over the past year-plus is really mobilizing our own CDRH CyberMed team to bring together folks within the other product centers to further inform, to educate, to provide examples of the work that we've been doing to share, to talk about how do we look towards addressing cybersecurity for the healthcare sector as it relates to products that FDA has oversight of in a more holistic manner. Right?

And that's been a very well-received effort that we've undertaken, and that we will continue to grow. In fact, one of the opportunities that we've seen in front of us is while the CyberMed team that's on my staff have been the ones engaged in this kind of outreach with our other product centers across the agency, we're going to mature that and evolve that further into it being one of the work streams under the Digital Health Center of Excellence's DHAB, the Digital Health Advisory Board.

So, that there will be opportunity, really to more institutionalize, if you will, the work that has to be done, the awareness, the situational awareness around cybersecurity for policy development there, the understanding of how to evaluate, how to assess a vulnerability. The impact of a vulnerability as it might cross over across multiple products, areas outside of medical devices into the drug manufacturing, the biological manufacturing, or on the food side, as well. So, those efforts are ones that we are undertaking right now, and they will obviously continue to grow and to mature as we move along.

So, with all of this talk about engagement and collaboration, the

Alliance might be wondering how is it that we do outreach to third parties. And you know, my answer to that is - I can say there is no secret sauce, if you will, with regards to how we do that. I think that we like to keep things simple. And that means really just, first off, keeping our finger on the proverbial pulse of what's happening throughout the ecosystem as it relates to areas that are touchpoints for us within OST.

And by understanding what's happening, that also lends itself to our asking the next question, how can we do better? How can we do better by connecting directly with folks, whether it's on an individual level, whether it's on an organizational level. It's about creating those initial touchpoints and being proactive in doing so. And maintaining what I consider, what is important for us at the OST leadership level, myself and my partner, Dr. Michelle Tarver, as my Deputy Director, really creating an environment that people understand there's an open-door policy of approaching us, and that we are not going to hesitate towards reaching out to others.

And obviously, there are formal ways in terms of engagement that become necessary in the way of whether it's executing agreements, or research agreements, or partnerships, or MOUs, or MOAs. And that's always going to be a part of work that we do whether it's across government, whether it's across the private sector. But first steps first, it's really about not being at all hesitant in picking up the phone, writing an email. But picking up the phone and calling and speaking with folks, it's really just kind of as simple as that.

So, I think this ends my portion of the self-interview. Hopefully, I've covered the questions that the Alliance had wanted me to cover in this section. But I look forward to the questions that the panel has for me. So, perhaps I can either elaborate or touch on things I didn't get to. Thank you.

Zach Rothstein: Suzanne, thank you so much. That was just a fantastic self-interview. I'm really impressed with how well you can manage all of those questions in a single monologue. So, thank you so much for working through them, for providing that update, and for starting off this webinar with such a great set of remarks. We do have a couple questions in the chat already. And I'll pick a couple of them out for you because I think they have a nice follow-up theme to the items you were speaking about cybersecurity.

On, is specifically about the cybersecurity expertise right now,

within the Center. You mentioned that the team is on what you called a shoestring budget. So, are there certain things that you wish or that the team should have more capability to do, but that you just don't have either the bandwidth or the funding to accomplish right now?

Dr. Schwartz: Yes. So, first let me say that we are also very intent on recruiting right now. We do have a few individuals that I'm really excited about who will be onboarded very soon, who bring different types of subject matter expertise that I think is going to really add extraordinary value to the work that we do within the Center. But what I would say is this, one of the challenges – and Zach, I think you're very familiar with this, is that even the whole topic area of medical device cybersecurity is such a niche area.

And it's not an area that we have seen when we've looked back at, and we continue to drill down into universities, academic places as to whether that is an area where there's interest in developing curriculum, developing graduate studies, expertise that could then go into the field, if you will. I do think that that's something that not just obviously we at FDA, but across other parts of government is focused on, of how to really kind of cultivate a workforce, a workforce that will represent newcomers into the field, but that are bringing a constellation, if you will, of all of what is needed within the cybersecurity of medical device space.

As opposed to it being a siloed expertise that you really – you have to bring ten people together – ten is probably an exaggeration – but you need to bring multi disciplines together to try to get a holistic view of a particular, whether it's a product cybersecurity, or whether it's assessment of a vulnerability with regards to a medical device, and what is the impact of that assessment. And does it have a safety impact for patients? And if so, what do we do about it? So, I think that a lot of it is really looking towards the future around what can we do even at FDA, potentially partnering with academic centers, with universities around potential internship programs and development of curriculum.

