NTIA-UNDERSTANDING THE PROBLEM

>>: We'll now dive in to hear what some of this hard work has been, and so the first working group that we're going to hear from today is the understanding the problem group, and they're going to give a presentation, and I think they're going to be looking for lots of feedback from you.

>>: One more moment for technology. Yay. Sorry. This is on, in this case? Red button? Okay. Hi. Sorry for the, um, sure, sorry for the technology fiasco there. Yes, so, um, Michelle Jump and I are the co-chairs of the understanding the problem, or as I refer to it, the framing working group, so, yep. Any opening comments, Michelle?

>>: Oh, so, we're going to kind of split this introduction session, um, and Art's going to talk, thank you. I'm not usually, um, I can usually be heard. Sorry. Um, so, Art's going to go through kind of some bigger concept issues, but we're also going to go through one of the attachments that you received from Allan, which is called the guidance document, and the intention of that document is to really kind of write

down what we're, the scope of our effort, as you may recall from our first meeting here, um, this group was stood up to make sure that we have a good idea, we're all in line, even though we have different task groups that we're working on, different projects, making sure that we have a good understanding of the objectives, um, and the direction and the deliverables and the scope of the work we're doing. So, we have a document here that we're going to go through in just a few minutes, but first, I'm going to turn it over to Art.

>>: Um, thanks, Michelle. So, just to add slightly to that, um, I think I've joined at least one of each working group's call, and I know we've got a lot of people that are crossing the working groups, but some of the stuff that's on our slides here is, um, themes that have occurred across working groups and across the entire, um, larger process. So, we're, we are slowly, um, congealing is the wrong word, but trying to get our working group framed, coalescing, annealing was the one, right --

(Laughing.)

>>: Annealing atoms or particles into, um, some common themes that keep coming up, some questions that keep coming up, that without answers to, we're not going

to probably going to be able to move very far forward on, and we're not trying to claim, you know, we are not the executive of, we're not the executive committee of the working group, but, um, we are looking at, um, can the framing working group collect some of these things, present to the larger group, and then, you know, keep yelling until we get some answers or some, um, some decisions on some things. So, we're trying to position ourselves roughly in that area, but, again, multi-stakeholder process, fairly open, so these are, primarily on these slides are things that have come up over the course of three months or so worth of almost weekly meetings.

So, let me get into them. So, this is a rough, um, table of contents. Um, I've heard the word use case used by everyone, in some conversations in the last couple weeks. We believe that what the framing group is calling use case is not really a use case, it's a higher altitude concept, so, um, very open to ideas on what to call the thing we're talking about. That bullet has some of the words we've come up with there. An activity, is it a functional area. Epic is out. Epic means something to software developers, it's not an epic. A story, an intent. Um, we canceled intended

use this morning, because that has special meaning as well. Um, objective, little bit too much like a goal to me. Functional objective is one of the leading contenders at the moment, but something that is, what I will call the high-level or generic use case, it's not the detail of a proper software development use case, but, and it's not sector-specific, for example, it's not healthcare or automotive or traditional IT-specific, but we believe that the, um, our work here needs to support or improve things like, um, vulnerability management, um, acquisition and procurement processes, also possibly with an eye towards product security, um, basic asset management, um, license management is already in place, it's working in a lot of places, but I would suspect that an improved SBoM would help with that. Um, basic supply chain hygiene, I have, you know, 50 suppliers with different parts, and I can cut that down to 15, and I just have less complex software, less complex things to have to deal with.

Um, I don't want to do a whole lot of interaction at this point, so we can get through our material, but if folks, so, actually want input on what do we call this high-level, high altitude use case, and please

keep an eye on these high-level use cases, are there things that are missing or things people believe do not belong there. We can answer this later in our later session, but, um, we actually, this is our proposal, and we'd like to feedback to kind of correct here. Um, sort of related, we're trying, we're talking about sort of scope. Um, for the most part, the things listed here are, in some respects, out of scope, we believe. We're trying to focus on what an actual minimum thing looks like, you know, so, the actual SBoM thing itself, um, might need to include how it's shared, or might not, but it needs to sort of consider that. Um, relationships between parts of the SBoM, licensed management is something that it might support, but doesn't have to be built into it necessarily. Um, back to the vulnerability management high-level use case, um, a list of vulnerabilities and how to master them may not have to be part of the SBoM inherently, but we need to keep that in mind, if that's an agreed upon use case. Um, providence is generally out of scope, although it could be supported. We're not trying to prove where the software came from. There is some question about proving that the bill of materials is correct for a digital signature, perhaps. Um,

