>> Thank you to everyone who came back from lunch, as we know that folks are going to trickle in. What we're going to be doing this afternoon is diving into some of the questions that we identified this morning. And we'll spend a moment just sort of trying to make -- walk through them.

And then the other thing we're going to do is we're going to talk a little bit about the process and we're going to dive in deep of not just scheduling, but how we see this going.

And some folks sort of framed this before the meeting -- before the lunch break of saying well, let's really have a punctuation of phase one with the minimum viable, set things up for more ambitious stuff down the road. But really say hey, listen, we're here, we've done this work, this needs to get out there. So let's figure out how we can make this get out there today.

So, we have four questions. And I want to thank Megan Dosher, who is my colleague at NTIA, who handles a lot of our national security cyber security work. She has been doing this for awhile and also is the person who makes a lot of these meetings continue to run while I'm up here jabbering. So thank you.

So, we've got four things here that I think will be useful to talk about. Although I'm going to shift the order, we're going to start with opacity and namespace. And then we're going to tackle transparency and tooling.

So, I'm going to sort of try to frame these and see if there's any feedback on how we're thinking about these problems.

The idea of opacity is there are no -- we want to make sure that we have the unknowns are known. So if we think of our tree, our dependency tree, can we be explicit about the difference between a leaf, this isn't using a new code, versus this is potentially the top of a dark branch and we don't know anything about it.

I feel that that data is going to be very useful to have as part of this discussion. So that is the opacity question, or opaqueness, we can talk about that.

Namespace is the complement to the challenge of uniqueness, right? We are worried, hey, are we sure that this software is this software. So uniqueness is making sure that only one thing has a name. But the problem is we've got overload rather than collision. So we have too many names for a single feature. And so there are some things out there, I don't think we're going to solve it completely, but I think there is some things that we can build into our documents and our thinking now so that it's not quite as big a problem as we all think it is. Because this is often something that is flagged when I talk to people about this.

Transparency is something that Art talked about. This is how we, NTIA, framed this initiative to start with, being transparent around the software components, but what does the act of transparency look like and how do we share it.

And I think there is -- we can talk about whether it makes sense to draw a distinction between sharing data further up in the build chain or in the supply chain versus that final piece of transparency of getting the data into the hands of the owner-operator is a term we heard earlier, the person who is going to be using it for a slightly different set of uses.

And then, finally, something that has come up across the board is tooling. From the beginning, almost all of you have emphasized this has to be automated, this isn't something we're going to do by hand. Looking into sketching out where. When we say

tooling, what do we mean? And let's really do a mapping of that space figuring out what we can do today and where do we need to spend a lot more time and attention on work.

So we're going to now we have a few minutes of agenda whacking. Is there another question that you guys desperately want to have on this agenda?

>> How do you define success on if we did everything that we wanted on one of these topics, what would we come out of this with?

>> It's a great question. Because I think some of these there will not be a concrete solution. What I would like us to do is make sure that we can make some progress and hopefully find things that for our deliverables we can now dig our teeth into.

>> Can I suggest that we identify the group that's responsible for getting to conclusion on that point?

>> That's a great idea, thank you.

We will, again, for groups there's always a little bit of a challenge, but I think having a point on it is going to be very useful. Josh?

>> Before the break we talked about can we carve off a phase one.

>> Yes. So after we have this discussion on the substance, then we're going to take a step back and talk a little bit about phase -- about what the phasing looks like.

None of that is to say that that's not an idea that we should bring into this discussion of say, hey, by the way, this is an important topic, we should address it, but that is a more complex than what we'll be able to solve over the next few months. So I want -- please keep that idea in mind. Is that fair?

We are definitely going to be talking about the importance of phase one. And then finally, just for those who are watching the webcast, this is where we really want your voice and your input.

And, again, I mentioned that we have a challenge which is there's a little bit of a delay. So it may be in your interest to -- this is now where you can get on phone line. And you will be able to raise your hand. For those who are already on the phone line, thank you.

You hit star one to get in my queue and then we can bring your insight into the discussion. If you are following along the webcast, it's just going to be a little bit further behind. So it's hard to do that. We apologize for that. Thank you for your flexibility and for all of the time you've given to us.

All right. So, we have this challenge of the known unknowns. And to put Art on the spot just a little bit, is there -- can you give us some idea about how your group has thought about this so far?

>> Let me take a crack at that. I'm going to start by just trying to more or less restate my version of what you just said.

So, I'm a supplier, and I create SBOMs for the things that my developers type with their fingers on their keyboards. Straightforward, right?

The things we include, one up the supply chain, I grab SBOMs when they're provided to me. That works. When there is not an SBOM provided but I know that I'm using component X, I can say I use component X, and I might be making up the ID and not that supplier.

But then the question becomes do I think there are more things in component X that I run SCA tools on them, do I know because I know this field very well, do I know or

have confidence there are more things in there, or do I know nothing? Or am I willing to make a claim further back than that?

So as far as I have thought about is some sort of mechanism. It might just be a field or a way to say I have got some variable level of confidence in what I'm about to say, but I'm pretty sure this is in here. I'm slightly sure this is in here. I have no knowledge, you know. We want to capture that assertion somehow and/or the confidence in it. Hopefully there is a technique to do that somebody already knows. But that is what I think it needs to do.

>> That is a good point. This is going beyond just the hey, there's stuff here, but actually saying I may know something about that stuff. So this is translucency to really twist the metaphor. Josh?

>> Yeah, I think originally we thought it was a huge win just to say it's a known unknown and call it opaque or blind spot. So a binary.

I think in the last couple of weeks we've noticed you could have, you know, a gradient of competence which could be a softer composition analysis tool thinks it's this version, you know.

But a finite number of values but to the strength of your claim or your confidence. And in a free market, people could take or leave different levels of that. And instead of making this a regulatory claim for like the FDA guy that was sitting here, I'm thinking the banks that already spoke at these things, they could say we'll tolerate no more than 10% blind spots or no more than -- we need a guess, you know. That could be borne out by the market demand, right?

>> I do think one thing we have to get into at some point that I don't think anybody said today related particularly to the SOUP, and that is in the field of Open Source when you're using the other person's source versus when you're using the other person's executable.

In the example Art said when I go get this thing, if the thing is the executable, then yes, an SBOM should come with it. And if an SBOM doesn't come with it, then we have to guess. And we were all in this discussion of how we're guessing whatever it is we're going to put out.

But I think in the case where you get the Open Source and you compile it yourself, that's no longer the Open Source person's supplier, you are now doing the compilation, you make the SBOM when you compile it would at least be -- I would not consider that SOUP. I would consider that known, at least to that level and then maybe it calls out and then that becomes SOUP.

But I think we're not distinguishing between the two and sometimes -- at least in all other discussions we've had, there has been confusion. I think we at least have to make clear what it is we're talking about being opaque.

>> Good point. I want to go to Dave, but I also want to make sure that we're all in agreement with the statement if it's Open Source source code, then it should be easy to figure out down all the way down to the -- you know, all of the turtles if everything is open.

>> If you compile it.

>> If you compile it.

>> So I understand the distinctness that you are making, Duncan.

But if you're -- if you're the -- if you take -- if you take source code for a third-party component and compile it yourself and then you redistribute that and another party uses that, you are not that much different actually than any other third-party to that new party that is using the software. And so --

>> With respect to opaqueness, I disagree.

>> And so confidence isn't necessarily transitive in those kinds of cases.

>> And this is where we're getting to some of the nuance around confidence versus lack of knowledge.

>> Right.

>> And I want to keep that theme running. Bruce?

>> One of the things you have to think about is JavaScript. And that is a whole different model than we've been talking about here.

But when you do JavaScript, it picks and chooses and all that as it's going from all over the place. You could be accessing a thousand files just to get one function.

You know, they need to build some tooling in that if you are going to do something along those lines. And it's not a question of compiling or not really.

>> I don't disagree. So it's a big problem. There's a lot of pieces to it.

In that really fancy chart that when Art put it up there, he said it's too complicated for everyone. The reality is eventually we have to deal with that whole chart.

That's one of the cases that is beyond the green box but does have to be handled. I don't disagree we have to handle it. But to Josh's point earlier of hey, let's do things we can do first. At least if you are within the green box, let's do a simpler case of hey, you're within the green box, it is in code that is executing on something you're selling, and it is code that you either wrote yourself, got from Open Source, or got an executable from Open Source. We can at least make that a fairly simple case and then we just decide on each of these cases, what do we do?

>> Does everyone like that breakdown? Do you have a quick note on that?

I want to let Duncan continue. I just want to make sure that we like that breakdown.

>> Yeah, except that there was a different suggestion -- and I can't remember who made it -- that I think it's SPDX lets you know that one of the linkages is, you know, compiled from. Right?

So there is an explicit relationship, I compiled from that source, you know, I'm going to share most of the same vulnerabilities as that source. Maybe not all, but most of it. I'm going to be mostly similar.

I don't think that's -- we never had that in the opaqueness category, but I can see why you're bringing it up there. But I thought we had a different way to handle derived from source.

>> So if we like -- I want to get -- Dave, go ahead and chime in here.

>> I just wanted to provide some context from a SWID tag perspective as far as how we are addressing this problem.

So there's really two ways that we deal with this opacity problem. There's this notion of authoritative versus non-authoritative tags. So the idea is if the person creating the tag is the same person that had some role in either creating or distributing that software, which sort of takes into consideration what Duncan has been saying, then that's considered an authoritative tag.

Then if there's a mismatch there, then if there are multiple parties that are involved in both creating the tag and distributing the software, then that is considered a non-authoritative tag. So that's the first way.

The second way that we deal with the sort of opacity problem is as it relates to the manifest of the software itself. And in that case, there is two types of manifests that you can provide. The first is a payload which is an authoritative manifest of the software. So the intent there is that the software components that are referenced in the manifest are -- the information is being provided by the software creator. And then the other one is evidence, which is more of a forensic type of capture of information.

So if you have a third-party discovery tool that is analyzing some installed software, it can produce evidence in the form of a SWID tag, a non-authoritative SWID tag that would define the information about that software. So that is how we handle opacity.

>> So that seems -- you hit both the known unknowns issue as well as the known questionable issues. So we've got Jim and then Art.

>> Yeah. So going back to Art's presupposition that if -- if I am well behaved and if my suppliers are well behaved, then that fills out the whole tree, right?

And what -- that only works is if everybody has a preference to obey Demming and to get well-behaved suppliers. So it seems to me that when we're talking about opacity that we're really saying to what degree did I choose a well-behaved supplier. And if we could indicate that, then that would be one way of measuring opacity.

Or, having gradations in it. That is, this is a supplier that provided all of this information, and I know, for instance, that this is the leaf of the node.

>> Um-h'm.

>> A leaf node. Or this is one where the supplier provided information, but I have less confidence in it because they expressed themselves -- they didn't express full confidence themselves. Or, I don't know anything.

>> Sort of a we've got three levels which is I've got it, I don't know it, or something in the middle.

>> Would you please just restate. You were checking a minute ago and you said something to the effect of is everyone okay with this axiom or something. Could you just rephrase that?

>> I want to try to capture two of Duncan's axioms. Which is, one, you're either -- in terms of where this code can come from. It's either Open Source, a binary. And a third option, which was?

>> Either code you created and compiled. Code you got from Open Source and compiled. Or executables you got from somewhere else.

And yes, it only applies in the green box area of the original complicated chart. It doesn't apply to some of the edge cases. But at least it applies to a large amount of software.

>> So we have that combined with the axiom that if everything is -- if you have access to the Open Source code you are compiling it yourself, then generating the complete all the levels BOM is not a hard problem. And those are the two axioms that we have on the table.

>> And I'll be very glad if they become Duncan's axioms and become famous like Moore's Laws.

>> These are the Duncan's axioms. David?

>> So you just raised the point that if you're compiling source code that's provided by another party that that's not -- providing an SBOM is not a hard problem.

I think we should answer that question after we have some of the namespace and naming kinds of conversations because what we found with talking to folks about implementing SWID tags is there is no substitute for actually knowing authoritative information about your own software product when it comes to things like characterizing it and naming it and that sort of thing.

Building things like a manifest is more of a computational process, anybody can do that. But not everybody can sort of understand the context of the software.

And so a third-party compiling software is going to know slightly less about the software that they're compiling than the first party that's actually creating it.

>> That's a great point. So I want to try to capture -- josh?

>> To partially satisfy Jonathan here, based on what Steven was saying from GE Healthcare, one of the demming benefits, forget necessarily what we do in this room, but one of the benefits of fewer and better suppliers that gets glossed over is it reduces operational variance to have less entropy and total catalog of parts.

It's not so much that they were the most superior part. In fact, Jim Ralph did this at Aetna. They had 11 log-in frameworks and UC asked can we standardize on three, and they got huge developer productivity.

So variance as an operational margin increaser is a good thing. It's also a good security thing. And I think a natural byproduct of the pursuit of SBOMs is going to be we're not going to just pick anything from everywhere all the time and we might favor a compiled binary that's vetted and hashed from an authoritative force over the spoke artisanal every time.

