>>: Um, but want to, um, hear from the healthcare proof of concept group. Let me load this slide here. While I'm doing this, Jim, do you want to introduce yourself?

>>: Sure. I'm Jim Jacobson, chief product solution and security officer -- my co-chair, unfortunately, is not available, but he's here in spirit. So, um, want to give a little bit overview of what's been going on in the healthcare proof of concept group. Um, so, first of all, our objective, just to reiterate this for people who may not have seen it before, it's a collaborative effort between healthcare delivery organizations, which I'll use HDO from now on, and medical device manufacturers, MDM from this point forward, to employ a provisional SBoM format and exercise specific use cases for SBoM production and consumption. We've been focusing, I think primarily on the consumption of SBoM, but we also need to have use cases for the production of SBoM. So, the goal is to demonstrate successful use of SBoMs and relate to the overall cross-sector effort that's going on here today. Um, so, in a one-picture view, this is what

we're doing. So, um, right now, we're in the definition phase, but we've got a definition phase, an execution phase, and the conclusion phase. Phase has to end in tion, apparently. Didn't think that joke would work.

(Laughing.)

>>: All right, so, we're in definition phase, and definition phase, we're doing two things primarily. All other auxiliary, um, activities, but primarily, we're defining the use cases, so we have a subgroup working on defining the use cases, and that group, um, that is a subgroup within our working group, and that group is responsible to interface with the, um, use cases and state of practice, um, work group. That will be happening as the use case, our use case group gets more, um, up-to-speed. We also have, um, the data format subgroup, which, um, is identifying which format we will use, and for that purpose, we will be consulting with the, um, standards and formats group. Um, as it turns out, because of how this all fits together, the use cases is primarily oriented towards the MDM, I mean, I'm sorry, towards the HDO, the healthcare provider, and the, I have to use the words now, because I screwed it up, um, the, um, the data format is primarily

oriented towards the MDM, the device manufacturer, and that matches the real world in that the consumer, um, is more interested in the use cases, how it will be consumed, whereas the manufacturer actually has to provide it, and so the real world that we end up with is manufacturers providing data in formats that may or may not be compatible, may or may not be digestible by, um, by the providers, by the HDOs.

So, once we have those two major components defined, and again, we're not choosing a winner here in terms of format, we're not elucidating every use case, but we want to prove that we can successfully transmit information from one to the other, from the manufacturer to the provider, from the, um, MDM to the HDO, and have it convey the meaning that's intended. So, once we have that defined, we enter into the execution phase, where the participants, that is the MDMs and the HDOs, will participate in the execution of those use cases that we define. Um, there will be members of the team that function as observers or recorders, so recording the findings that we come across, um, finding where the problems are, and, um, then we have a feedback loop, so we're interested in a kind of rapid prototyping approach here, where we take finding that are blocking us from proceeding further and bring it back in and maybe do some redefinition so as to reduce those obstacles and be able to make forward progress, the end goal being the proof that we have conveyed meaning from the MDM to the HDO, and that it is used in the way that it was intended. So, after we are, have gotten to that point, hopefully successfully, but we're willing to recognize that there could be a negative case here, um, but once we get to that point, we will prepare a report for this entire group, review it with the group, make sure that everyone is on the same page there in terms of understanding our conclusions, our results, and then, um, to take that information and also bring it to other groups who are working in SBoM, um, government groups, um, industry groups, and we want to have a global, um, approach to this, so that we're talking not just to groups in the United States, but groups around the world, depending upon the quality of our findings, but hopefully, we'll have a good story to tell, and again, hopefully, a positive story, but could be negative.

So, let's look at some of the details that are defined. Um, you're going to see these come up in funny orders, but the two primary use cases that we're looking at, um, are procurement on one side, we've talked a bit about procurement already, and the other is asset management, and three sub-cases of asset management, the risk management that a hospital or healthcare provider would be conducting, the vendor management that they would be conducting, as well as the vulnerability management. Again, this is a high-level description of what we've identified so far. There's going to be significant work done to refine these results, um, to refine these use cases, and to, um, and to the specifics of what we will be executing during the proof of concept, but this is where we're starting point. So then, let's take a look at who's participating in the proof of concept so far, and by the way, this is an open proof of concept, so if there's someone who isn't on this list, feel free to volunteer to participate, but these are the organizations that are actually going to be executing the proof of concept. So, we've got, um, from an HDO standpoint, we've got New York Presbyterian, which is the organization that my co-lead is, um, affiliated with. We also have Cedars-Sinai, and there are others who are in conversation right now that we are, um, signing up, so to speak, and then from a manufacturers standpoint, we've got Abbott, Bayer, Philips, and Siemens participating, so four, um, major medical device manufacturers, but, again, in both these lists, we're open to additional participants, but these are the ones that are actually part of the working group right now, that's why they're listed. Those are the participants.