hardware being included is a, has come up recently, if folks are familiar with the cyber bill of materials from FDA, I think they're trying to cover hardware in there, and we've got a little slide about what's hardware, what's software. Um, we probably need to define some things. The one stand-out term we had trouble with was component. We've got a crack at it here.

Please take a look, I'm not going to entirely read it, but it's some sort of unit of software and how you want to define that. If we're going to talk about relationships between components, we have to define sort of the level of the thing we are talking about. Very tightly tied to the question of granularity that we're going to get to in a minute. Some of the major open questions we're looking at, what does a really minimum viable SBoM solution look like? Really must have what you have to have in it for it to be functional at all, and lots of optional things, possibly, as well. I'm stealing a Josh Corman-ism here, minimum must have, in order to crawl, for those who can do more than crawl, can you have optional things that help you do what you can already do? Um, this granularity and detail question, I've got a slide on in a minute, um, a big discussion in our working group is about the SBoM being

self, sort of self-contained and flat, or do I have relationships and hierarchy and references to other things I have to pull in to produce my SBoM. Um, we were about 50/50 split on our last call, I think. Hardware question again and the line between hardware and software, um, we had a, again, I always provide a recent security example of the line between hardware and software, there was something last week with, um, Bluetooth system on a chip, and it was hard to tell where the line was.

Um, granularity, so, there's a couple of dimensions here that we're looking at. Sort of the size of the unit of software, um, the top of that column, integrated system, I would consider something that's, you know, multiple operating systems, a couple of units IRAC, a whole system that someone's installing for you. Down at the bottom, this sort of line of code, um, personally, somewhere around file or library, I think is where the right sort of line is, but, um, open question here. Um, there's also sort of how you change or install the software. Way down at the bottom is I need to create a new chip, you know, physically burned in Silicon, which is a possible thing. Up at the top is I can edit an existing file, and I get my changes

to my liking. Um, there's a lot of options here. You know, somewhere around firmware and microcode is the hardware/software boundary a lot of people think about. Um, unanswered, my personal opinion is about where it is on the size of the software unit, but open question. Um, again, this minimum viable product, a very, very beginning light proposal is do those, does that triple a vendor product and version good enough? Is it better than nothing? Is it functional right off the bat? Even if the person producing it is allowed to pick whatever they want for those three fields. In my dream world, it's a standard format, and there's some naming, um, some tricks for the naming to make it not, um, not collide, but this might be a functional start.

Um, we talked earlier about what's in and out of scope. A way to share this information is that inherently part of the SBoM, is it something separate, just include a file with the thing, with the, with this string in it. External references embedded in the component somehow, and again, question to the larger group here that we've identified on the framing group, what is in this minimum viable product? What's missing from an absolute minimum thing? Very complicated world we're in, we have existing standards that are

already out there with lots of stuff and lots of fields in them, what's the really core minimum thing that'll get us anywhere? Um, we've tried to work on mission statements, well, I'll say mission words. For the framing group, we're trying to sort of identify, um, things like scope and these high-level use cases, functional areas, objective goals. Sorry, what did we call them? Fundamental objectives. Thank you. Um, big questions, preliminary answers, trying to identify those, bring them to the group, which we are actually doing right now, and try to see if we can get some decisions on some of these things, or consensus. We're not claiming to decide on anyone's behalf, but there are probably some of the big questions that if we don't answer them, or just agree enough to move forward, that it's probably going to block progress is our concern. So, instead of being executive, we might be annoying and keep asking did we decide on X yet, did we decide on X yet, we talked about it again, did we decide on X yet, so we can kind of move on.