I think we should only customize when we need to. I think we will see a natural harmonization around fewer better catalogs of parts. And I think there is some language we could crystallize from what you guys do.

>> And I think that's also going to come up in the namespace issue. So I think hey, look, it's all related. It's almost like we're all talking about the same problem.

So I'm going to try to sort of offer a suggestion because, again, or let's phrase it as a question. If we have these two separate issues, one is --

Let's try this again. The Art framework. There is we've got known knowns, known unknowns, and then data with caveats. Right?

That is this middle layer where I've got it from someone else, but for whatever reason it is not at the full-on level of just being one of a SWID tag that, say, is made by someone else. But there's some reason why I wouldn't trust it. Red comes from an SCA tool, or there's something sketchy there. So that's the translucent case.

And I think does it make sense to say we're going to leave the translucent case aside for now as a flag for future work on it. And then because I think we've sort of got a pretty strong notion in the room that said hey, we should flag when we don't know something, and we should perhaps kick that over to the Standards Group to say is this something that we can do today in SWID and SPDX.

Reactions? I've got a thumbs up. We've got a thumbs up. I can restate that if it's helpful.

>> Thank you, Allan. I'm just trying to bring us back to the use case in terms of whether it is -- if it's not responsive to your initial use case, then of course, move it to phase two.

But if part of the -- if part of the initial use case includes the manufacturer just trying to figure out what it is that their upstream is using, the translucent actually has value, if you will. So I'm not going to comment on thumbs up or thumbs down. I will leave it to the MDMs in the room really to answer that question. I think it would be better for you guys to speak.

>> I think it's okay to put phase one to say you have known knowns, you no known unknowns. And if you have anything else then it's -- then it's translucent, right?

So you may or may not have anything in that category, but it's okay to consider it in phase one.

>> Okay. And so do we think that we have a way of capturing that best effort or the uncertainty with the tools that we have today?

>> Do those familiar with the SCA tools, do they give you a confidence word? I think this is in here, I'm pretty sure this is in here, I don't know if they --

>> Mileage varies when you're using something, for example, like a black deck which was originally for license matching and snippets. They want fuzzy pattern matching. Some people call those false positives. I don't think so. I think it's potential violations, right.

If you want precision, there is other tools like the zone type stuff which is the bad at the partial matching but very deterministic, right.

So I think there is not a standard of process SPCA has to confidence level that I've seen, but someone on the phone might have a different opinion

>> Thank you for giving us, as always, the caveat if you are listening on the phone and you want to chime in, hit star one. Yes?

>> So just I -- Peter Eastman, Refirm Labs. We do offer a confidence level through our API. But through our like web interface that customers see is typically a binary it either is here or not. We are making that decision for our customers.

>> Les, did you have a --

>> I thought I did.

>> Okay.

[LAUGHTER]

>> I do agree with Jim.

I'm not sure about SCA's giving us that at the moment. So I think with the known knowns and the known unknowns we can do that. And we can definitely give you caveats.

>> Perhaps to move forward, we can take the known knowns and known unknowns and give that to the Standards Group and say hey, this is something that we think can be part of minimum viable.

And perhaps Art's group can take a first crack, unless someone else wants to take a crack at thinking about how do we think about the translucency or the uncertainty side of things? Or do you think we have enough we can go forward? Duncan, yeah.

>> No, I do think you can do exactly what you said. I think we should make sure we're not over-qualifying it to just what I will call is the machine readable what an SCA could do. Because at one of these previous meetings, and I don't remember which one,

somebody made some observations on their data and what they had and how they had a lot of suppliers that were one person, you know, e-mail unknown versus a Red Hat or an Oracle or somebody big.

So there is a certain aspect you have to take into account in that confidence that is not only what the machine can read and zeros but where it came from.

>> Right. So I think we'll be sure to try to revisit that and capture the overall problem of hopefully -- we'll call this uncertainty if you don't like the term translucency so we can sort of document, okay, what's that look like.

So I'm going to -- I want to make -- and any last words or, you know, things that we can put in the notes on this topic so that when it is picked up by these working groups they have -- they are empowered to move forward?

>> Just -- I can't remember if it was swamp or carwash, someone in this room might know this, but DHS had two different programs that we're looking at common packages.

And there is an opportunity here for Cloud intelligence here. If someone hunts down and determines what was a low confidence and becomes a high confidence, that could be shareable for everyone's benefit, in theory.

>> And I think that gets strongly to our next topic discussion, the sort of the convergence is very tied to the namespace side of things. Duncan?

>> So just recap again, whose doing what to conclude this?

>> We have the Standards Group is going to explicitly denote the known unknown side of things. So this software is not a leaf, there is something underneath it in a way that, you know. Pulling this out myself, this is not something you have to do. But, for example, a tool could say okay there is this much, these are this many things that here's the name, we don't know what's below them.

And then the framing group is going to do a high level discussion to try to unpack this translucency or uncertainty space. And potentially tee that up to something that could be more applied if the standards group down the road.

>> And then just a question, I guess.

Would it make sense if there is information that comes out of the proof of concept that might be a value in this area, could we highlight them to hey, we know we're having these issues, help us however you can.

>> That's a great point. And I think this has come up that the MDMs, the Medical Device Manufacturers, part of their work is going to be capturing what are the obstacles for doing this.

Jim, do you want to chime in on that?

>> Yeah, that's right. We want to identify any issues that block or prevent information from agreeing with the format that we've defined already so far.

>> And I think that's going to be one of big value adds even before we get to the HDO, what are we learning from the vendors.

And there could also be some work that happens, you know, as -- from the use case group again as there are a number of organizations that are starting to do this. And so, again, capturing those obstacles. We'll work on feeding that into the right thing as well.

Okay. The -- so any last words on this topic? Yes.

>> I would be -- I would be a little more comfortable if we said that the standards group will allow for translucency even if it is a null set at this point.

>> Say it a little more.

>> That is, that we can -- that whatever standardized ways we come up with to define the -- define known knowns and known unknowns that we also specify a way to -- to indicate that it's neither. And that it's up to us then or the framing group to define what that -- what would fit into that category.

>> I don't think that's going to be a problem from the --

[OFF MIC]

>> Thank you.

>> From the formats and standards, I don't think that's going to be a problem because at least with SWID it's very flexible and extensible for how much people want to provide or not provide with SWID because it is a supplier attestation. You know, assumably whatever goes in there is the supplier attestation.

>> Right. I'm just assuming let's don't exclude it at this point.

>> Okay, thank you. We will add that to the list. Thank you.

And I'll help with the coordination on the framing group to make sure that that's -- that those discussions are happening.

>> And one thing on the obstacles, I think our plan was to provide internal and external obstacles. So I think we've been talking a lot about external obstacles, but as MDMs we have some internals that we want to possibly share.

>> Just for the edification, can you give an example of how inside your organization the state is hard to get.

>> Because the way -- especially if you are a big manufacturer, you have multiple product teams and multiple engineers, as we talked earlier, whether it was developers.

They to pull in different source, whether it is Open Source or others, right? Some of that is not as visible and easy for us to get to. Whether it's people have left, it's become legacy, the documentation of that's hard. So that's the part.

>> The comment says we'll provide comments later.

>> Yeah, that one.

>> All right. I want to -- Jim, and then Duncan, and then --

>> I just want to -- another example is if we're not all as disciplined as Steve Abrahamson and we can have already a common list of names, for instance.

[LAUGHTER]

>> Which is a great segue to naming.

>> And the reason I asked for could we make sure the proof of concept was up there as one of the group's tasks for answers -- which I don't see yet up on the board -- was so that they would recognize that we would like to information earlier and perhaps separate from everything else.

Because I recognize that in the medical field like you have to ask a lawyer before you do anything. And therefore waiting for that final report might be later than we might get this input.

>> That's a great point and something that we should sort of include in the feedback for that working group is since there is the generate phase and consume phase, the working group can sort of start on processing the generate data while we're waiting until the end of May. Okay.

And we just had the great segue of, you know, the things inside an organization as a way of collapsing the namespace.

So the namespace problem, I'm going to try to offer sort of a very basic model which is are you using com.sun.java or com.oracle.java.

We have many different ways of describing a unique piece of software. And so that obviously generates problems if we are trying to think about things in an automated fashion.

I don't think there's going to be a single solution, but what I'd like to do is try to capture what are some of the solutions that we have at our disposal now, and what might we want to think about moving forward to help reduce this problem?

And I want to start by putting -- we'll go to Bruce, and then I want to put Dave on the spot to talk about how he's already tackled this problem. But, Bruce, you had a comment first.

>> So the big -- everyone likes to think of there is going to be unique ID someplace, but there isn't.

And basically what we have to do is create alias lists for vendors, products, brand names probably because a lot of people don't know what the brand name is, this supplier and things like that. And probably if you're going to do that, you're going to say, you know, this is a distinguished one I'd like you to use but I'll accept any of them.

If we don't do that, this isn't going to to work based on my experience with trying to do MVD database versus what the acquisitions that we have done and what internal people have done, and legal and so on and so forth.

We should just think about it in that way. It's basically alias lists and then some way to get to the actual supplier for whatever reason.

>> And just very quickly, when you say we should do this, do you see this is going to be something that each organization will be doing for themselves, that each supplier will be doing to create the alias list that people can go to? Do you have an organizational vision? No is a completely good answer.

>> The first organization I think is creating at least a situation where the supplier lists, they will hold that.

>> First.org is going to create sort of the centralized list?

>> There is a format for this someplace. And Art is a lot further ahead on this than my understanding so you can ask him about that.

But once you do that, then I think the individual supplier creates the names for themselves. The problem you're going to have is all these suppliers that are single name people, of which half of our third-party complements are, and what to do about that. But that's a detail that we can solve once we get, you know, to phase one.

>> So I see J.C. and Duncan, but I do want to get Dave Waltermeyer because I know that he spent a lot of time with CPE and then ultimately was involved in sort of realizing that we need to do something else.

>> Yeah, so I -- based on our experience with CPE, we know a lot about what not to do.

>> Can you briefly just give a 30-second CPE for those who may not know it.

>> So CPE is the common platform enumeration. It's a naming standard that has been around for maybe 15 years, 12 years, somewhere in that ballpark.

It's currently operated by NIST out of the National Vulnerability Database. Its goal is to provide standardized identifiers for product names really down to the version level.

And what that ultimately means is the NVD analysts create about 90% of the product names.

And that's largely done when we see a vulnerability for a product for the first time. Not really the time in which you want to actually identify a software for the first time. It should really be done at the point where a software product is actually released.

And so one of the reasons why we actually got involved in, you know, SWID tags and product naming and all of that is because of this problem space.

So the way we feel is that we should leverage existing mechanisms for uniqueness. You know, one thing you could do is use like a UU ID as a way -- a method that has enough entropy and that the likelihood of collision is actually not very high.

Another way, which I think Elliott mentioned earlier in the day, was using something like DNS. We already have -- I don't see a reason why First or, you know, any other organization needs to develop a new list of vendor names when we already have the DNS as a way to effectively provide that for us.

And so the guidance that we've provided around this, and with related to SWID tags is really to use UU IDs or to prefix -- to ensure that a value will become unique, prefix it with a DNS name as a basis to accomplish that.

>> And that gives us towards the uniqueness, but it should ultimately be a path to reduce duplicates.

>> Right. And then I think the other point that you were asking about is another way to do this is to put the authoritative parties in charge of actually providing the information.

So instead of the NVD, you know, creating 90% of the product names, basically by doing a forensic dig of the internet to try to discover information about software it is better for the vendor itself, the software provider, creator, supplier. I was told to use supplier.

>> Supply.

>> It's better for that supplier to actually supply the data.

>> All right. I've got Duncan, J.C., Josh has two fingers, and then Elliott.

>> So first let the record show that Duncan agrees with Bruce and Dave maybe for the people who heard us a lot, that isn't always true.

What problem are you trying to solve that we need to make this super unique name? What is the big picture again of what we're -- what needs to be more consistent? We don't have any at the moment. We are trying to just get going in phase one.

>> Do you want -- someone want to take a stab at answering that?

>> I will answer that correctly because it goes to --

>> Mic, thank you.

>> Sorry about that, Elliott here.

I was going to ask a slightly similar question which is what are the properties of a name?

It's always something that we always ask this in computer science. What is the property -- what are your security properties? How is the name going to be used? Is it -- does it have to be recognizable?

What -- I went to the question of uniqueness because, you know, it really depends on its use. If it's -- does it have to be authoritatively assigned? Can it be randomly assigned?

I'm asking these questions without answers. I think I crassly blurted out domain name. Even someone who is a big fan of using that for distribution purposes and declarative purposes, I don't want to jump right there because I think this is stuff for this room to answer these questions, what properties do you desire? So I'll leave it at that for now.

>> So we had J.C. and then Josh, and then we'll go over here.

>> On the entity resolution front, it also depends on the criticality and assurance posture of the system itself. So for some, you know, just getting a supplier might be sufficient.

For other systems, you need specifically to understand like which mirror site was this particular package taken from. And so, again, this -- this -- this raises the need for like that extensibility to be there on all of these formats.