So, some constraints or conditions that we've identified so far. First of all, the data format will be machine-readable. That seems like an obvious point, but it's not necessarily a given, because up until now, when communicating SBoM information between, um, manufacturer and provider, it has not been machine-readable for the most case. Um, the data will be remotely accessible, that is we don't expect to send a USB stick or send media, that it has to be accessible over the Internet, some manner, again, that isn't defined yet, but a web service will be some API that's provided. We don't have that defined, but it's something that needs to be covered, and we will also be dealing with products from the manufacturer side that are present in the inventory of the provider, of the HDO. So, we don't, we're not trying to create made-up data at this point, we want it to be something that's within the database of the manufacturer right now, where they already have an SBoM represented internally, and they need to translate that and prove that it can be translated into a format that can be consumed. So, that's an overview of what we're doing right now. Some potential concerns that we've identified, um, so, first of all, there's, we've been talking about the interactions between the different groups today. One of the interactions, especially that we're concerned about, is interaction with the standards and formats, that we will probably be fairly well-along, maybe even having conducted the proof of concept before that group reaches its conclusions, so we want to be clear that we're not choosing a winner in this process, but it is possible that it could be perceived that way, so that's one possible thing for us to watch out.

Another one is, um, that there are some confidentiality concerns that some of the, um, participants may have, and this isn't necessarily what you might think in terms of medical device manufacturer doesn't want to expose to the world, um, all the, um, all the potential, um, vulnerabilities that are in a product, but they could be processed, or competitive process information that, for instance, a provider is using internally that they may not want to talk about. It could very well be manufacturer as well, but, um, we have to deal with that and figure out what level of confidentiality we need to assure the participants that they won't be damaged by the work that we do. Um, second, um, or the next point after that is that the, um, we need to do more work in terms of defining the roles of the participants in the proof of concept, as well as defining the roles who will, for the members of the team who will be, um, doing other tasks during the execution, for instance, the observers and the, um, recording of events, and then, finally, there was some concern expressed in the working group that we will have real customers of real manufacturers talking to each other and using information that they provide, and they want to make sure that this is truly a proof of concept, that we are going in this with open, um, with openness, but what we discover during this process should not affect real procurement processes that might be ongoing between any of those two pairs, so it would not affect procurement, would not affect any service activities that go on between the two, so that we have some level of assurance that we can go into this completely open and share information freely. Any questions?

>>: Hi. Duncan. So, not anything I could help with, but it would, looking at the fancy picture that was shown in the use cases at the beginning of the meeting, is there any possibility, besides a medical defense manufacturer, you could get some of the, I'll call it normal IT infrastructure or something involved? Because that use case they showed at the beginning sort of had the two pieces, and how the one vulnerability went both into the healthcare side and into the rest of the hospital side. Have you looked at all at that?

>>: No, we haven't. We identified pretty early on that we're just trying to exercise one slice of this, to prove the fact that this can happen in one industry, specifically one that has attracted a lot of attention lately.

>>: Um, this is not a criticism, but in some ways, I wish we only had two. I had three, um, use case columns per stakeholder, one was the procurement, which you have, one was the supply vigilance, which you have as well. The middle one is, in some ways, maybe the minor player, but, um, I'm trying to decide if there's benefit in us keeping it or just simplifying to yours, because the middle one is, um, when they go to deploy

the devices they already decided to, you know, I want to bet on your company, I'm going to deploy your devices, part of that planning and roll-out includes, um, compensating controls given the current landscape for the current exposures of the device, so is that just for, um, expedience, that you cut that middle one, or should I cut it as well, or should you add it?

>>: No, we should talk, and I think that might be something that we want to discuss with Josh.

>>: The FDA draft does talk about, you know, I mean, I know you know this, you probably read every syllable, but it does talk about equipping operational deployment and all the assumptions and network context and systems dependencies, so in some ways, it's a one-time activity, but it has a very long consequence horizon.

>>: Yeah. So, this is, again, the original list of use cases that were off the top of the head of the providers that were participating in the discussion, so we have a lot of work to do to refine this. Any other questions?

>>: And if you're listening on the phone and want to ask a question, star 1 is how you get in the queue. If you're in the room and you can find a star 1

button to press, that will also work. All right.

>>: Star 1. Didn't do anything.

(Laughing.)

>>: Okay, thank you very much.

*****

This is being provided in a rough-draft format. Communication Access Realtime Translation(CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.