20181106 NTIA-REVISITING DEFINITIONS

>>: So, I want to first of all thank all of the folks for presenting today.

(Applause.)

>>: It has been fantastic to see this much work happening, um, in relative short space of time from a government perspective. I also am going to be inspecting an increased curve of work, because a lot of that time, um, over the last months were just getting our feet under us, and it sounds like all of the working groups are pretty clear, um, focused. Jim, do you have a timeline for, um, for the proof of concept, of at least when you want it to be operational by?

>>: Yeah, our goal is to have it completed by, um, end of Q1.

>>: All right, so he's good to have it by, um, end of Q1 calendar year, um, for 2019, so that'll be after the February meeting, but you'll be able to give us an update then.

>>: Yeah, we should definitely have a lot to talk about.

>>: Um, and, so, keeping in mind that our next chance to all come together is going to be in February,

there's a lot of things to be done between now and then. Um, so, we have about 20 minutes till our scheduled lunch break, so what I thought we might do is rather than diving straight into the problems, just take a few minutes to flag what are some of the open questions, and we may go back to, um, one of the slides that the first group had, but I wanted to sort of do some brainstorming about what else you'd like to put on the table to talk about this afternoon, what do we need to explore as a group while we have this incredible brain trust, both here and watching online. Josh, you have a thought?

>>: Um, it's somewhere in between his talk and what you just said. Um, you correctly made me wait to hear from Afton until his chunk, but we haven't done that yet, so I know a little bit about the relationship between this activity and the FDA's regulatory action, but I don't think the whole room does. When do we hear that?

>>: Um, well, so, I'm going to give a very high-level discussion, and then I will let the representative from the FDA chime in, because I think one of the things we want to emphasize is this is, this effort is meant to capture the entire interest of

software community and the users of the software community, which, frankly, is the entire digital economy, one of our buzz words. A little duck should fall down from the ceiling whenever an NTIA person says digital economy. Um, but there is a lot of work ongoing. This is something that has been a priority for the national health coordinating council, as well as the FDA's medical device team, and Afton is in the room, so there are a couple things going on. One, there's an open, as Josh already talked about, there's an open call for comment. We can put a link out there. I don't want to dive too much into the weeds, but I think, Afton, if there's something you feel this community should know about what the FDA is doing in this space, um, it could be useful.

>>: Sure. Good afternoon, everyone. So, as they said, we do currently have a draft, um, revision of our pre-market guidance for medical device cyber security that is out, and as has been highlighted earlier, we did put, um, a component in there that's relevant for this group as it relates to transparency, which we call the cyber security bill of materials, because we also have some interest in understanding on the hardware components as well, recognizing that that

can also be part of the threat, and what we are very excited about, um, with this group, um, is the work that is being done as it relates to the transparency, and even if we only get, um, insight, um, into some of the challenges as it relates to software, that is still very helpful, um, for us and for industry and for our stakeholders. Um, and, so, we very much, um, appreciate the effort that is happening here, because we recognize that, um, medical devices are just one of many verticals that have, um, transparency concerns, and we very much have tried to, in our previous, um, guidances, to leverage, if you will, um, other best practices across, um, the different, you know, verticals, because we do recognize that, you know, medical devices definitely have some unique aspects, but they're also, you know, part of the traditional IOT.

>>: I think that's a fantastic point, which is there are going to be verticals, where they say we have unique needs, and what we're hoping that the use case group will cast a wide enough net to kind of flag what's common and what's unique to ICS, what's unique to regulated sectors versus un-regulated sectors, etc. Um, further comments on, I guess any last questions or anyone want to chime in on something else that is

happening else where in U.S. government? Remember, this is, one of the goals of this process is to make sure that you, as participants, can actually set the agenda on how we think about this issue of software transparency. Um, Michael Isenberg, I see that you are patiently waiting to chime in. Perhaps you have some thoughts on what we should be, what are some of the open questions we should be tackling?

>>: Um, Allan, can you hear me all right?

>>: We can. Thank you.

>>: Yeah, I wanted to, um, put stomp on something that Steve Lipner said. As you know, we have been addressing the policy level of some of these considerations and their presentation within the, um, the interagency constellation across, at least the civilian agencies of the federal government, and that, um, community's role as an influencer over, as customers, um, over the behavior of the vendor community. The discussion this morning, I think is a fantastic evidence of the, um, importance and intending convergence of the practical boots on the ground work that the working groups of your process have done and the concerns about developing guidance for the evolution of higher level policy, um, that's both

actionable by civilian agencies and consistent with shared objectives for improvement in vendor community practices and behavior change. So, again, I really just want to foot-stomp on, um, on the comment that Steve made about the importance of a strategic vision evolving and the utility, I think, of integrating that vision with the existing direction of the software supply chain assurance forum and some of the other parallel efforts that are going on in this space.