>> And I think, am I correct in saying this is sort of we have -- we have the core of the name, which I'm now going to put air quotes around, and then there are going to be other fields that we imagine will be attached to it of sort of where are it came from that speak to the pedigree problems, is that right?

>> And there's even like the software heritage project and package URL and a lot of attempts to get some great granularity. It's a little bit of a cold start problem. Like it would be a wonderful thing if everybody used it, but no one does. So, you know, like that's an issue.

>> And can you give us 20 seconds each on the software heritage in PURL?

>> Software heritage is, you know, was I kind of referenced in my overview, it's kind of like the way back machine for software. So like what -- what was the version of this at a particular point in time.

And it's a kind of really interesting longitudinally auditable repository of metadata about software, which is great. And it's Open Source. And then the other on Package URL, PURL, sort of gets to what Dave Waltermeyer was saying about the deficiencies of CPE, which is since, you know, a lot of Open Source developers don't need no stinkin' CPE, you know, they don't create them. And there are issues with the CPE even within NVD. There are actually more CPEs in the NVD than there are in the CPE dictionary for the NVD, but that's a whole other issue.

>> Yes.

>> So the -- for package URL, the notion is that you would essentially use the vector or the path through the package manager to resolve the location of a particular piece of software. And so you essentially get to more of a geographic understanding of the entity.

So it's not really a name, it's an address, right. And addresses are more unique than names. So, you know, if you can essentially get the equivalent of a lat/long on a piece of software, that is a more granular and more unique way of identifying it.

>> Josh?

>> So the context switched a little bit from what I was going to say, but I'll keep it in mind.

It's a bit of a complex point, but I think it's an important one. I said it really quickly in passing, but we want to project into the future a little bit of how the ecosystems will harmonize and adapt to these new objectives.

One of them, if we look at the past for an indicator of the future is there were a lot of malfeasance Java projects on mirror sites. So people started only using Maven Central with canonical binaries instead of maybe getting a bad one.

Other things like dot-net didn't do that and haven't yet done that. And I said it in passing, but the Linux Foundation's core infrastructure initiative badge has a couple of tiers to the badging and there is criterion for the badging. At least as of this morning, there were 274 projects that have the badge.

One could imagine if they added criterion for SBOM or level of SBOM or a certain percentage can't be opaque or translucent or bioluminescent or whatever other values we add. One could imagine that an average developer sitting down to do something for an FDA-regulated device or a safety critical thing or a DOD partner would only choose from the logging frameworks that had such a badge.

So it's tough to project into the future how this will all look, but one of the incentive problems we saw was these small volunteer Open Source products may not have the capital behind them to do a lot of work. But they may want adoption, and one of the ways to get adoption is to supply these things as built and avoid artisanal spoke things.

A lot munched in there, but core infrastructure initiative tagging type signaling, some sort of accreditation. I mean we made a joke at the first one about we don't want the names of cows, but we do like Grade A beef, you know, we do grade certain things. And such a thing could be applied to the software we consume.

>> Yep.

>> No, I withdraw my same --

>> We can go to Jim. You can go ahead, Jim.

>> Okay. Jim first.

>> I was just saying I withdraw my request to speak.

>> Okay.

>> Okay, then I'll jump in. So I can give an actual, you know, example scenario or real life scenario.

So in our SBOM system, we actually do use -- excuse me -- we actually do use the CPE format. And the reason we went that route was because the initial primary purpose of the SBOM system was to use it to automatically associate vulnerabilities with products. And we have the capability to do that.

The challenge is exactly what you indicated in that many software components until there is a vulnerability may not have a CPE number. So, you know, on the good side it is a system that is established. It has a -- you know, a linkage to something that's relevant. So that's very good.

There are certain challenges perhaps in the way that the CPEs are initially derived or maintained. So that I think is something that, you know, if we go that route that could be worked on. But it is a system and, you know, we have implemented with the challenges that were indicated.

Now what we do is if we are adding a component to an SBOM that doesn't have an existing CPE, we make up a place holder that is in that similar format but not an official CPE. And when the CPE is created, then we can flow that update through our system and update our place holder CPE to the actual CPE.

>> Art and then Bruce.

>> Just to go back on something. Understanding PURL is more address than perhaps CPE. But looking at them both last night, they're not dissimilar in sort of number of fields and the way they kind of get more specific.

So kind of a question a little bit for argument sake. If suppliers were behaving as desired and all providing good CPE, would CPE perhaps have just worked and be a -- were there other problems with it perhaps? Or is it just a matter of it's very expensive for one organization to supply the world's dictionary of CPE?

>> Can I answer that?

>> Please.

>> Yeah, or --

>> Internally, so.

>> That is where I was going to go.

>> So the problem with CPE is it sort of has an identity crisis.

It is intended to be both an identifier, a matching format, and a metadata format sort of all munched into a single string. And as a result of that, it actually -- it does a not so satisfactory job but really addressing all three of those use cases.

What we really need is something that is simply just an identifier for, you know, for a product. And because of all of those other things, all that other baggage, you know, maintaining CPE is an extremely large expense for NIST.

And because it hasn't been adopted by industry to the extent that the majority of CPEs are being created by industry partners, if we were to stop supporting CPE today there would be a small fraction of CPEs that would be created on an ongoing basis. And that just isn't a sustainable model for that kind of effort.

>> Bruce?

>> First, I mean this is not exactly directly on the point, but if we had known that we could supply CPE names, we would have done that. And I'm sure that would be true of many other vendors. So if you want to -- if you want CPEs done by the vendors, just ask us and a large percentage of us will do that.

But the thing is that the CPE dictionary is really the only thing we have now today and I like it. And we're adopting it much the way that you guys were doing it which is basically you know, we're making them up when there isn't one in there and using the similar format and we're adopting the ones that are there.

But again, we're using aliases. Because the vendors change names, the products change names. We don't -- we don't -- a unique ID doesn't help. You just basically have to do aliases, and you can decide the unique ID is an alias, but that's what it is.

>> I want to follow on this because I think we've got a couple of different issues and let's sort of tease them apart.

So one is this notion that entities may be the best -- in the best position to create their own names. Except they may not all use the same format.

And so are we okay in a world where we have decentralized that responsibility but we're still going to have a couple of different ways to do it?

And then two, we're still going to have this legacy problem of, you know, a bunch of redundant names for the same thing.

And so is there a way other than having, you know, centralized alias repositories to move forward on that? Or can we imagine a world where, okay, this is going to be the alias repository. You know, node will handle the alias repository for node, and this

community for its things in that community and we will sort of still again federate that approach.

So I want to sort of tease apart those two issues. So response to that? I've got Elliott and Duncan, and then Art.

>> If you want to look at this horizontally, and I think that's your plan, the naming of -- again, I think we're almost putting the cart before the horse a little bit.

There's naming of componentry and there's naming of -- and going back to the model that was presented at the endpoint, there's different levels of naming.

So I do wish we could go into the properties a little bit more rather than the solutions of whether we're using a CPE or something else.

And we have distributed ways to do naming. It's not -- we can do it. But I'm still not hearing the properties discussion other than, you know, we need to be able to search upon it.

I think what the one thing I've heard is that we need it to be human readable or something close to human readable. But the other thing I think I'm hearing is it needs to be indexable against a CVE which is I think a key component of the solution that people are aiming for, for the primary use case.

Am I misunderstanding that?

>> So does anyone want to follow this thread down in terms of we need indexability and we need common -- we need

I don't know what the appropriate information science term is. But A should equal A. We need the property of identity.

>> Cross reference ability.

>> Cross reference ability. Thank you. So is there any two fingers on what Elliott has said? Yes, Duncan.

>> So, I agree it's use case specific.

I agree the use case I care most about is vulnerability.

But we did all of those use cases in the fancy petal up there. So I think we have to recognize that they're not all the same.

I think to Bruce's point again on aliases, I don't think we need to come up with a unique way. So Allan's point earlier of do we have to have a unique way, I don't think we to unique way.

I do think for the vulnerability use case we do have an existing industry problem that Dave mentioned that we don't come up with the name for the thing until after it's broke. And several people have said hey, we come up with it, we invent our own if they haven't done it.

So not totally facetiously, we should maybe consider it is a vulnerability for a piece of software if it is not already assigned and therefore you get one assigned for it.

>> And who gets to do the assigning?

>> That gets into industry will probably have to help.

>> We don't do that.

>> The bigger issue is I think we have to solve that problem --

>> Right.

>> -- somewhat independent of SBOM. And if we solve it, great.

>> And I guess what we should be very clear of we should have an actor when we are talking about this. If it isn't going to be completely decentralized, then someone has to do something. Bruce.

>> Okay. This is a two finger one, right?

If the CVE organization demanded a CPE when you submitted the CVE -- CPE --

[LAUGHTER]

>> Give that.

>> Researcher, I like it.

>> And the only people that are allowed to do CVEs, generally speaking, are the supplier.

>> Right.

>> Then I don't see why, you know, that can't just be a demand. And most of this, of the mechanistic problems we're talking about here, at least for things that are in MVD, which is what a lot of people are concerned about here, can be resolved, at least severely reducing the amount of overhead that these guys have to put in to create the CPE directories.

>> So just --

>> Yes, and we have Dave in the queue.

>> We talked about DNS and the naming convention of the world. And they were able to solve it, right? Name, no?

>> So just so you know, NTIA created ICAN in the late 1990's and a lot more history about that. But that is a massive institutional global organization.

>> So my thought is that we have -- we have industries that have a stake in being able to scan products and to identify vulnerabilities.

So with that stake, they have to identify by product name and connect to CVE to identify that there is a vulnerability.

So my thought is, is if they had a stake in the game, and there was a process that any time a software was developed that they issue or they manage the issuing of the SWID, a tag, and they identify and keep the centralization of all of the software by tag number because they have a stake in the game.

>> Um-h'm.

>> So I'm just trying to think I guess jumping to the solution.

>> So I'm going to go to Art and then Daniel Beard on the phone.

>> This is -- I think wrapping back to I think Bruce kicked this off, and there was sort of two parts to what he was saying.

On the aliases part, so actually agree with that class of problem. It's occurred to me that we've talked about references for saying, you know, component A includes or is compiled from component B.

One of the ways I looked at this awhile back internally was component A relationship is, you know, otherwise known as or also known as. Is this solvable, it's just a relationship that you can just say, you know, Solaris 5 equals Sun OS5. I forgot why they match up. But just, right, you can do it that way without having to have a separate special magical aliases field.

Question for the -- for those who have thought about this. Yeah.

>> Anyone have an immediate response?

>> Generic relationship function that I can do lots of things with also has alias to, alias of.

>> Elliott.

>> This is something the more I think about it, the more I think this has to be left to tooling. You are going to need the alias thing for awhile. But I keep coming back to a couple of things in my own head which is Python provides a certain way to do this. The various software update systems provide a certain way to do this.

So I think a certain amount of thought has to go into the flexibility of this. And, again, I'm hesitant to give more recommendations on the spot. But I'm thinking in terms of that line because a lot of these -- the reason I'm there is, you know, in terms of the -- you know, that all the way to the left guy who wrote some crappy little piece of procedure code that somebody wanted to borrow in, God help us, JavaScript for some purpose that he had no idea you were going to use it in your MDM, right. He was never going to go to anybody to get this information.

But if he wrote, you know, if you wrote it in Python, for instance, at least he had the sense to create is setup.py file and you might be able to derive some information there for -- as an example. So I think some thought needs to go into it.

>> Daniel Beard, often a man with thoughts. We can hear you.

>> I had one, and then right as I pushed star one, Allan, you basically said what I was going to say which kind of happened.

When you are doing software development, you know, there is package managers now for any language. NPM for Node, Nougat for dot-net, and Pip for Python. And typically that's where a lot of the third-party libraries are coming in.

So doing a federated approach is something we can leverage right now because these names already have to be unique within their namespace.

>> So what I'm hearing is we've got federation. We've got aliases for the short run. And we've heard from Josh that there probably will be some convergence as we move forward.

I've got Dave, and then I've got J.C.

>> A few points. I want to reiterate I think using package managers is a swell idea here because that is something that can actually happen at build/packaging time which is I think one of our desired outcomes, you know, for this effort.

I wanted to talk to a comment that Bruce had about, you know, why doesn't CVE just mandate, you know, that folks provide a CPE.

So I'm a CVE board member, so is Art. We are about to start going through a CNA rules revision process. And part of that is about setting what the standards of practice are for what constitutes a CPE, what are the required fields.

So we are starting to have more conversations about what additional data can we get from the CNAs that are assigning vulnerabilities. Product information is certainly part of that.

It's always a juggle as to how much you require because the higher the bar, the less people you get signing up to actually do the work.

So but we're going to have a conversation about that in this cycle. So maybe some progress can be made.

And then I wanted to touch on one thing that Duncan was saying about use cases. I think it's really important that what we do actually allow organizations to map across use cases.

It's not enough to simply just provide an identifier that can be used within a given use case. In a lot of organizations today, I have a vulnerability management tool that identifies software one way. I have a configuration management tool that does it another. A license management way that does it a third.