I think folks are probably aware that we had a wonderful guest as an Acting Medical Device Cybersecurity Director in Dr. Kevin Fu, who was on sabbatical in prior year. And this is an area that he is very engaged in, and that what he did, even in terms of launching for us at FDA through the CERSI program, a lunch-and-learn series, **[inaudible] [00:37:18]** let's make sure that this is understood to be

an area important to FDA, important to the academic community, important to the user community, important to the device industry community that we're looking to build that.

Zach: Yes. And I think that's a really good point that the educational piece is a really important element of training the next generation of cybersecurity experts and making sure that they realize this is a space that really could use that level of expertise. Do you plan to have a new replacement for what Kevin's role used to be?

Dr. Schwartz: We will look to recruit a Director of Medical Device Cybersecurity. I don't know whether we'll be able to achieve that within this coming 12 months. We're working towards that. But we will be recruiting for that position, yes.

Zach: And one more cyber question before I ask Nancy to take a couple. So, in terms of the cybersecurity requirements that FDA has in place today and helping manufacturers understand in particular, the pre-market processes that are required of them. FDA just recently announced that they're starting to pilot it under MDUFA V. Is TAP a program that you and your team will be part of, and in particular, any cybersecurity elements in how they might be involved in this pilot going forward?

Dr. Schwartz: Yes. That's a good question. So, I will say, first off, kind of zooming out a little bit, OST will be involved in the TAP program, in certain areas as it relates to breakthrough devices, which is what TAP is really designed to support. Certainly, in the area –.

Nancy Myers: Can you explain? Because I'm not sure everybody knows what the TAP program is unless you've been following the user fees. Can you just back up 30 seconds on TAP?

Dr. Schwartz: Yes. TAP stands for the TPLC, Total Product Life Cycle Advisory Program. And it is a program that has been funded in a pilot form through MDUFA V in order to really do what we can in a more innovative manner to push what would be devices that have the breakthrough designation to be able to get through the kind of the FDA marketing authorization process in a more accelerated and more streamlined way, to bring all the pieces together that will be very helpful, very beneficial to the sponsor, to the manufacturer.

So, that means really having an understanding of the patient perspective, empowering patients to provide information

particularly around breakthrough as to why this device is important. Having a perspective from the provider side to really try to bring all the players to the table almost as though, you know, it's a cohort of folks that can engage with the sponsor in that regard. That's probably the best I'm going to do off the top of my head.

Nancy: That's perfect. That's exactly what I needed, thanks.

Dr. Schwartz: Okay. But getting back, I guess, to Zach's question as to whether cybersecurity itself, or an FTE for cyber would be part of the TAP. I don't think we were envisioning that aspect of it. I suppose if there was some breakthrough element, that's a different story. But really, where we're going to be focusing on the TAP side is in the patient science and engagement.

Zach: Thank you.

Dr. Schwartz: Mm-hmm.

Nancy: So, that's actually, the TAP program, it's fascinating. But the thing I wanted to ask about is part of your organization is to advance innovation, especially the breakthrough innovation. So, what kind of steps is CDRH taking to advance innovation? And I know you've talked about lots of cybersecurity. You've talked about the Digital Health Advisory Board. And I'll ask a question about that. But are there – you've done a lot on AI and machine learning. How does CDRH kind of pick those topics? And then, how do you kind of choose to advance them and find the people to advance them?

Dr. Schwartz: Yes. That's a really good question. So, some of it isn't so much topics that we've picked, but recognizing that, again, where is the puck going, and really trying to skate there so that we can meet there at appropriate times, as opposed to trying to catch up with it. And recognizing that so much of the emerging technologies today are really happening within the digital health, and the AIML space. And I would be remiss if I didn't mention all of the work happening around wearables, and sensor-based wearables that frankly, are changing the way healthcare is being viewed.

If you want to even call it healthcare. It is really more about wellness. Right? About not waiting until one is ill, or one has a disease diagnosis, or a chronic illness, but rather people, individuals as a whole, the population, are very interested in being much more in touch with - - and being empowered with - - what's going on with

themselves physiologically to the extent that they're wanting to take advantage of different types of sensor-based wearables.

So, a lot of our work happening across with industry as well is recognizing that. And what does that mean even in terms of reimagining or re-envisioning how care delivery is taking place as far as in the home, or outside, as opposed to what was in the standard brick-and-mortar facility of the healthcare institution, the hospital, the clinic. These are important observations, some of which have been building up since prior to the pandemic.

And I think that the pandemic, COVID-19 and how care had to change during the pandemic. How we saw innovation happening in the context of a national crisis, if you will, really has within it – I shouldn't call it a silver lining, but there were lessons learned there that impact on the direction that technologies will go in the future. One of them, as I mentioned, was the health inequities that rises to the fore that had been under the radar for a long time. But another also, is just simply the reality that many providers were not able to see patients, their patients face-to-face in the clinic, or in the hospital, or care needed to be rendered elsewhere.