Um, in the draft paper Michelle mentioned, we have, um, I think she quoted from the NTIA website, a mission for the overall process. I'm not sure if other working groups care about mission or mission

statements, but we'd happily sort of think about those, if that would be helpful. Um, user results of all of this to help guide, you know, things forward. In our working group, there's a guidance document Michelle mentioned, um, we have a sort of preliminary notion of guidance for an SBoM user, but that can't happen until we figure out what the SBoM is and some other things. Um, that seems to be the last slide. So, yeah, in terms of the document, I think I can actually --

>>: While Art pulls up the document so we can go over that, are there any questions about what Art went over just now? This is a read-out. Yes?

>>: Hi. So, I'm new, this is my first meeting, so I'm catching up some, so I apologize if it slows you down, but is there anything in, is this the right point to ask what the process of getting to the answer is? So, you had a meeting, this is another meeting, there was working groups that met in the middle, you have a document, what happens with it, and how does it become real? Is there, would it be helpful to at least cover the big picture a teeny bit? Thanks.

>>: Thank you. That is, I really appreciate it, that's a great question. Excuse me while I jump in here to talk about the big process, because, um, on

one hand, there is a general way that it happens, which is we identify issues, um, groups are formed with particularly interested parties, they produce drafts, they bring them to this broader community, we circulate them, criticize, input, suggest, and through that iterative process, we smooth the edges and find something that most of us agree on. This is a consensus-based process. That's a little bit tricky, to define exactly what that means. How we think about it NTIA is that no one person should be able to derail something that has support from a very broad case. On the other hand, the majority should not be able to overwhelm a core group of stakeholders, even if they all come from the same perspective. So, that's roughly how we try to define the way consensus works. Essentially, it is an exercise in exhaustion. We work on something until all of us are like, yes, this is obvious, and we're already doing half of it by now, so let's move on.

How that works in practice for each group is going to be a little nuanced, it's going to be a function of the work that we're doing, what makes the proof of concept from the healthcare group quite different from this high-level discussion, and that's different from

the technical question about standards and formats. So, each group is going to produce a document or tool or whatever that meets their needs, but they're always going to be checking in regularly with the broader community. This is also a chance to remind the folks who are watching and listening on the phone that you can get in the Q & A queue by hitting star 1 on your handset, or just shouting really loud. We'll see which one works.

>>: Allan, we're trying to pull up the actual guidance document on this computer.

>>: It's almost like there's a lot of traffic right now going through NTIA. Is that not working?

>>: It is now. It was just super slow to load.

>>: Does everyone have a copy in front of them? I can bring them and pass them out.

>>: Okay. Sorry, guys. There we go. All right, so we're not going to go through every line item, um, on this document. Basically, what I'd like to do is to just walk folks through the content of the document, and then what Art and I talked about doing is we felt that as the framing group, we probably shouldn't be the only ones taking a look at helping to develop this. We drafted this initial document, um,

but we'll be sending out, um, a request for anyone who would like to engage in a specific meeting, um, a WebEx, to talk about the content, get some feedback, um, and we'll be sorting that out through Allan, and then he can distribute that to the group, so we can get anyone who's interested in fine-tuning the mission, scope, goals, or any of these aspects of the document, we'd like to welcome you to a specific meeting just for that, because we won't have time to do all that today, um, but I'd like to just point you to the red text in the beginning. Always a good place to start, meaning that I would like to draw your attention to this part of the document, which is basically saying we're offering this up as a draft, to try to get the conversation going and to help kind of coordinate and collaborate across the different working groups, this isn't intended, as Art said, we're not trying to be an executive committee here, what we're trying to do is just write it down so we can start to have the conversations that we need to have to help move that forward, per our question just a few minutes ago. Um, the mission statement here, um, and I didn't ask Allan for permission to put this in here, but I did my best to pull, um, what sounded kind of mission statement-y, I know it's a little long for

a mission statement, as it came up in our meeting on Friday that we didn't have quite the mission statement down here yet, so I pulled some relevant language from the NTIA software transparency website, but we'll be working to kind of hone this down, make it a little bit more precise, make it sound a little bit more of a mission statement. This is a placeholder as we stand now.