And really to address some more advanced cyber security use cases, you need to be able to synthesize data acrossed all of these different information sources. Like why are -- why are my folks running software that's unlicensed and unpatched? You know, those are the kinds of questions that I should be able to answer.

And I can't do that if I can't connect these data sources. And I can't connect the data sources if I don't have a common way of identifying software.

>> J.C.

>> So in certain cases, those manifest and dependency files are not present. And so you have to account for the, you know, known unknowns in that case.

The other thing is I agree that package managers are awesome to use. We have also detected package managers do get compromised as well.

So, you know, for that reason it is very important to understand when a package manager is taking source code in clean and spitting it out dirty.

>> Okay. So I want to -- I want to sort of try to tie this up a little bit. But Duncan, two fingers.

>> Just a clarification on my use case.

>> Yes.

>> Because I do agree with what Dave said. So I want to be clear, I think for any given thing that needs to be done there should only, if possible, be one way to do it.

We might agree to disagree at times -- and then we might have to have two ways to do it. But we should try to minimize the number of ways to do a given thing.

But my point was that not all particular -- I will call them fields -- not all fields apply to all use cases. I don't want the requirements for the nuclear launch code software to have to be put into webcams in my house. They're not -- that's more the point I was making.

Different use cases require the different things so when we get to Elliott's point of hey, what do we need this for, it is dependent and we do need to make the superset but we do have to be careful that, again, perfection is the enemy of the good. To Josh's earlier point, we want to get some stuff out.

>> Okay. So I've got Art. And then, Daniel, I think you're back in the queue.

>> I will be quick. This is Art. J.C. I think just said this, I want to reiterate it.

We talked about in the first question of the afternoon the unknown thing, and as a supplier trying to play by the new rules I'm going to make a place holder invented by me, ID for someone else's thing because they haven't provided it yet.

So that's a case where there may or may not be a package management system. I've got to make up some nearly arbitrary name for someone else's thing, and that is something we're going to have during transition. So we need a generic ID system also. That's all. Connect the questions, yeah.

>> Speaking to that. So let's sort of start to lay out what the work to be done is going to be since I think -- I was hoping someone would magically solve this problem, but --

So given that, we're going to need what Art just said, which is hey, when you are rolling it yourself, we should have some guidance on what naming looks like.

And then we should also have some description of what an organization that is creating something new building on what we already have from NIST and PURL and probably another approach or say hey, here is the guidance we already have in naming. And if the group wants to put some normative judgment on the existing guidance, that's great. But I want we want to start with documenting.

>> I will add, as much as we love to beat up on CPE, and it's a great pinata, the elements of it we have found very useful running more sophisticated entity resolution capabilities.

So we can actually use -- you know, if two of those things are provided, we can bounce them off against various automated capabilities to get the other ones. And so it actually is a very useful framework if you've got a big engine in the back doing entity resolution. Just saying.

>> Dave, and then Elliott.

>> I was just thinking as far as work to be done, I would like to revisit what Elliott had suggested earlier which is we should maybe describe what are the characteristics of identifier that are actually desirable. Because then I think guidance simply follows on from that. You know --

>> I have 11 if you'd like.

>> Yeah.

>> I didn't say that. He just said that. I'll --

>> Mic.

>> The one thing I want to cover is also make sure we're adding who's using the name and who is asserting the name and how that assertion is being secured.

>> We're going to succumb to Elliott to whichever working group is going to pick that up and is a good fit for the framing or is there another --

>> Elliott did just register for our mailing list so.

>> Excellent.

>> And we're meeting tomorrow at 11:00 so we could handle it.

>> Somewhere else. Every Friday, yeah, right.

>> And I have Daniel from the ceiling.

>> No, it's fine.

>> Oh, sorry. I didn't see you again for awhile. So thank you for your patience.

All right. So we're going to try to capture some of that and we have the notes that we sort of captured here of sort of first let's be more explicit about the problem we're trying to solve, as folks brought up, and then we'll move from there. All right.

So the next challenge to tackle is the -- what was on my list. What is the -- there we go. The active sharing. These are getting harder as we go on so.

So this is vision of hey, there is data but we imagine the data flowing down the supply chain. How does it actually transit?

There are some cases where we can tell a fairly straightforward story. So the model behind SWID has always been that the data ships with the binary. And so you put a

binary on a platter, it's just going to have as part of the installer, right, David? The -- installer puts the SWID there so it's always handy.

That's challenging for embedded devices, although Dave's fixing that one, too, in the IETF with co-SWID.

But there are other challenges we may want to think of. One, this was something that came up earlier today which is do we want to draw a distinction between the software build side of the supply chain and the last mile of going from the final supplier to the owner/operator who's going to have a slightly different set of use cases?

Does it make sense to think of them as separate issues, or should we try to say hey, listen, we're just going to think of all of it as going from supplier to the next person. I've got one, two, three.

>> You don't always know who your last mile is. Your last mile could have another mile and another mile and another mile.

>> A great point.

>> I think you have to bake in the end model.

Separately, though, while the mic's on, the thing most of our conversations forget when we talk about the act of transparency is that if it is a web resource like Bruce and I might want for our attestation part, web resources are sometimes unavailable. Sometimes they go out of business. Sometimes you're in an air gapped environment where you can't look these things up.

We should make no assumption that we will have universal access and pervasive access to a resource that isn't bundled together.

>> All right. Jim.

>> And I was just going to say that the model that we're talking about where you're depending upon your -- your previous supplier in the chain having done the same thing means that we should continue the same format all along basically.

>> Okay.

>> So I think there are a couple of SBOM acquisition use cases that we're talking about.

I think one thing that we definitely want to support is if I have -- if I hold a piece of software, you know, as built probably, I need to have some definitive way of being able to find the SBOM for that if it exists.

So that could be that the SBOM is bundled with that software or that, you know, some -- some URL or resource identifier is made available. I think there is ways to deal with resources in a way that addresses the air gap problem that was brought up. So that's certainly I think the first required use case.

I think there's also a secondary use case where -- that we don't often talk that much about which is there are lots of reasons that organizations need to know something about the collection of software that an organization has.

You know, because they're vulnerability managers and they want to know, you know, what software versions are available that I can pick from. And I want to understand what vulnerabilities are present in those.

There is organizations like the NVD that are trying to do value added analysis of vulnerabilities, and we need to be able to attribute that to a given software.

I think there is another use case where vendors could actually host a repository of their own SBOMs to make those publicly available. And ideally that would be done in a standardized way.

>> The suppliers hosting.

>> Yeah, the suppliers, yes, sorry. Old habits.

But I think it's important that that be done in a standardized way because it is information that is effectively unusable if I have to implement ten different access methods to actually retrieve it or hundreds or whatever, right.

>> Les, Jim.

>> I think -- and maybe it's just me, but I think we need to define as-built. Because everybody determines that differently. There's as-built, there's as-installed, there's as-configured. There is as -- so can we define as-built before we go.

>> I don't want to do that now just because that is a known open question that I think Art touched on which is where/when do you generate your SBOM and what exactly is it referring to. I'm going to kick it over to Art and then I'm going to go to Josh for his two finger.

>> I consider that's stable, but perhaps that was a mistake. So we can talk about it in the framing group, no problem.

>> Josh.

>> To Dave's point about this should be a standard repository access method or whatnot, I didn't think we were going to try to define that here. But I do agree some of the regulators I have spoken to don't like this suggestion, but I think it's maybe part of their public safety mandate that if there's a bunch of medical device makers that go out of business and they have the opportunity to have all of these in one place and could do safety notifications to hospitals that this vulnerability affects these 12 out of business MDMs.

I think there's those purviews and opportunities. It could be an ISAC or an ISOW for the sector. It could be a sector coordinating council. But there may be natural custodians of the superset even if their sensitive information -- it doesn't have to be public, but it may be really smart for us to have this done by certain custodians.

>> Duncan, two fingers, and then Jim.

>> Just on the terminology issue. I would actually propose that you add another -- we have these various topics we're going to discuss this afternoon.

I think a whole different topic that should be added at the end is the term terminology and input to the framing group which is the one that I think owns terminology. And just a list -- not to resolve them here, but to give a hey, if you're going to use these terms, let's get them commonly defined or whatever.

Because we have in the framing group discussed fit for use and fit for purpose, decided that hey, we can't use those terms because they're legal. And then I saw them twice in the B graphs today. So if we're going to use those things, we need to define them.

>> Thank you. A good thing to flag. Jim?

>> Josh actually stole some of my thunder. Sorry about that, don't mean to call you out.

But one of the things we been talking about is whether or not ISOWS, for instance, can source this data. And for industries that have ISOWs in place, it is a good solution

to it because then it is -- it doesn't depend upon the vendor not only providing the data at the time, but also providing the infrastructure in order to expose that data to make it transparent.

>> Thank you.

>> So this might be slightly off topic, but in the interest of transparency, right, so we talk about suppliers of SBOM as the people sort of giving you the software. As an SCA vendor, we're analyzing other people's things and trying and generate SBOMs.

So is there termionlogy that has to come down for not only who is the supplier of the software itself, but who is actually the supplier of the SBOM that's being generated, right? And how we share that, right, like who is the source of this SBOM and where is it coming from?

>> So this came up a little bit earlier with the notion of translucent data or different sources of data. And I think we've talked about how that can fit into both SWID and SPDX in terms of authorship. Yes?

>> So, as a supplier, I almost certainly am going to host SBOMs on my own website and distribute it with the products. I think it would be pretty interesting for a centralized type repository. I'm thinking like the Cloud Security Alliance Star Registry as an example where people voluntarily submit to it.

There's some interesting -- not to go back to the previous section, but if we're going to have overlapping names or different names for different components, you could actually do -- I almost said machine learning, but let me say classifier of some sort to say these groups are saying XML2 and this says Lib XML2, maybe that's the same thing and we can actually sort of converge on a single name for some of these components if you had it all in one place.

>> And I think that speaks to some of the aliasing work that we were talking about earlier collecting that data.

So we've got this interesting challenge. On one hand, there are unique enough use cases and different interests that we're going to have different approaches to solving. There isn't going to be a single way to do this. At the same time, I think there seems to be a number of you came up with saying we should have, if not centralized at least federated approaches. So we shouldn't decide what they are, but we should think about building that capacity in so that if different organizations wanted to do that they could have that role.

Is there a way to take this and turn it into a small manageable space so that there are, you know, here are six ways are doing this?

>> So there is an IETF standard that I worked on called Rolly. It's RFC 8322 which basically describes a protocol, an exchange protocol and a metadata format for representing arbitrary what we are calling security automation information.

One type of which is, you know, an SBOM. And so that is a protocol that would more or less standardize how you would represent that on the wire, how you would establish the sites.

>> Is this a transport layer protocol or is this a sort of an organizational who is putting it in where?

>> It's a transport protocol with the assumption that this data is actually federated. And it's -- it's built on top of Atom Pub which is a syndication format.

So the idea is that if multiple organizations sort of federate their own data through syndication, you could actually coalesce that into more centralized repositories as well.

>> Further thoughts? Anyone want to sort of imagine from the user perspective? So we've had a couple of folks saying all right, if I'm generating the data, here is what I want.

What about if you're using the data? How would you sort of want to get it push, pull?

>> Consistent.

>> Consistent.

>> Yeah.

>> You would like to have a very small set of ways that the data is available to you?

>> Yes. I don't want every MDM to have their own way of sharing me the data so that I have to create a gigantic system to collect it.

>> That's -- and I think that's one of the challenges if we sort of say we're going to federated but without the institutions that are going to do that federation. Art, and then Duncan.

>> Just very briefly to that point. The rough thinking at the framing group is we are sort of hoping or aiming for is, you know, well, two formats.

One would be perhaps better, but there is two formats, multiple ways to get it. To your point, yes, many ways to transfer it and receive it is still a problem. But at least if you have three or four collectors, you are getting the same data.

But I don't see a way -- well, sorry. Specific, it might work. If you're talking medical devices, there might be a system within that ecosystem that is consistent and you are good to go, right?

At the sort of framing working groups level of we want -- the idea is that I'm transferring the component to my downstream. And with that component is the thing, the as-built document that manifests for it. I want that to go or be available at that time, however it gets transferred.

I think that's about as far as the framing group is going to be able to say, but further down in the weeds, sector specific, device specific, regular software that has lots of file system space can just do what SWID and SPDX does and have the files that are on the system there.

But at a high level we're going to have to say something general I think like provide it consistently at the time of handoff or delivery.

>> Duncan.

>> I think we have to be careful and think in terms of the past how things used to work. And there are lots of problems.

Phase one what we want to work immediately and what we want to work further down the road. And I think one issue that is a little conflated in what we just discussed is the tooling topic, which is next up on the list that we haven't got to yet.

What I think I heard you say is not necessarily you want it all in a common way, you want tooling that supports doing what you need to do which is not the same question.

>> That is a very good distinction.

Well, let's look at it from the supplier perspective then. How would you like to share? Is this --

>> Define a format, and we'll put it out that way.

>> So we've got the format. I guess what we're trying to get at is what do you mean put it out? Is this just like you're going to have like a canonical part on your --

>> We'll make it download in XL files, we'll make it available in some sort of rest interface. Just define it, we'll do it.