>>: Thank you. Um, and since you've talked about, and for those that don't know Michael, we just had, I think he just stepped out, one of the authors of the recent paper, Secure on Delivery, um, which is DOD-focused, but one of the things they explicitly call out in supply chain security is the importance of potential of, um, supply chain transparency for software, so it's nice to hear this being echoed around, um, and, again, underscores the importance of the work that you guys are doing.

>>: Likewise. I mean, I think the convergence is, and the, um, integrations are essential.

>>: So, I think, you know, it's been a busy morning, some of you seem to be needing a refill on your coffee, but I'm going to suggest a few potential things

that we can tackle when we return from lunch at 1:30, and you guys, what I'd like you to do is sort of chime in, either nods or just raise your hand and say that's a terrible idea and who the hell do you think you are anyway. Um, so, one of the ideas, um, can be to revisit this question of modality or granularity or sort of essentially getting to what Art and Michelle talked about this morning of what is a bill of materials, and if we can find some common ground, not necessarily thinking through the technical side, but just from an organizational and operational perspective, um, what do we want to include in this side of things. Um, so that's one approach. Um, the other aspect, which I don't think I've heard as much about, but a number of you sort of touched on, is what does the act of transparency look like. So, in some solutions, like SWID, it's fairly straight-forward, where it sort of, it ships with the binary, but that works when you are shipping a binary, so in other contexts, it may not, so what do people think about that, what are your concerns around different approaches to that.

And then the final thing, this touches on something that Omar raised, and a number of you have also touched on, which is, um, the cloud side of things, so how do we think through on prim versus off prim, and then, finally, um, if we still have some time, and I'll let you guys sort of, over lunch, think about which ones of these you want to talk through, um, all of the groups, as I understand them, have actually made some great progress in saying we want a lightweight software bill of materials, we're going to focus on, um, what the components are, but a bunch of you have said, you know, we need to still think about vulnerability data, and perhaps even as important, some way to communicate when the vendor says that we're doing okay actually, so what is, what are some of the other data planes that we may want to think about, not necessarily to address directly in sort of the crawl phase or the walk phase, but certainly, we can start planning out, as we start thinking about exploitability, um, and how the vendor can sort of make it easy, um, and sort of systematize the communication to say don't worry about this, I know this is going to trip an alarm, but we've got it covered. Um, Josh?

>>: Just the phrase that keeps coming up is how do I make an attestation that persists across stakeholders and time.

>>: As always, you frame things more succinctly

and better than I can. Thank you. So, I've sort of listed four things, we'll make sure they're on the screen afterwards. Does anyone else have some further ideas of what else you would like to make sure that we, as a community, can tackle today?

>>: Yeah, I just have a, actually a quick question. So, this is something we have in our guidance document. Are we settled on the term, SBoM? Because, I mean, I don't want to, like, really open up a huge Pandora's box, but since we're all here, it would be nice to have that discussion, because I think, you know, it has been mentioned several times in the meeting just today, certainly gets brought up on our framing calls, SBoM does not really represent, I think, clearly what we're trying to do here, and it does seem to just liven up the conversation around is this really what we, even when we had our conversation at the FDA, um, meeting back last year, two years ago, that was one of the first things that came up when our topic was SBoM, and the first thing was is this really what we want to call it. So, I can tell by the laughs in the room that, maybe, I'm --

>>: This is a great way to have the last 10 minutes and get everyone juiced up. I will say I'm a

little sad that none of you just sort of picked up and started rolling the tongue-tripping software component transparency. I think it just rolls straight off the tongue, but, no, who has thoughts on, other than you really shouldn't talk about it explicitly while you're standing in an airport? I've done this.