As for scope, um, we have a fairly straight-forward scope around, um, defining and, um, and looking at the uses of SBoMs, how it can be used to foster better security decisions, including a note there that all industries will be included. I don't know if there's any kind of restriction on that, I don't think so, Allan, I think we're basically saying all industries are welcome as part of this process, and that's another point here in this scope. The other part here that says related dependencies and supporting activities, um, I'll just share, used to say out of scope, but we didn't want it to say out of scope, because, really, we need these pieces, but we aren't necessarily putting that in our queue for the work being done here. There's some related needs that need to occur around mapping vulnerabilities back to

components, around, um, documenting relationship between components on any given SBoM, etc., but that's not what we have in our queue right now for this first round on this initiative. So, um, all of these items here are up for conversation, and that's the reason that we put them here, is this is our understanding, but it may not be the overall group's understanding, so we're putting it up here really to start some conversations with folks, and we're hoping that we can have those conversations on a dedicated WebEx or two, and we'll bring it back to the larger group at that point. Um, this next section, let's see if this will work on this computer. No, it doesn't want to.

Um, the next section is a longer section, which includes goals. This is a long list of goals, um, for this initiative, the larger initiative overall that we're looking at, and, really, um, we've just taken what we've, from our conversations with other group leaders, um, conversations we've had within our own group for the last couple of months on our weekly meetings, and we've started collecting what we feel are the high-level goals, and you'll see they're categorized here, um, there's some goals around terminologies and definition, um, around defining SBoMs, um, sorry for

the scrolling, but sharing SBoMs, using SBoMs. We're just kind of trying to put these goals into categories, because I'm sure that there is some work that can be done around how these goals are stated. We may want to remove some of these goals, we may want to add to some of these goals. So, um, all I'm doing is pointing out to you we have some categories, we may even have another category, um, this was just our first stab, again, to start the conversation, because I think these kinds of conversations are very important for us getting to the end goal, right? Um, the big open questions really just points back to, um, Art's slides, he's been working on those, kind of also thinking about our meetings that we've had over the last few months, um, and we'll be adding those here. Um, and then some initial deliverables are listed here. We haven't done as much work on this, this was really just kind of a train of thought, I started listing some things that I felt that we were probably going to try to deliver, and we have asked each group to provide a list of deliverables from each group today here, and we'll be collecting those, again, trying to pull, we're really trying to be the glue to kind of pull everything together, so people can look at it in one shot.

So, I took a stab, and Art and I didn't quite get to connect on this, so there might be some additions actually from Art as well, but our first deliverable, I don't know, Art, if you had any changes to that, but, um, I had listed that this guidance document, tried to get this mature, get some feedback from the overall group, um, initial list of these functional, um, objectives, meta use cases kinds of things that we've been working on, and then initial structure of the SBoM, and so you saw, you know, it's interesting, because Art and I kind of were working on this in parallel over the weekend to try to get the information, um, back, and it was interesting, because we both kind of coalesced on very similar things here in our documents. I guess that's a good sign, right?

>>: I think we just switched the columns.

>>: Yeah. So, this actually came from our notes, we have a Google Doc that is running notes, and we wanted to just put this out there as a baseline crawl level SBoM of what is a base minimum. So, we wanted to put it out there, because we really want to start talking about this, and, so, right now, this is, um, I don't, I think , Art, maybe you filled this in as an example, didn't you? Somebody in our Google Doc filled

it out as an example, I actually don't know, we could probably find out, um, but I pulled this out from our discussions, someone actually filled out some examples of what the content might look like. I didn't make any judgment either way, I just copied it and put it in here, so, again, for discussion.

>>: And all apologies to the, there's a working group on standards and formats who's probably laughing at our three or four columns, but again, we're trying to get the core minimum conceptual thing down. We fully recognize there's a whole working group that knows a lot more about the details of the fields and things.

>>: Yes. Absolutely. It just has come up so many times that, um, we figured we would start to draft that, and then as we can continue talking with our standards and format, um, colleagues, then, um, hopefully start to coalesce around something that works. Um, there's space here for phased deliverables. We have talked about, we're currently in phase I, we expect that there are going to be some things that come in, um, I guess, probably similar to the crawl, walk, and run. We are in the crawl stage right now, but as we start to get those pieces

solidified, there's probably going to be further, um, objectives and, um, deliverables that we're going to identify. This is a space-holder for those. So, um, are there any questions around this document? The purpose of this document, I don't know if we want to necessarily get into talking about the details of that, but are there any questions around why we're doing this, what we're doing, and, um, what's the purpose of this overall document? Yes?