>> All right.

>> The theme.

>> I'm just -- the one thing I do worry about is we have a joke on our team that if you have seen one medical device patching patch process, you have seen exactly one medical device patching process.

>> Yes.

>> And what we don't want to see on the HDR side is 300 different ways of doing it so we build book of figuring out where everybody's SBOMs are and then hope that they never change them because re-indexing all of this is going to be cumbersome.

>> So comment on both of them. So I think when you say we, I think you're -- you're saying I because at the moment --

[LAUGHTER]

>> Yeah.

>> Okay.

>> Bruce has my proxy so he is speaking for us.

[LAUGHTER]

>> What I'm getting at is I understand what you're saying when you say give it to me one -- the whole patch, I get that whole one patching, got it, all right.

If we don't come up with some way of trying to and all of us come to it or you guys come to an agreement on the consumer side of that of how we would produce these to you, you will get it 300 different ways handed to you.

And that we becomes a bunch of 300 I's, right? We will give to you. Give me a spreadsheet, and I'll give it to you, but I'm going to give it to you one way and he's going to give it to you another way.

>> And that's not what we're trying to get.

>> I think one way is good.

>> So I said we because I was thinking about the CVE effort. And we're getting pretty good, you know, on that.

I mean it's not just us. It's lots and lots of people, people that put in CVEs. And they are defining a format and people are pretty much adopting to that, or formats, I should say.

And I think that you'll get that, you know, if we can tie it to CVEs particularly for things like that, at least the naming parts and things like that.

I think we can make great progress there. And as far as saying I meant, you know, large manufacturers. I'm sorry, I should have -- I was being presumptuous.

But I would say that would apply to us and Cisco and Microsoft and IBM for -- at least.

>> All right. So that's -- that's a small number of companies, but they're large market share.

But still, again, from the total quantity of vendors we are trying to sort of see how we can collapse the space. I have one, two, three, four. I forget who I pointed to when I said one.

>> I'm number one.

[LAUGHTER]

>> Yeah. One thing to consider in this discussion as well is that we're talking about the SBOM and how do we make the SBOM available in some kind of efficient consumable format for HDOs.

And I think my friend Tim from Mayo would be the first to admit that's not the only element of product information that they're looking at.

So when we're sharing information, we need to expand that -- which may be beyond the scope of this group -- but we need to consider that HDOs are looking for information well beyond the SBOM. Things like the answers and comments with MDS2 questions and other things. So the extent to which we can make all that relevant information available in some consumable way, that's where we could benefit.

Just like we don't want multiple solutions for SBOMs for different use cases, we don't want a solution to share SBOM information, a solution to share MDS2 information, et cetera.

>> Can I flip that question around? Are there existing channels that you you are using already?

>> No.

>> For the data that you are sharing, is it done pretty much with Spoke?

>> Yeah. I think each manufacturer has a mechanism to do it. We typically have portals where we put our version of the information and our format, but eventually -- and the good news is that early on in this journey towards secure healthcare there hasn't been that much information to share so it hasn't become a huge problem.

As we have more information, more SBOMs, more MDS2 data, more patches on a regular basis, it's going to become much more of a need.

>> So collapsed communication channels when possible so we'll keep an eye out for things that are already happening. Two, yes.

>> Right here. I heard the concern about 300 ways to consume SBOMs as a vendor.

Whichever method I pick is going to be wrong because I'm going to have 1,500 customers that all want to consume it in a different way as well. So no matter what I do, they're not going to like it.

We all have websites. If we could define something like a rest API with a well-known URL that said this is the place where we've all agreed by convention or we've agreed by standard this is a place where you can find these things. We are not a standards body here. That might have to be an IETF type thing, but that could be one way to go about it.

>> So having a share website.

>> Three, right?

>> Number three, yes, thank you.

>> So Rolly is a rest-based API with a well-known URL. It is also a generalized approach that can work with many different kinds of information.

So I mean it was -- it was effectively designed to be able to support publication of like vulnerability information and configuration information that relates to products. And there is no reason that it couldn't also be extended to, you know, to support some of the medical device use cases as well.

I just kind of wanted to reiterate, though, what I was hearing in the room which is there seems like there is some desire to at least look at where there are standardized ways to, you know, to share SBOM information.

Does that mean in the formats and standards working group that we should maybe spend some time looking at that, too?

>> I mean, I think one of the things that we have been looking at with SPDX and SWID is like here is what's most commonly consumed.

>> Yeah.

>> And then the question is does that meet the need?

>> But I think what we're talking about here goes beyond the format of how you express the SBOM data. It is more about how do you discover SBOM data that's out on the internet, per se, and then how do you share it across communications channels.

>> Well, it is --

>> Sorry.

>> There were a bunch of people in the queue. So we've got Jim, and then Josh, and then J.C.

>> Jonathan.

>> Sure, I -- I'm next, right?

>> Yes.

>> Just making sure.

>> So in thinking about a federated approach, it has two advantages. One is it prevents Mayo from having to have a book of how to access each supplier's SBOM and maybe other information.

But also, I think of the small medical device manufacturer who doesn't have to build up an infrastructure to serve up -- I know it is not very complex but there are a lot of very small shops where they're focusing on providing medical device technology, not on providing -- and they may be handcrafting an SBOM because they only have to do it once every six months or something like that. And so a federated approach would help them out, too.

>> Just need to have a federation that actually covers enough of the bases.

>> Right.

>> Josh.

>> To the original question of as a producer of SBOMs, which I am, how I -- when I produce them I don't want to be completely redundant with Bruce, but my different markets I serve are going to want to consume it differently.

So as long as I have the content, I can vary the presentation layer of the content. I do think I'm going to have to remind everybody, once again, that if it's solely a web resource then it doesn't help the air gap offline networks. It doesn't help once you go out of business. It doesn't help when we have internet outages.

So I believe I'm going to communicate this plural ways. One would probably be shipped with my installer, one would probably be on my support portal, one of them would probably be rest API or something like what you're talking about with my website.

And I also want to clarify the noun or the subject of the sentence because the SBOM inventory, minimum viable inventory, or whatever we're calling it, should move around the way I just described.

As far as my current best attestation as to exploitability, that should be on the web because that's a femoral or will change upon the revelation of new information, whereas the other is static and true all the time.

So which thing we're sharing may dictate how we're sharing. I wouldn't want to give my CVE listing in a static way at build time because it's going to be different a week from now.

>> Right.

>> So which thing we're sharing may dictate how we share.

>> J.C., you still have --

>> Yeah. I actually think that a lot of the stuff can go into our next kind of how-to guide that standards and formats produces and is like we can get to this.

>> Great. So and I think we're going to try to test that with saying all right, collect what is out there with an emphasis on what's being used.

So like Rolly is being used for a bunch of other stuff, then that's fantastic, and we will sort of ride on top of all of that. Jonathan.

>> So I would be a proponent of having a central area at least from the medical device industry where SBOMs and CBOMs would be located as the source of truth.

Understanding the industry once you put things out there for public consumption, it gets on the internet, you know, it becomes someone's bible because they found it, hey, this is the SBOM for this product. I was thinking that the FDA is going to require the --

[LAUGHTER]

>> The submittal of an SBOM, CBOM, whatever BOM, a BOM. And not to say that they are the central repository of truth, but they are certifying the product at least from a medical perspective.

>> Seth is going to do this.

[LAUGHTER]

[OFF MIC]

>> All right. I want to -- I want to make sure that we have time to touch on the tooling side. So we're going to sort of delegate this to the standards and formats group with the notion that this going to be sort of one of the things that is going to be working on possibly for the next rev.

All right. Let's give 10 minutes to thinking about the tooling side. And I want to start off with these lovely questions that we have come to which is hey, guys, when we're talking about this, what do we mean?

So the things that have come up that I have seen, seem to be fitting into the large buckets of tooling to produce this stuff. So let's get this into IDEs, let's get this into build management tools, things like that.

And then let's focus on how we can automate the consumption of SBOM data. So getting this into management tools, getting this into your internal development tools that are sort of building your white listing and things like that.

Are there other categories or things that you guys want to sort of add on to this list when we talk about tooling?

>> Hi, my name is Ed Hyman, I'm with Abbott Laboratories.

I think I can give you a little bit of practical comments around the producing as a med -- from a medical device manufacturer who is participating in the SBOM proof of concept.

So when you talk about producing and tooling, I think it's kind of interesting, at least for me, to note that there's a little bit of a difference with a manufacturer versus maybe a supplier, a supplier being software only, in that not only do we have software and hardware that composes our product that ultimately gets delivered, installed, and configured.

So there is really at least two steps to that. One is software we build and software that is somewhat built in the traditional manner of I have an iterative build process and I hooked tooling into it.

I think you could certainly put tooling we talked about that could help identify and manage and establish the content of our application.

But there is also an activity around I'm defining the platform it actually runs on, right? So that's a -- it's a Windows operating system with 10, 15, 20, 30 other components that are all part of the -- that are all part of the platform that ultimately then we install our software on.

So I think you have to kind of consider, you know, we're really getting it from sources. One, the application we built. And one, the platform we defined.

>> That's helpful. And that is sort of something that we want to make sure we capture in our -- in the whiteboard model that the framing group has been doing.

>> And can I add one other because I kind of saved this as well.

>> Please, you've been holding it in all day.

>> I kind of wanted to wait for the other discussion.

And so one sort of a practical comment, as I think really was confirmed by Steve and even Jim, is that I think ultimately -- and this may not just be specific quote to a manufacturer, but there certainly is an identifier mapping activity that has to take place within our organization.

So as we establish here's what we will identify the Windows embedded 8.1 operating system, here's how we will identify Windows 10 or whatever it may be. If we are developing multiple products, then we've got a mapping activity where at least internally we've got to identify this is what we call it.

So then we can handle multiple aliases that Bruce and others have identified. Ultimately when it is time to produce the SBOM, we may have to either pick and choose. We may have to generate more than one. But it's all going to have to take -- internally we're going to have to establish what that mapping is -- how we manage a mapping until either the industry catches up or establishes a final identifier or we just have to be able to manage multiple.

>> Great, thank you. And I think it's the federated thing that that we were talking about earlier.

Other approaches when you guys say hey, we should really be focusing on making sure this is something that we can build into. Bruce?

>> One other item eventually some of these come at the very bottom, but --

>> Yes.

>> And -- sorry, your mic, please.

>> A lot of those -- a lot of times there is somebody that is building the very bottom component. And it would be good if the tools make it very easy for them to identify this is the bottom level and here is its name.

Half of the components are identified by somebody with a single name. I would like to make it easy for them because that really cuts down the problems a lot for everybody.

>> So make sure that whoever is writing left pad has something that will just automatically prepopulate or give them the tools.

>> Really easy, free tool, download and run it, yep.

>> I think that builds on what we were talking about earlier with sort of the trying to rely on some of the ecosystems that already exist for that. Dave?

>> I mean but what I heard you say is that we need some party to agree to a name, you know, for this thing, and then share it with everyone else.

Why can't the thing just name itself? And then that folks stop coming up with new names for things and just use the name that it's providing?

I mean doesn't that simplify things dramatically than, you know, than having to appoint someone to centrally manage something and then have to keep everything in sync all the time?

>> I'm not saying the supplier can't name it. I'm not sure what name itself means.

>> Yeah, that.

>> If by that you mean the supplier names, then I think that's fine. But the supplier should try, you know, their very best to make it unique or provide an aliasing facility if it isn't.

>> And the other think I wanted to clarify is by root node, do you mean like some leaf node that everyone depends on? Or are you talking about the end of the line software that is actually running on someone's system?

>> He's talking about the leafs.

>> I may be the odd ball out here, but the tree is standing upside down to me. So I say open SSL or notepad are root nodes, there is nothing further back.

>> Meaning that it is the end of the roots.

>> If the leaf --

>> The leaf is the HDO who builds no software themselves, only consumes things. The root is open SSL or left pad who only writes their own software. I'm happy to flip my mental tree around, but let's --

>> So we don't have to get into a metaphorical discussion.

>> Sorry, the tree is upside down, it's easy.

>> An atomic component is one that contains no further subcomponents. A monad, if you will.

>> And they should name themselves, hopefully. They might not be doing it, which is the problem, we have to name it for them because they aren't doing it. But ideally they would name themselves and we'll just use that name and we're done.

>> All right. We don't have to belabor this. I want us to start thinking about this as we move into Phase N. And this is going to set us up for our next discussion. But just wanted to say hey, we're talking about this.

>> Again, it gets into which use cases. Because I believe the database that Bruce referred to was their licensing database which probably uses a lot of software from single developers like now that I'm an old retired guy I write software and put it out in Open Source and some people use it occasionally.

I don't compile things for people. I put my Open Source out there and let them compile it and that that does make this problem a little bit trickier. Because when you

do take several components and compile them yourself, that's really when the name we're talking about -- at least in the vulnerability use case that we're talking about, we're talking about the name associated with the raw uncompiled code in the licensing use case which is, for lack of a better term, I'll call it an earlier point in the pipeline.