And what is that kind of trite phrase that, "Necessity is the mother of invention" something like that. I think it's really about recognizing that we are in a very different place now and where we're going. And keeping our eyes on the horizon as to what we need to be doing as a result of that. And AIML, as an example, is an area that warrants a fair amount of work on our part.

Nancy: Do you have a team that skates to the puck? And I just – because I worked sensor technology 15 years ago, and it was very hard to get everybody to realize that it was a device. But how do you –? Do you have a group that is looking for that next thing that really is going to change how we give care?

Dr. Schwartz: Yes. I think, and particularly, we're talking about the work happening within the digital health division, the Digital Health Center of Excellence, there has been a very concerted, a very dedicated effort to recruit individuals who are bringing that passion, that desire, that energy, and the experience, enough experience to be able to do just that. And it is very encouraging for me, and very promising to see some of the, again, recruits that we are bringing on board who, I think, really just change the nature of what we had been doing years back and position us well as we look towards the future.

Nancy: Let me just ask one question about staffing because with COVID, everybody is working remotely. And if you're bringing in new experts, how, as a manager of a large organization, how are you making sure that those connections are happening, and the mentoring is happening for younger teams? Because so much that happened – I'm former FDA, too – so much of that happened in the lunchroom or just somewhere else. So, how are you managing that? Because this is a big change than what was there three years ago.

Dr. Schwartz: Yes. That's a great question. And I think that's another example where we've had to be really creative and innovative. And some of that, I won't take credit for, it comes from our folks – on their own, looking to create opportunities by virtual platforms as well as now, you know, even meeting in different types of scenarios in order to create that kind of kinship, and community, and peer-to-peer mentoring as well as mentoring that we are establishing for folks that are, again, newly onboarded through the pandemic who've never stepped foot on FDA campus. Right? One thing that has been important to me, I want to circle back to it.

I mentioned at the beginning that in setting OST up in terms of being a new organization, and the culture, and I talked about the sense of inclusivity. That inclusivity and belonging was important. I have asked myself and I've asked each of our managers to take on a core value, and one that they would not only espouse, but therefore, be able to demonstrate, and internalize, and show. And for me, it's been about showing inclusivity and belonging by reaching out to every staff member. I've not made it through the entire office, yet. I will say that.

Nancy: Good for you.

Dr. Schwartz: But I have been, through my assistant's help as well, setting up one-on-ones with every single member of our OST organization so that people, whether they are new to the organization, whether they've been here 10 years, feel valued, feel that what they do has impact.

Nancy: Are you sensing some burnout? Some potential burnout because of the heavy workload during COVID? I think other parts of the FDA have kind of admitted that they've seen some of that, but have you?

Dr. Schwartz: There has certainly been burnout, or signs of burnout. I think what we really try to do across OST and other parts of the Center is

empower managers as well in terms of really looking for what might be the initial flag of that, and addressing it, and making sure that a sense of quality of life, a sense of people need to take a break, people cannot be working around the clock, which there is a tendency to do even more of when you're working at home because there is no divide between the workplace and home if you've got files that you're working on or whatever it is.

It's harder for people who are very conscientious and very committed to walk away from their laptop. So, I think that there's been a lot of emphasis at the Center around wellness as well, and making sure that managers are appropriately equipped to identify what might be areas of – or signs – early signs of burnout or fatigue, and that people need to re-charge. That people need to re-energize.

Nancy: Great. Zach, let me pass it to you again.

Zach: Thanks, Nancy. Thanks, again, Suzanne. So, Suzanne, you and I have been on a lot of panels together, and sometimes I like to, towards the end, ask you these open-ended, maybe a bit ominous-sounding questions. But I'm truly curious today. We haven't done this in a while, you and I. But what are the cyber risks today that are kind of keeping you awake at night that you're most worried about?

Dr. Schwartz: Yes, Zach, and I will say that some of that evolves, especially given what we're seeing today. So, I'll start off by answering it, kind of scoped, very specifically to medical devices. And then, I'm going to kind of zoom out a little bit further based upon what we're seeing in the ecosystem. For medical devices, I would say our biggest challenge today remains the legacy drag. The legacy technologies or devices that are in place within healthcare organizations that while they work - that they function clinically, and therefore they're providing value to providers and they are depended upon to provide the kind of functions and performance that they do; but they are so very vulnerable, and they are brittle in many cases, in terms of being able to receive the kinds of updates, or patches, or fixes. So, that's very worrisome. And as you know, one of the reasons why it's particularly worrisome – we have not really been able to come to a place of being able to solve this, since this is not just merely a technology matter. This is an economics case as well, a very, very significant one. And so, I do see this as a whole government, as well as whole of community needing to come together to solve that.