>>: Hi again. Um, if it's a detail, then defer it to the other meeting and make sure I get invited to the other meeting, but I realize this is a Department of Commerce meeting, so it's industry-focused, but an awful lot of the underlying desire of this is associated with the open source community, so I presume this does not just apply to manufacturers and products, that it will make, we'll make use of it in government-developed software and in open-source software as well? I hate to be semantically pedantic, but it's very vendor/manufacturer designed, it seemed like at the moment, so I just want to make sure those two other communities don't get left out and are within scope, correct?

>>: Um, yeah. So, certainly, the whole open

source part is the part I'm very much caring about and trying to make sure that we get that in the discussion effectively. The last line there, you see open SSL, open SSL, that's a way of potentially representing some things, but I think that's an area we can refine.

>>: Yeah, I don't know if we're diving into the red lining of this, so I'll assume no.

>>: I'm going to suggest very briefly we focus on the process now, and we pick up some of the big questions that Art raised and the document raised after we've heard from the other groups.

>>: So, somewhere short of red lining, just to short stomp that, I think when you see our use cases thing, a lot of them are developers of software and consumers of software in a chain, so it's really less about a commercial relationship, more about communication up and down the stream.

>>: If you're using software, you can use, you're in.

>>: Right.

>>: Whatever form, open, closed.

>>: And that's why we're trying to get a diversity of opinion as well, is we're presenting this as a starting point, if it doesn't work for all of the

areas that we're looking at, we'd like to make sure that it does. So, um, if it comes off as somewhat manufacturer-centric, a lot of us came from that space, so we're just really looking for great feedback around how we can make it usable for everyone. So, any other questions on the phone or before we move on? Because I think this is the last thing we had to talk about, is our update. Yes?

>>: Mike Bergman with CTA, Consumer Technology Association. Um, I assume part of your process would be, could you scroll up just two lines to the headers? There we go. Um, to define how something called a major version is created, scoped, and updated, and what triggers a major version update, what triggers a minor version update, or not what triggers those, but, I mean, part of the process has to be define these things well enough so that two different people putting them in will put in the same equivalent kind of information.

>>: Right. Yeah, that's a great question, and it's actually listed on one of the deliverables that we have, to be able to better define that, when the updates are happening and how we're using these words, and, um, I think the standards, um, group will also be leveraging, um, what the standards say, how we write

some of these things as well. Would that be correct?

>>: It's an area that, yes, it needs refinement, because there are different stories out there and different definitions, depending on the communities, and it needs work.

>>: And we do have that flagged, so that has come up in our discussions as well, so, yes.

>>: In the room, and then after that, we have someone on the phone.

>>: John Willis with Turn Around Security. This is my first meeting as well, so just a big picture question. What is the intent as to who is going to use the, um, output of this? Is it going to be industry voluntarily accepting it? Government mandate, etc.? And, I guess a follow-on to that would be is part of the phased approach, um, making sure that we include all the right stakeholders?

>>: Do you want to answer that, Allan?

>>: So, I will jump in and say that NTIA processes are entirely voluntary. It was, in this particular case, we are aware that a number of government organizations are very interested in thinking through software bill of materials We wanted to make sure that what a software bill of materials was

and how it came about was something that had input from as many stakeholders as possible, and, so, what happens with these guidance documents afterwards is going to be a very particular, unique function for whichever community picks them up, but as they are written, they're certainly not meant to, in any way, they are meant to be voluntary guidance to help people have this process. I should note that software vendors and and producers and open source community, we also have lots of consumers of software, and so it is our hope that they play a very active role, not just in helping to decide what this stuff is and looks like, but ultimately making sure it's used. Does that help answer your question?

>>: Is there another phase that'll make sure that we have all the right stakeholders? Because I know one of the steps was to identify --

>>: It's a great question. This is an ongoing discussion. We work very hard to make sure that we have the stakeholders that we know about, and we've beaten the bushes for the past few months. A lot of it comes from folks like you, saying you know who's not in the room is blank, we need to get this community in here, and we can talk during one of the breaks about, um, how

I can help with that.

>>: Or you can shout it out, and I'll make a note.