And we're talking about the vulnerability package name at the point of the executable, which is usually made at the build time, particularly if you are in the nuclear launch code business and you want the full providence and everything.

So, unfortunately, it does become a little gray because of the use case issue.

>> Jim.

>> So it keeps coming back to me to this model of iteration where every step in the chain has to be well behaved.

So I would say that what we really should be coming up with as one of our deliverables is a very concise description of what it takes to be a well-behaved supplier. Which means not only providing the SBOM but naming yourself appropriately, however that's defined.

>> And, Art, you are nodding enthusiastically. I feel like that is something that will be in the framing group.

>> Please add stuff.

>> And think about that.

>> Please add stuff like the badging, right, the free market like scoring like CII.

>> But I think that's -- once we have the recursive step that everyone can follow, then we can hook into all of the other efforts that are going on around the world of how do you be a well-behaved actor in this.

I want to move on now to make sure we have a chance to talk about this overall process. Because one of the things we heard this morning is, you know, what do we want to get done now as sort of a phase one. Getting minimum viable out there with the real acknowledgement that it's not going to be complete. It's not going to be the final perfect thing. It's going to be a good enough.

And we want two things. One, we need to get it out there. And two, it needs to be built in a way that we can refine it later on.

And I wondered, does anyone have a vision of beyond what I've just described what you'd like to see for sort of the version 0.1 that we're going to release to the world of what you would like for these?

>> I just want to point out that maybe we're in a slightly different category in the proof of concept because what we're going to be delivering primarily is information that will inform the rest of the groups as well as talking about the experience with the public.

>> Definitely. That's a really good point. Speaking primarily to the working groups. And I've -- as a shorthand as I've done briefings for a bunch of different folks in D.C. and around the country.

So describing the work that you've all done as the what, the why, and the how. And so getting the first level up there of what is an SBOM? Why are we doing it? And then how do we do it? Go ahead.

>> This even came up at lunch talking to a member of the press, but there continues to be -- despite our efforts, a massive conflation between the pilot's goals and the minimum viable product definition.

And I think we must have explained it 50 times in the last couple months, but we have to be crystal, crystal clear that your pilot is to shake out surprises on the creation and/or consumption in an HDO/MDM pair-up.

But not to be the minimum viable product from this initiative. And I don't know how to say it differently but I just implore people it continues to be very confusing to folks. And then it is added to by the fact that, you know, there is that looming point that FDA says if we produce something useful in time they will use it.

So they'll be like the first proof of what the minimum viable project is or isn't. And I feel like we might have a slight race condition now that I framed it that way which is I really do want to see what they encounter in the tabletop exercise before we codify that this was a minimum viable product.

So there might be a slight Gant chart mismatch here and impedance mismatch that we should factor into our June target is all I'm saying.

>> I think that is a great point. I blame the lawyers. Certainly all of the work that the proof of concept had done sort of set up to be under way by now would have gotten away with it if it wasn't for those pesky lawyers.

>> Let me just follow up on that.

>> Please.

>> So we've said from the start that we're not trying to key fine the minimum viable product, right?

>> Right.

>> I'm not criticizing you. I'm remarking on the level of confusion in spite of our best efforts.

>> And this goes even all the way back to the first meeting where this shows the word proof of concept rather than pilot exactly for that reason.

So one tentative timeline could be the notion that by June we would have some draft deliverables by the framing use cases and standards group, and the standards group it might even be two deliverables. And we would have time to have input from the proof of concept on the generating the data by then.

But the notion is these would be very much drafts that are mature enough to get much broader feedback. So they're polished enough that we feel comfortable sharing them, but making very cheer that they are drafts for input.

I've got a two finger from David and Art as well.

>> This will be quick. I don't think I have it in my notes, but does the healthcare pilot have an estimate of when the exercises may commence?

>> Yeah. So we expect to have the SBOMs completed, ready to go by the end of this month. And then by the end of May to have fully executed. Not finished our report, but fully executed.

>> And will that be in the normal meeting cycle, or will you be going out of cycle sort of events or something for that? If I wanted to come to your tabletops, how would I do that?

>> We haven't --

>> The HDOs are going to be doing them internally. It's not going to be -- and then they are going to share out their lessons. In fact, there are two nested groups, and you guys who are participating, do you want to sort of talk about your trust relationships?

Like there is the NDA which is between the hospitals and the manufacturers. And then they're going to report out to the working group, which has a broader group.

>> I will just join the working group, and that will be my answer, thank you.

>> I would also add to that that the HDOs have their own processes.

>> Exactly.

>> So it is not a constant across all of the participants.

>> It's a feature, not a bug.

>> As well as the MDMs are creating their SBOMs as best they can to the formats that are requested, but they may not be all the same. And that's part of discovery.

>> Duncan?

>> So if I could reiterate my previous concern. I recognize that those final reports because they're being generated under NDAs, they got to be reviewed by lawyers, they're not going to make it in time for the other people's June deliverables.

So if there is anything that can be done like some of the manufacturers right now are creating SBOMs and running into issues. If there is anything that can be done to get that input out of them and into the other groups to answer the questions that you all now know the other group is going to be spending the next two months on, it would be very helpful. Thank you.

>> We already mentioned the fact that we should collect and report out on the MDM experience of creating the SBOMs. And we'll bring that into the meeting next week.

>> Thank you.

>> Right.

>> Dave?

>> So one clarifying question. So are you going to -- would you be willing to come to some of the other working groups and do that out brief?

Because not all of us attend every working group meeting. Unfortunately, I have had a standing conflict with the healthcare working group so I haven't been able to participate. I mean if there are findings I think that are useful for the other work groups, it would be really useful to go there to share those findings.

>> I'm happy to help facilitate that so that we don't overload the HDO, but certainly we can get a selection of the manufacturers that are generating this and try to do -- make sure that we've got some briefings -- not briefings, as soon as possible.

>> And then I had another question.

So for these public drafts, what are -- what's the sort of characteristics of these drafts that you would like to see? Like how -- how done is done? How drafty? How complete? You know, any thoughts on that?

>> So that is a fantastic question. And really it sort of turns back to you because the next setup was going to be to sort of have a discussion about the audiences.

They should be complete enough that people don't feel their time is being wasted reading them. So this also includes editing for those of you who read lots of other people's documents. It's a good sign, hard not to take it personally when somebody gives you a poorly edited document. But also polished to the point that we're as clear as possible.

So we have done some internal wordsmithing and made sure that yeah, we've all talked about it. So Not every single sentence needs to be committee-sized, but what I was going to say is part of that timeline for getting that draft ready will include some

working groups where you actually have a conversation of how do we make this sentence better.

That level of detail while certainly not -- while acknowledging that hey, ultimately we're going to be getting feedback from other people. Does that make sense?

>> Allan, if I could just add. Try to make them so that somebody who hasn't been participating understands what you're talking about at every point in your document.

>> Yeah, what's the target group I guess is -- what's the target group for reading it?

>> I'm going to touch on that in a second because that's something that I think has to come from each group. And having input from this body of what's the audience. But I have a two finger here and I have a microphone on there.

>> If I could add to the end of your sentence including what is in phase one versus what is further down the road with a focus on phase one.

Do remember what was said earlier that the FDA is looking to use some of this, so there is at least one use case on a much tighter time frame than many of the other uses are. So if we could try and meet their needs because recognize, as Allan said earlier, governments do govern, if we don't give them input they're just going to pick so let's get them what we can.

>> Thanks.

>> Not that the -- going not that the SBOM proof of concept becomes the de facto when it's done, which is we're trying not to make.

FDA has been very flexible. And even though it becomes something in a guidance that's SBOM or CBOM, or whatever you guys want to say it, is there's going to be a period of time with that thing being fettered out anyway so there won't be --

>> What I'm saying is we don't have to solve all of the other industries and all of the other use cases by June, if we can just decide to defer that to phase two if it will get us better output by June.

>> Exactly. The NDAs, to answer your question earlier, the NDAs for internally for the participants is just for us to make sure we share -- we mentioned that earlier, right, the summaries that would come out of that, it is just a matter of not providing proprietary information. Outside of that, it's to provide everything we've learned.

And on the June draft deliverables and having input from the proof of concept, can we make that more the end of June?

[LAUGHTER]

>> Well, let's -- we'll drive into the calendaring in just a little bit. But I think that's an important thing to acknowledge so we'll flag that.

But what I wanted to sort of try to capture is what really came out earlier which is we've got phase one, and do we think we have an idea of what that looks like?

And then two, question that was just raised which is hey, what do we think the audiences are going to be? This is going to be your chance to take the work that's happening, you know, NTIA is a small agency. This in the scheme of it is a fairly small process that is purporting to offer guidance to the entire digital world.

And so we're going to want to sort of say hey, here's our vision, and get feedback. And so we want to make sure that that's something that we can try to have an internal audit in our heads of who's who going to be reading this. Josh?

>> I was also going to urge for late June.

But in terms of phase approaches, having been on the receiving end of some very heated fear and trepidation over being cut out of scope from DOD, for example, I got a lot of calls over vacation weekend.

If we do talk about phase, we should do some expectation management. Phase two can't be never or question, question, question. I think the notion of phase should be, you know, a bit of a consensus here, but it should probably make clear that we don't mean in 2025 because that deliver uncompromised thought paper and defer kind of heat and light is very intense. And they don't need it as soon as FDA needs it, but they want to see it is tractable and this is a viable delivery vehicle for them.

We don't have to hit their requirements. I'm just saying for anyone who sees their baby cut into phase two, we should put some reasonable expectation horizon around what two is.

>> So tempting.

>> So as far as what should be in phase one, I think we have a lot more confidence on that. And I think to me it's the harmonization of the MVI and the amplification of its adoption. And the first, you know, alpha customer is FDA essentially.

People -- I mean just as a strawman our initial opening remark, I think it's MVI and harmonization and amplification.

>> Very good points. And also a very good point on sort of, for lack of a better term, is the sort of high assurance use case because I think we do have some idea of what's involved.

And that's something that we can do a little extra work fleshing out of what that will look like even if we're not defining it with quite the same precision as the MVI. Les?

>> So just to be clear on phase one, I would like -- I would like to see phase one definitely have some recommendation out of -- I guess we said the standards group for -- oh, can't hear it?

One thing out of I think we said the standards group was the sharing. So sharing how this may be and how we may share this.

Because what will happen, as we know, yes, it's a proof of concept, FDA is going to want whatever. And phase two is going to be down here a little bit and we're still going to have to deliver something and the customer is going to want something.

So that piece is going to fall between phase one and phase two so if we have something where we can start down that path and not just push it to phase two.

>> Okay. Further thoughts? So let's talk about the audience of -- and we might even want to go group by group here.

I don't think it's fair for any of these to assume that, you know, someone who has never touched any of these issues should be able to pick this up and immediately understand it. I think that is going to require a little too much background.

But certainly the framing groups and what is an SBOM guide probably -- may not want to assume the most technical background.

And so do you have thoughts on, you know, think of a hypothetical or an Art type of leader that we can start to have in our heads as we think about each flap. Josh?

>> So to enumerate potential candidates?

>> Please.

>> There is a -- I like to design for Bobby Stemply. No.

There is a procurement team on how to ask for during purchasing. There is an operator that may use this for inventory and vulnerability management. There's a producer or build person. There's a lawyer or a government affairs person. Those are two separate things.

And I'm not trying to flood us so that we have to have 10 papers, but I almost wonder if we need like 10 intros, right? Like we -- in this room alone, we have government affairs people, software developers, hospital operators, device manufacturers. And again, the nouns and verbs we use are different.

So I think they with point to a canonical main body document or documents, but they may need an on-ramp per stakeholder type.

>> I think that's a great point.

We may -- from a drafting perspective, that may be a better thing to think about say all right once we've gotten the feedback then we'll have to custom interface. But we could do that how to if we have the time if we can start planning. Duncan.

>> So I heard two groups left off Josh's list which was the people who actually have to do it. I'm not even sure we need to name that as audience but more importantly the people who decide should be doing this at all.

More the executive or industry or regulator or whatever and the pros and cons because it's not necessary in all cases, it is necessary or it is helpful in some and sort of the decision makers would be what I would think if -- what Allan's original listing of sort of the issues was one was yeah, people aren't doing it now. And we sort of collectively think they should be. So what could this set of documents do to change that should be aimed more at the decision makers.

>> Thank you. Bruce.

>> We might consider what we'd have to to write if we were going to send it to some place like CNET or PC World or something like that and then decide if that was adequate or too much work or something like that, and then back up or change the target a bit.

But it seems to me that at least some version of some of the documents ought to be suitable to sending to publications like that.

>> This is tech journalists, being able to make sure they can easily understand it?

>> Yeah.

>> Says the guy sitting next to a tech journalist.

[LAUGHTER]

>> And I think building on that a little bit, this gets to the broader awareness and adoption piece which is even if the documents themselves are more traditional white papers, as we move from draft to something that we think is going to be the phase one deliverable then we're really going to want to spend a lot of time thinking about packaging.

Josh talked about facts, and Josh even talked about videos. If somebody wants to come forward with some production value, I think that's a fun idea.