I want to zoom out for a minute and talk about ransomware attacks

on healthcare institutions, on hospitals which have just really risen to a far greater frequency over the past several years. And we've seen one, we know of one that right now, that has not been fully resolved. And what the impact is on the ability to deliver healthcare that is not degraded. And while that certainly has an impact, it can have an impact on the functionality of medical devices. I'm very concerned – and this is wearing my government coordinating council hat is, you know, for the healthcare public health sector, with respect to even if devices aren't affected, the fact that systems are down. And that clinicians who totally rely on those systems to be able to make decisions, perform evaluations, provide care without that, we're operating blind, to a great extent. And patients will suffer as a result. They will. I think that that is becoming more and more apparent. And not to sound too scary, either, but it is cybersecurity awareness month, and I think that to some extent, there is a failure of imagination out there with regards to the fact that many of these systems, if they were to be taken down, and if it involves multiple institutions, then healthcare, the ability to deliver healthcare kind of can grind to a halt. Very much like any natural disaster. And are we, as an ecosystem, ready to deal with that?

Zach: And I saw last week the White House announced a new initiative through HHS on healthcare cybersecurity, and it sounded like it was at least initially focused more on the hospital side. Are you able to share any more information about that initiative?

Dr. Schwartz: I don't really have any more information on that. I think that we're all going to be waiting with bated breath to hear a little bit more about it.

Nancy: How about – we do have a lot of food members, and are there any cybersecurity issues that you've kind of been thinking about on the food supply chain side?

Dr. Schwartz: Yes. I think that that is an important piece to bring up. And I do want to mention that we, at CDRH, on the CyberMed team, have been working very closely with CFSAN folks on really kind of exchanging or sharing best practices, and recognizing that there are some really similar – there is real parallel with regards to supply chain, and impact on supply chain, and how that can have a cascading effect with regards to, obviously, the ability to not compromise the food supply. So, that is work that we're going to continue to develop as we go forward.

I think that we were very pleased to find our kindred spirits, if you will, on the CFSAN side, recognizing that we're stronger if we do this together, for sure.

Nancy: Great. And I know one thing that the administration has been very focused on is health equity and all of that. Have you – and we really haven't touched on the Women's Health Office that is under your purview. Is there anything really interesting happening with that group that it would be – it's not quite cybersecurity, and it's not – well, actually, it could be digital health solutions. But is there anything that you've been working on there that this group should know about because we're talking about resources?

Dr. Schwartz: Yes. So, we have a Health of Women Program within OST. And this program also led by Dr. Terri Cornelison, who is quite amazing. She set a strategic plan, an agenda, if you will, for Health of Women within the medical device space. And there are three elements to it. I'll just kind of overview. They are important to health equities, without any question. One, is sex and gender- specific analyses and reporting. The second is integrated approach for current and emerging issues related to health of women. And the third is on creating a research roadmap.

And I think it's important to emphasize here, we don't call it Women's Health – Terri was very particular about calling it Health of Women as opposed to Women's Health to making the distinction that we're not merely talking about, for example, reproductive health. Yes, reproductive health is part of it, absolutely. But it's more about, again, understanding the disparities with regards to, at times, studies that are performed on cardiac devices, or vascular devices, or orthopedic devices with understanding how do they perform in women versus in men?

There are differences that are going to manifest themselves. But if we do not look for those differences, and if they are not part of the design of a clinical study, and reporting out, then we won't be able to identify why it may be based upon physiologic, metabolic, endocrine – whatever the reasons, the performance may be different in one population versus another.

Nancy: Great. Thank you. Zach, did you have one more? We only have about one more minute.

Zach: Sure. Suzanne, this might be a quick one, and this is the last one I

have from the audience Q&A. Which is, the process you are using to continuously update cybersecurity guidances, do you have a plan in place for how often you would expect to update those guidances?

Dr. Schwartz: I don't have a plan in place. I think that to-date, it's been iterating as we go along based upon recognizing that there is a need to understand really where the ecosystem is, and how rapidly the ecosystem would even be able to implement changes that are articulated in guidance before you would come around with another set of guidances. But to the extent that something comes to our attention that we recognize the need for further work to be done, we would look to do that.

Zach: Well, thank you for that response. And also, Suzanne, on behalf of the audience, and Nancy, and the Alliance for a Stronger FDA, thank you for joining us today. This has been a fantastic conversation, really enlightening, and really appreciate you taking some time out of your busy schedule for us.

Dr. Schwartz: Thank you. It was great. I had a lot of fun. I appreciate you giving me the time to speak about the work that we're doing here.

Zach: Yes. Please keep it up. It's great work.

Dr. Schwartz: Thank you. And thanks to the staff at the Alliance for doing all their work to pull these together, Elisa, Phil, and Steven. Thank you.

[End of Audio]

Duration: 61 minutes