>>: Right, and we do actually have a place in the guidance document that's going to be very specific around not only the industry, the industries that we have involved, but also specific stakeholders within those industries, so, um, we haven't quite filled that out completely, but I think that'll also be part of the living document part of this as we move forward. Certainly welcome additional input.

>>: The use case group is probably going to speak to this as well, and hopefully can shout out during that. I want to make sure that we, um, hear from Steve Lipner, so, Melissa, if you can open his line.

>>: Hi. Can you hear me, Allan?

>>: We can.

>>: Okay, thank you. Um, so, I, um, I apologize, because I haven't really been engaged in the process since the last call over the summer. Got the, um, got the materials, um, for this meeting last night. Um, it may be that this will come out, um, in subsequent, um, subsequent sessions, but, um, but the material that, um, that has been presented just now by, um, by

Art and Michelle, I believe that's right, um, seems to be more focused on attributes, um, attributes and characteristics of a software bill of materials, you know, the mission, the scope is about what a software bill of materials is, the goals are about sort of creation and attributes of a software bill of materials, and I would kind of expect, um, the exercise to start out with why we need a software bill of materials and what it's going to be used for. Is that going to be covered in a later session, or is that assumed, or did I miss the memo?

>>: I think you'll be hearing from that in the use cases group. Um, this is a little bit higher level, but the use cases group has definitely been working on that diligently.

>>: It's really not higher level. I mean, it's, um, you know, it's low level, but it's low level with implementation on the assumption that we're solving a problem that we haven't defined, I think.

>>: Sure. Sure. Understood, but I think, um, I think you'll hear quite a bit of discussion around, um, why the software bill of materials, um, would be considered useful from the use cases group. Would you agree with that, Josh? You'll be talking about that

a bit?

>>: Yeah, I think, ideally, we would have presented all of the sub-working groups to each other. Just before this, we did harmonize some language, but I think part of getting in-person today will be more harmonized by the end of the day than by the beginning, and if people are patient with that, light will dawn gradually over the hole.

>>: And to your point, um, all four working groups have flagged this as an important notion, that how is this data going to be used, and then working backwards, and, so, I think you're dead-on, that this is a priority that I think everyone involved has tried to say, yes, let's try to get as much awareness, information, and data collected as possible. So, keep pushing on that as the day goes on.

>>: Okay, thanks, Allan.

>>: Thank you.

>>: Can I just take a minute?

>>: Of course.

>>: So, we'll wrap-up our section here, try to stay on time. Again, the drafts guidance document here and the bullets and the slides, again, emerging role of the framing group, we're trying to identify, and have

in some cases identified big questions, um, questions of scope, questions of we need to figure things out before we can move forward, open issues, we're trying to bring those up to the larger group, and we're basically, you know, doing the best we can to come up with what those are and present them. If we hear nothing back, do we assume those are the right things? That's not very safe to do. So, um, if you have feedback on any of the stuff you've seen here on this document, particularly on the big open questions sorts of things, please let us know. We are representing the larger group, we need the larger group's input, or else we're off in our corner, making stuff up, which is not a good way to work.

>>: So, apologize, but again, a process issue, how do we do that? I know your name's Michelle, I don't know your last names, I don't know --

>>: We can get you all the materials. There are periodic, um, WebEx and phone calls and some mailing lists, and I guess Allan will hook you up with all the information.

>>: Okay, thank you.

>>: And, no, thank you for flagging that, and for anyone who is new to this process or wants to

re-engage, um, if it's not information that you have at your fingertips, please reach out, we will tell you all about the working groups, how you can join each one. Um, most of the working groups, they don't overwhelm your inbox, so even if you only anticipate, um, you know, following the e-mails, but not joining every call over the week, still, I think, useful to sort of stay engaged as much as you can.

>>: And the meeting, or the invitation to have the larger discussion around this draft guidance document, um, that will include our contact and how to arrange to join that special meeting.

>>: So, and the final thing I'll say on this work is great job. It's really helpful, to have someone keep the bigger picture in mind, and I think what we're going to do is after we've heard from the working groups, one of the things we're going to tackle is the big open questions that you guys addressed, and we may not answer them all today, but we can at least drill down a little bit about how we want to.

>>: Thank you.