We have go the -- important to say who is going to be consuming it, and then we can also sort of say we can predigest certain parts of it.

What about the standards group? So standards group we talked about we've got the white paper which is in draft form.

>> So I think the how-to guide, which is essentially okay, so where do I get one of these SBOMs anyway? And how would you maybe hand that to a technical person and have them situated and oriented enough to actually start doing it.

>> I like that. I think that's great.

And that may be combined with the recursion step guide that we just talked about earlier that I think Art's group is going to be thinking about which is hey, an organization is going to do these, check these six boxes to be a good actor or to say we are now SBOM-ready. And then one of them is going to be do it with these tech specs. Yeah?

>> This might be self-serving, but the language you use in somehow suggesting whether it's true or not that this may become a future requirement for government procurement will help me properly motivate my technical teams to actually pay attention and get started on this and take it seriously.

>> I would certainly never suggest such a thing. Is -- I would not, this is true.

But it is very easy to start coming up with a very long list of people in the last few weeks alone have suggested that that might be a thing.

Certainly NTIA believes that industry can lead this, especially with a decent understanding of the market to drive demand.

>> I can give you a list in the hallway.

[LAUGHTER]

>> And I think that is a big part of it, which is that if this is coming we have to get in front of it. And that is again your -- as we get into the afternoon and everyone is a little tired, that is your charge is saying that this is -- this is the power of -- we can define what this looks like.

And so trying to make sure that we can do that in a way that's effective and still nimble enough to move forward. Art?

>> Sorry, I was just trying to catch up and make sure my notes matched.

The third bullet and the fourth sub bullet seem to conflict. And I would say I think we are going to define minimum viable product. I have a note here pending results from the proof of concept.

>> The proof of concept.

>> Of course, everything is modifiable by reality of a test.

>> The proof of concept is not going to define the minimum viable product.

>> Yes, I just want to be --

>> Thank you. Thank you for catching that.

>> Right.

>> And, yeah, that was --

>> So we will -- okay. Thank you.

>> The use case group. Do you guys have an audience?

I think the work they've done, I just saw all of the faces react when they sort of just show what their research was able to capture in terms of packaging that.

Do we have thoughts about audience for that and how we can maximize it and we can sort of do a short version -- the near term and then the sort of stretch goal for how to package that and how to frame that?

>> Our current thinking is we're nearly done collecting. Just to recap what I said during our 30 minutes, we definitely captured quite a few state of practice of current behavior.

What we wanted to shift to between now and June was to capture the -- we'd really like to do this, but we're stuck and there is obstacles type stuff which could introduce and amplify which things should be in phase two is the way I'm thinking about it.

As far as what we would deliver, though -- so as far as harvesting, we would harvest some of those less tangible, less concrete, less successful stories right now for future requirements.

But in terms of deliverables between now and then, I think we've the raw data, we have to package it in more consumable ways for the CNET type audience or the consumers we talked about. We have a nice unified story but we don't have it well packaged.

>> Thank you, I think there is some good work to be done there.

>> Is there consideration to consolidate all of the working groups' information into one?

>> So that is also on the list of how we're going to check down because I think some of this stuff is going to be free-standing.

And so the vision could be something like we have documents that fit quite neatly together, and we want to minimize redundancy.

But at the same time, if someone picks up the standards or the quick start guide, can that exist as a free-standing body with pointers to the other side of things. Art.

>> One specific example, I think I saw three different groups give three different lists of use cases.

And they were mostly the same things but different words and different levels of outlines. So the framing group will take on a task but we're going to just collect and propose one or we'll use else's. But we should have one and not call them different things and two papers, right.

That's a small example, but we've got to get that sorted out. There's some basic like editorial conceptual harmonizing that will make things look more consistent.

>> And could we please standardize on Oxford commas.

[LAUGHTER]

>> Yes, the framing working group supports the Oxford comma.

>> As does NTIA.

>> Good.

>> Jim?

>> So the proof of concept group envisions an output to be of two forms. One briefings for the internal NTIA efforts, and the second public briefings or public discussions or public presentations.

>> I think that's going to be very useful because there is different time tables there. All the other working groups are really going to want your input as soon as it comes out. And the framing probably is going to address also some of the healthcare-specific work the HSCC is going to be looking for.

Speaking which it's a good segue, Afton, we're sorry that you've been waiting in the queue for a little while. I got bumped from the meeting view, so please chime in.

>> No, it's okay, Jim covered it.

>> Oh, great. How efficient. Duncan.

>> So in the interest of trying to meet the June date, I think we'll have to work out, you know, between now and then.

And one thing I would recommend highly be early on the list is come up with a document structure, come up with an outline, and come up with swim lanes so we don't get into the use case thing that Art just mentioned of the framing thing has one set of use cases when we have another group actually named use cases.

I'm presuming we should refer to theirs. But we can't do that if we don't know what they're thinking.

Come up with some structure or at least bullet point outline early on, then we can cut down on the wasted work being done in multiple places.

>> And I think there is a pretty -- so standards group has a very solid draft. The framing group has a pretty good outline that on Friday had a discussion.

Now, neither of the co-chairs were there for that discussion so there is probably some room to revisit that.

Also, I want to flag something that Art mentioned that's online and if we have time we could probably even visit which is terminology.

There is -- they have sort of done the first step of saying hey, what are some things that we should define. And also speaking to one point that Duncan made earlier there are also some things that we just want to try to avoid. There are terms that for whatever reason are going to sort of set off alarms and distract from our efforts. So how do we choose our language carefully.

Other things that you think we as a group should try to touch base on moving forward?

I want to sort of take you back to this morning when it really was impressive to see convergence for the minimum viable inventory model that I think had some real power of saying we can achieve this, it meets a lot of the use case work, it fits into the standards work, we're trying to build it today. Duncan.

>> So to Josh's point earlier on -- my point earlier of hey, let's focus on phase one to Josh's point of hey, let's not forget phase two and beyond, how do you see the phase two and beyond either in these documents?

Is there a separate document of just for us of hey, we kicked this can down the road, put it in the parking lot here? I want to make sure we have a down the road.

>> That is a fantastic question. It's like you know the agenda.

So there are a couple of things which is, one, how do we want to address things that are outside the scope of MVI, but are still reflect work that we've done?

And I think that's the precise way to capture it, which is each group -- and I think in particular we're talking about the framing group and the standards group -- can say listen, we've talked about this stuff and it can be useful, but we're going to be addressing this later and here's what we know about it.

And I think there is even some further polish that can be added on it, right? This is known hard problem and will require outside work beyond the scope of this versus this is important and we're going to get to it. So let's take the high assurance use case.

We can lay out hey, here is the stuff we though about it and here is how we think we can do it and we're going to finalize it very soon. Yes?

>> I would propose leaving off of what Josh said before that we just -- we create a backlog and define the second sprint as being in a certain time frame.

>> Saying what, just to say you want to sort of define the fall schedule?

>> Define the fall, yeah. And then we will work on them in priority order, I'd say.

>> Well, the other thing that I want to make sure that is on your radar because it's something that a bunch of you have come to me about is the awareness and adoption side of it.

I think NTIA has been criticized in the past for saying we wrote a document, yeah, it's on a government website, go use it. We're industry friendly so industry go do all your magic thing and prove us right that industry can solve all of this stuff.

I think this is something that is going to require some coordination to promote.

So what I would like to do as we get into this is maybe spend a few minutes talking about what awareness and adoption looks like in general. Because I think this is going to require a bunch of ideas and have those ideas turned into a strategy, right.

I think this is something that is going to require someone -- a bunch of people mentioned global coordination. This is something that has attention around the world, and has lots of points where we can try to both drive interest and inspire demand.

And I know a bunch of you have thought about this problem.

>> During the CVD, you had an adoption awareness working group, they did surveys to capture sentiment. And I thought it was pretty good. And I often refer to the survey results sometimes when I'm trying to sell someone on adopting a disclosure program.

I'm not sure if you want another group for adoption awareness or not. Secondly, I think a couple of us should do a global world tour like a rock band and just --

[LAUGHTER]

>> No, just kidding about that part.

But there may be some natural watering holes or a calendar of events throughout the year like First, like this, like that, some of which we've missed already. But there may be some appropriate venues to try to deliberately participate in once we know what we are evangelizing.

>> Let's try to capture some of what was just said.

First is should we have a working group that is explicitly focused on awareness and adoption? And that can be something that we can sort of slowly spin up as various folks are doing that.

Or, is this something that we should try to coordinate in some other fashion?

>> I think the answer is yes. The question is when. Because I don't think we should start that before we have the thing we're adopting or we're going to do our usual collision and stuff like that. So, I think we need to plan for it. I think we've got to be a little careful on cart before the horse.

>> Except for the fact that on the CVD one the inputs from the surveys about what do you want neither fear from disclosers or whatnot was vital input to the final product.

>> And I don't disagree the calendar is happening regardless of when our output comes out so we do have to deal with that so I agree.

>> I think maybe with all of the interviewing that's been going on with the use cases that that is almost like an alpha version of outreach and communication.

And so maybe think about that because there's contacts, there could be calendars.

>> And it already has a multi-sector perspective.

>> Yeah.

>> Which is going to be -- that is a really good idea.

>> Except that it's --

>> I agree. And it is part of our strategy, right?

And we're talking to the choir, we want to get outside the choir a bit, right, for the adoption and awareness. These are the people who have already pioneered. We want to find the people who haven't started yet.

>> Yeah, sure, yeah, absolutely. Just broaden the concentric rings of the audience out instead of replicating the process.

>> And further to J.C.'s point, if we are talking about a sort of version one and beyond, the sort of version two is going to be work that I see the framing group and the standards group pushing forward into the fall. Whereas, the use case group I think they say we've done this qualitative research, folks can enter and exit different working groups.

The leadership can change, but I think the institutional knowledge is going to be a very useful starting point as well as the framing that you guys developed, the supply chain to help identify what are some of the leverage points that we can use. Duncan and Les.

>> Tracking on Josh's point of we're peaching to the choir and we want to get beyond the choir, I think one of our aspects needs to be to get at I'm going to say the competition. I don't know any other way to say it.

I don't think it's the goal of anybody in this room that we want to come up with some new standard, some new regulation that we're all writing. Trying to do this in an cooperative NTIA let a market drive fashion of hey, let's all agree, let's do it and then prove that we don't need international standards in this area and regulators doing this and all that kind of stuff.

So if we want to avoid that, we have to take that into account in our audience is my point in our how we choose to do this.

>> I do want to say since there are cameras on me that NTIA is completely in favor of international standards.

>> I do, too. I didn't mean it that way, I meant we should be good enough that we don't need to do that.

>> No, and I think the understanding the economics of it so that we can say hey, we've got these international standards, let's use them for this is going to be very powerful.

>> So I say, yes, too, I'm in favor of some type of work group or something that is a fan base for us.

I'm not up on the other industries because this is supposed to be industry wide. We have been focused as a proof of concept more on the medical.

Are there entities in those that can bolster that? For example, you had Seth sitting next to you most of the day so we do have FDA pushing us on our side, so there is a lot of interest in the medical side.

Is there any in the other industries that can help with that?

>> I think you're asking me -- and he's not a regulator.

There's a lot of interest in the defense Federal Acquisition Process. There's interest in the UK Code of Practice for -- there's a lot of pioneering work in automotive ISAC. So not government, but the ISAC.

And then similarly, the Financial Services Sector Coordinating Council, or FSSCC or and the financial services ISACC has already written a couple of papers on this that are several years old now.

They did it more to -- they did it for a couple of reasons but there is some mature thinking there that we could maybe borrow this from. They basically sold security hygiene as productivity and operational performance boosts successfully. And we might be able to do something similar. So there is no single answer. Each of those markets are --

>> I was going for more of a -- is there agencies? I understand to push these things like the FDA is trying to do on our side.

>> Well, I think even as we drill down to agencies, this is something that as a different part of government hears about this, they all get very excited. And so we spend some time talking to our colleagues in government.

But the real power for adoption comes when, you know, there are a couple of big energy or folks who play in manufacturing for the energy sector, oh, we know that things are coming down towards us, let's get in front of the problem.

>> Right.

>> And when we can take those early adopters and leaders and have translators who can help share the good news, it has been very useful. Somebody who is an expert in energy.

>> My name is Kelly Collinane, and I work for New Contact Services, and I represent all of our electric utility clients.

And we are working out a lot of these types of projects both at an industry level with our government partners, specifically DOE. And these are things we are starting to talk about.

So not nearly as -- as developed as the healthcare industry, but we're kind of in that crawl phase right now.

>> So are there other sectors that folks want -- sorry, we had a computer freeze which I guess it has been awhile since I have seen a computer freeze before.

The -- so are there other sectors that we want to sort of reach? We've got finance. We've got energy. We've got healthcare.

And I know, by the way, that the healthcare sector coordinating council is interested in looking past just medical devices to the broader space of healthcare software, which is kind of all of software.

And we know that some folks in the software, the general software space are just interested in this idea. Art and then Duncan.

>> Just a brief comment. I don't have a good sector to recommend, and I think sector specific approaches is a great way to both push adoption and do proof of concepts and sort of get things rolling.