>>: Um, I just want to reference a document that was released, um, during World War II by the Office of Strategic Services called a Simple Sabotage Manual. If anyone's read this, it's a guide for how to, if you don't want to be part of the resistance, but you're behind enemy lines in Germany, how to sort of sabotage things from within quietly and safely, and then there's a short chapter on management, and, um, one of the items in there is anytime it looks like you're making progress, insist on a return to first principles and question the authority of the group to actually make decisions, and, so, you know, I think that there's a real concern in, that the perfect can be the enemy in the good in all this, and, so, if, it may be that SBoM is not an ideal term, it might be, but it might not be, um, but we run into real risks of hamstringing, um, our efforts, if there's not a strong case to be made for empirical and concrete reasons to get into the

litigation of terminology. I just, you know, it can be very, very, um, it can be a productivity grenade, and I think that we have to be cognizant that everybody's time here is valuable, and we're all professionals, and we need to make progress.

>>: I've got John, Josh, and then Duncan.

>>: So, I don't disagree with any of that, but I think one of the cases that we need to think about is when it comes time, and it is time, it's going to increasingly be time, to talk about this with regulators, to talk about this with policymakers, is software bill of materials going to resonate? I don't know the answer to that, but we need to think about that issue. We can use the term SBoM in this room, that's great, we all get it, it makes sense, no problem. We're ultimately not the people that really matter in all of this, right? It's going to be regulators, it's going to be policymakers, they're the ones that we have to convince ultimately. So, if we think SBoM is the term that will do it, and you can see people on the hill talking about SBoM this and SBoM that, um, then, great, it's a perfectly good term. If not, then we might need to consider what other ways can we think about talking about this will actually move the needle with the people

whose needle needs to be moved.

>>: So, I kind of hate SBoM, and, um, just a couple independent points. A BoM, or a bill of materials, is incredibly well-defined, well-rigored, understood by executives in board members and adjacent industries who are increasingly becoming software, so there's a ton of potentially positive patterns to be gleamed from adherence to the BoM, whether it's SBoM, SWBoM, whatever. Number two, I couldn't stand it when an executive branch person called this SBoM and made jokes and songs about it, but also, the Congress folks that have been attracted to this are also using SBoM and have been, despite repeated attempts to get them to not do so. Um, and number three, I think a lot of the people close to the pioneering of this and the capture of state and practice kind of don't care that we call it, just what we do it, which I keep going back to, like, that simple definition of ingredients and the use cases surrounding that, so we could have a word cloud of, like, adjacent words, but I think redefining it may set us back or slow us down, to your espionage point.

>>: So, I support the not renaming it. You can call it SBoM, if the reason is you're worried about

saying the word bomb, but as Josh said, BoM is a very established acronym, bill of materials, in the supply chain. I don't think we should redefine logistics terms, if we can avoid it. If you don't want to call it software in front of it, you want to call it something else, fine, but bill of materials, I think is, unless I missed the point being made, bill of materials is what we're trying to make. Is the point we're not trying to make bill of materials, or is the point people don't like BoM as an acronym?

>>: So, I'm going to step in here and say does anyone have an alternative in mind? Does anyone have something that they're very excited about, ideally, something that makes a clever, but really corny acronym? Okay, continue, but if we don't have an alternative --

>>: We actually had a number of them when we had this conversation with FDA. That was our topic, um, and just to be clear, I'm not opening this discussion point to make a big stink or try to set us back, it's an actual thing that we have on our agenda that we need to get resolved, and the more people we have here, and if that's the case, that we are going to keep that, that's fine, it's just we have to, in order to move on,

we just need to be able to close it. So, um, and I'm not hearing any objections, unless there are some objections, just a topic.

>>: Mm-hmm.

>>: Okay, at the risk of stepping on Michelle's attempt to close the topic --

(Laughing.)

>>: I just wanted to say as a former product design, when you say bill of materials, something pops up in my head, I see a very, very clear picture, it's an Excel spreadsheet in my domain, and it's got a hierarchical format, and it's got stuff in it, and I know exactly what you're talking about. When you say software bill of materials, after participating in the files and formats thing, I have a picture in my head that is almost the same, it's really, really, really similar, it's XML, it may be something else, but, I mean, it's a really similar thing. If you say bill of materials to someone who doesn't know what we're talking about, I think it's a very short path to convincing them that they do understand what you're talking about, it's just a little different.

>>: Okay. So, um, with that, unless someone comes back from their lunch break with a great idea of

what we could frame this as, I am hearing that we are going to stay with this issue, and again, these matters are always open, if someone comes forward in a few months and said I just came up with the most brilliant label, and it will win friends and influence people all over the world, then we'll re-open this, but for now, I'm not hearing strong objections. I'm going to check on the phone. Michael, I see you waiting in the queue, but I think alas, we have some hungry people in this room, so we will pick this up at 1:30 p.m. eastern time.

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.