My suspicion is pretty quickly software becomes software. All of the sectors use Lib whatever and Linux. So pretty quickly we have to get the traditional compute all software sector to be engaged in this, I will just note, yeah.

>> And I've done some preliminary outreach in the DevOps and Dev Seg Ops world. This message resonates incredibly well in that community.

[OFF MIC]

>> Probably the most excitement I have seen because they are looking for what can they fit into their incredibly fast build cycle that solves having someone to do the thinking for them.

And so they said oh, we can just have the data there and then use some other source of intelligence, and then we can sort of, you know, increase our pace. J.C. and then --

>> I would sort of echo but then flip the coin around.

There is incredible enthusiasm for DevOps because everyone in DevOps gets to start with a clean sheet of paper. And so they can have all of the modern engineering practices and the GIT and version control and like it is the easiest part of all of this to solve. And, frankly, solving it is becoming commodity.

Not withstanding huge amounts of venture funding going into it. The hard part is for, you know, a medical device or a legacy system or something on-prem. And that is the nut that it seems like we are actually starting to crack.

So it's almost like don't -- don't take coals to Newcastle. I think those folks are going to get there whether they want to or not. GitHub will do it for them.

>> Right.

>> And let's just continue to focus our energy on like solving the tough problems which we actually have a shot at solving.

>> Right.

>> So on your industry list, just because I consult with them some on the issue, but many of you in the D.C. area know the public transportation has been doing some of the same.

So Josh mentioned in transportation the auto industry, but sort of the public transport and train industry has been looking at some of the same issues related typically or almost like DOD providence issues but similar in that regard. So that one would be one that I would recommend.

And two, my career has been mostly in internet security doing cyber security. So I would recommend both -- obviously, the whole telecom industry, but more importantly the security industry itself. I think we are probably the most blatant at being barefoot cobblers children as anyone is.

>> We have one security vendor who actually does S phone in the back.

>> Yeah, one. Yes.

>> Jim.

>> If we're trying to identify industries, we might look at OT or, you know --

>> Does Siemens make other things other than healthcare devices?

>> We actually do a few other things, yes. But ICS is an area.

>> And that may be something to drill down on is the organizations that have very large product families. I'm looking at GE there as well. That touch on these different sectors as a way of sort of saying well, how hard is it to leap from this product family to getting -- you guys have done the hard work, how can your colleagues take advantage of the hard work you've done inside an organization?

That could be something that would be very valuable to document because we could sort of sell that to other companies that have a bunch of different cross verticals.

>> Another way to advertise or get this out, an example that is helping us on the manufacturing -- on the medical side is the MDS squared form.

So in that group we have included SBOM as part of the questions. And now it has become a lot of customers are asking for the MDS squared form today and wanting the new form around the world. It just isn't just the U.S.

So if there are other places or things that are -- that you can partner with, that actually bolsters the SBOM as well.

>> Thank you. J.C.

>> Another area is the whole smart cities domain because, you know, my global search replaces anyone who says smart just paste in vulnerable. It's like a vulnerable grid, and a vulnerable, self-driving system and all that.

They're procuring like they want the trash trucks to talk to the trash cans. And I mean there is no -- there is no assurance around any of this crap.

[LAUGHTER]

>> And it's -- it's -- there is a massive surface. And so I think there might be -- it might be a really good opportunity to engage on the sort of it's industrial but sort of a Greenfield but rah-rah but nobody cares but everyone's going to get killed. So that would be a good one.

>> Smart cities is a great example in that it is more of a funding mechanism. And that means there is a few more centralized points to influence and do some outreach for it that can trickle down across a whole bunch of different types of companies.

[OFF MIC]

>> Yeah.

>> I almost want to say this without my mic on first. This might be jumping ahead to the list of topics we don't want to talk about so I will watch your face as I say it. There have --

>> It's 4:00.

>> Just before and during RSA I have been approached with renewed vigor by big insurers. Because, well, a tiny anecdote you and I have spoken about is the lawsuit between Cadbury's parent company and their insurer Zurich about is it an act of war because it was not Pechia and there's a lot of people saying how strong is our insurance policy towards cyber, and have we really thought through our underwriting.

And as they're looking for new ways to do this, I have a hunch that a quantifiable measurable thing like SBOMs and hygiene are the practice being present or not could be instructive to their renewed focus.

So did you cringe when I said that? I can't tell.

>> I didn't. And so for those who don't know me, I spent about 15 years thinking about security and economics and so I have some opinions that I won't share about insurance because they're not NTIA opinions.

But I think with ongoing efforts like the Marsh initiative of sort of doing some security tooling work, I think that's -- there are some active points of the outreach that we can go for.

I want to put one more thing on the table as we all sort of get slightly punchy heading towards 4:00.

Something that Art brought up earlier, which is very few people say the future of software is on-prem. And as we think through the Cloud side of it, of course, it's very vague, right, this covers everything from pure SaaS to API infrastructure and then going to all sort of fun nuances of I've got an app and it talks to a thing.

Is there anything that we want to say to it or at least to put a marker down about how we talk about it?

>> I propose it not be phase one.

[LAUGHTER]

>> That is the joy of having a phase two approach.

But we've already said we are going to put -- say certain things about phase two. And it would be that oh, by the way, down the road we'll talk about the Cloud side of things.

But it's more of if anyone had a thought this is now a good time to sort of start getting everyone else's brain working on this topic. Bruce?

>> So the SBOM has different benefits.

>> Put your mic a little closer.

>> Oh, sorry.

>> There you go.

>> The SBOM has different benefits depending on whether you're a supplier or a customer.

The supplier, if it's Cloud or not, has the same benefits. And so, you know, if you focus on both the customer and the supplier benefits, then Cloud at least has all of the benefits of the supplier today.

>> That's a great point. Everything upstream of the user is going to have that, yeah.

All right. So let's recap a little bit.

>> Actually --

>> Yes.

>> Actually, before we recap, when do we get to the sort of retrospective how can we improve this process part of the conversation?

>> Experience has shown that any time is a good time to criticize.

>> Because --

[LAUGHTER]

>> -- one of the things that I heard earlier is that we want to bring a whole bunch of new people in to this effort to have them, you know, provide their insights, to review documents, that sort of thing.

I think a lot of the groups have actually done a really good job at taking notes and capturing artifacts and that sort of thing.

But if I were an internet user sort of from the outside looking in, finding all of that stuff can actually be a little bit challenging.

Is there any way that we could actually improve on that? You know, there's a lot of long-running, you know, documents on like GoogleDocs. There's lots of long-running notes.

Could we post links to those on the website? Anything that would actually help people sort of come in and understand where we're at.

>> I think --

>> Any thoughts?

>> I think that is a great idea and certainly something that probably different groups based on how they have documented may have different approaches on hey, if someone's coming in, here's a 70-page GoogleDoc and if you read it from the top you're going to think we're idiots because it took us 40 pages to get our feet under us.

Not saying that -- what does the introductory process look like? How can we -- so, for example, this is something that we can look at the NTIA created web presences for

the working groups where we can try to capture some of that stuff as we go. I think that's a great idea.

>> And also to make sure that it's not lost to history.

>> Yes, that's true. If only there was some sort of heritage project for software.

>> So one thing when we say this is always what can we do better, you also have to include what do we want not to break that we have done good.

I want to commend everyone for having the documents for this meeting on the website as the meeting started. That's a first for us, I believe, and I really think it helps a lot.

Next time maybe if we had them 24 hours before the meeting it would be even better. But I do think it was great we did that.

>> Yes. So that gets us to Duncan has been great at teeing up the next agenda item, it's fantastic.

I would like to put the next two meetings that we're going to have on the calendar now.

I think there's incredible value about having all of us in a room together. On the other hand, I know that flying is a pain in the ass and most of you already do it way too much. Which is why we have been sort of having this rhythm of every other meeting being a virtual meeting.

So we'll have slide share and try to have some discussions. Discussions sometimes a little harder, but last time the one we had in February I thought was fairly productive.

And so in June, we have -- I have heard a call for late June, especially if we are going to try to have some deliverables then.

And then what I would like to do is have an in-person meeting during the first two weeks of September. Probably in Washington, unless someone has a very strong and immediate proposal of where it can be hosted.

>> Hawaii.

[LAUGHTER]

>> Do you have space?

[OFF MIC]

>> Duncan?

>> On the late June, I guess it's a question do you foresee the meeting being after the documents are done and then sort of what's the purpose of the meeting?

Or is the meeting to basically I have the document and let's draft them. I'm not sure it should be late June if we want to have the thing out in late June because I'm worried we will create them all the day before the meeting and then we won't actually get them out.

>> Fantastic points. And I appreciate that, and that gives us an option to say well, if we decide to give ourselves -- we want to have the shareable drafts, this gives us as a community one last chance to sort of share things and kick the tires internally.

So that speaks to sort of saying hey, let's try to get something on the earlier side of June, and then maybe the -- so first is the second week of June. So this would be the third week of June. And that way we could sort of have that.

Again, I'm going to sort of encourage a virtual meeting, but if folks think a face to face is more effective, I'm happy to sort of hear that feedback.

Anybody want to come back to Washington in two months? In June. It's lovely.

[OFF MIC]
>> No.
>> No.
[LAUGHTER]
>> I don't know. Ask the guy from Texas how bad the summers are in D.C.
>> This would be virtual?
>> This would be a virtual meeting. In the past, we've done it as sort of three hours from sort of 1:00 to 4:00. So for folks on the west coast, it is not quite as painful as a 10:00 a.m. For folks in Europe, sorry, but you're not watching now because it's already too late. So we will try to work on that.

And then the goal there is to have them -- we would have the drafts in advance because I think Duncan has a great point. If we want people to show up and actually give feedback, they need to have had time to read them.

>> Sorry. May I suggest virtual meeting the week of June 24th. Draft documents due internally to our group, the larger group two weeks in advance. You have two weeks to comment and come to the meeting with your strongest set of most important comments on everyone else's work.
>> I think that works well. We'll do our internal work on the calendar, but nothing --
>> Something like that.
>> Bruce.
>> Can we -- if people submit, you know, comments, can we cover those first by the, you know, the authors of the groups.

So if you are going to send something out two weeks early and people get comments in by let's say a week later, it would be nice if you were prepared to address those.

>> Great. That is the advantage of the two week is it gives us a one week barrier to say if you get them to the group within seven days, then the group will already start to think it through. That is even better for feedback. Thank you.
>> And we don't have to deal at the meeting with what we can't settle face to face or hopefully it will be nothing.
>> Or the heartless inconsiderate people who didn't bother to do their feedback in time. There are like three of them in the entire process, and I'm not going to make contact with anyone.

And then the second thing is a face to face in early September. Can I ask someone that I sent an e-mail out to look up?

I threw out a couple of dates. I want to say there was September 10th. Mainly to say it so we can circulate it. And hopefully folks know about the most important conference in your field is happening that week, that is something that we want to try to plan around, if possible.

[OFF MIC]
>> They canceled DevCon, sorry.
>> You suggested September 2 or 9.
>> Thank you.
>> In your message.
>> September 2 or 9. I believe both of those are --
>> September 2 is Labor Day.

>> Oh, the week of September 2.

>> The week of. Not those dates, sorry.

>> And I think -- and I think -- hang on a second.

Does anyone know of major events? Obviously, there are going to be conferences all the time. Does anyone know of major events that are going to be happening either of those two weeks?

>> The second week is my vacation so you can avoid me.

[LAUGHTER]

>> What was the (indiscernible).

>> Celebrate -- who doesn't want to celebrate, Washington, D.C. known as the city of romance. It's --

[OFF MIC]

>> The week of the second is good. That is Labor Day week.

>> We're not going to be here all week.

>> That's true. We will do some planning. This was sort of your chance to give us that kind of feedback. And I think that hits most of what we wanted to cover at this meeting.

And I just want to sort of try to do a little recap here because I'm kind of blown away by all the work that's happened here.

If you go back even to November and think of where we were, we are just now -- it is very easy to look and say oh, this is what an SBOM is. And it seems like it's pretty easy to imagine a world where we can do this without too much trouble.

There are always going to be edge cases and always going to be complexities. As Diane said this morning, if this were easy, it would have been done by now. But you guys have tackled some pretty hard problems.

And so what we're going to do is we're going to take this framing around the minimum viable inventory identity, minimum viable identity, the MVI.

First, we're going to define what MVI means. And then we're going to say this is what is sketched out in terms of the what, the high level sort of overview of it. The why, how it can change. You know, how we think about software risk and quality all across the ecosystem. And then the how, documenting here are all the tools that we have, and also here is how you can do it today.

This is kind of the core. This is kind of an exciting point to be at this process because we're now actually can sort of say this is what not the end look looks like but what the path to progress is really going to look like.

So unless there are any final comments, I want to thank Megan who has been doing all of the work to capture what we have. We'll be posting these notes online. This video will be available online in a few days.

And the only thing left for me to do is to give you all my heartfelt thanks. This only works because you are passionate and hard working and are willing to find ways to bridge your differences and figure out how to make this work. So I want to thank you all.