TRANSCRIPT FILE

JULY 19 NTIA - PART 3

>> I just want to remind those of you who are listening or watching along that we really want to hear from you. So on the call bridge, and if you don't see it, it's the number right below the web screen, hit star one and you will get our question queue and we will be able to loop you in. So I said before lunch break that I think it's good to focus on scope, but before we go there I know that some of you had some very good conversations over lunch and managed to come up with some new ideas perhaps. So I thought I'd do a quick check and see if there anyone who wants to add something new to the table that hasn't been raised yet that we should fold into our conversation moving forward this afternoon. Yes, and can you remind us who you are?

>> Sebastian Bentall, NYU centers for cyber security. We've been talking about kind of a bill of materials document or format and we've been talking about, okay, what about process, what about business processes? And at one point what came up in conversation over lunch is that you can have any syntax for document that you want but the semantics really depend on the process that generates it and the processes that consume it. So really we are talking about the same thing. If we are standardizing processes then we are immediately talking about automation, scalability. So there's no contradiction there. The other thing I want to say is just to contribute to, you know the metaphor wars, personally I'm anti-metaphor. So the whole concept of a bill of materials for software which is the most immaterial thing we could think of is already getting us into weird analogical territory. And if software is a result of a human production process, if software is people, if software is process, it's going to be process all the way down and all the way up. I just wanted to note that.

>> And I really like the term you coined of the metaphor wars. Where were you? On the phone we have Jeffrey Snover from Microsoft.

>> Howdy, can you hear me?

>> We can indeed. Thanks for joining the conversation.

>> Great. Howdy I'm Jeffrey Snover. I'm a technical fellow at Microsoft. And I really have two points I want to make. First is Microsoft and all the other vendors in the industry are stakeholders in the success and protection of our customers and our communities. So I think this software bill of material effort is very very important. The second is as technical fellow I've been chief architect for both products and platforms. And there's a difference. And I think that difference is relevant to this conversation. With products we deliver solutions but with platforms the goal is to enable a set of solutions that can be delivered by others and can be delivered by an ecosystem of others. So when it comes to the software bill of materials I really view it as a platform because it does not deliver safety. It enables safety. And it does so by allowing others to integrate

information like vulnerability assessments and what this does is it then empowers the people who have the software components, it empowers them to become safe and allows them to identify potential risks and then potential strategies to mediate or address those risks. Some of those solutions might be, I'm going to byproduct A versus product B but more likely it's going to be things like I'm going to press that vendor for a patch or implement a compensating security control. There's lots of stuff that isn't going to be patched. Vendors that have gone out of business etc., but you can still, if you know what your risks are, you can often address those risks through compensating controls. Firewall rules. Disconnecting things. Ensuring you've got good auditing etc. So those are the two points I wanted to make. Thank you.

>> Thank you. I appreciate that. Any other observations, ideas, thoughts you've had over the last hour that you want to put over the table as we work thinking about scoping?

All right. What I wanted to do is pull up a slide that Jim offered earlier that I think was a very good scoping. And that means we are not going to have the notes taken live and that will give me an opportunity to also thank Megan Dozier. For those who don't know Megan Dozier is part of the cyber security team at NTIA and she does a lot of the national security work that hopefully you don't know about. But has also been instrumental in our multi-stakeholder processes. This might be a useful straw man for thinking about sort of the scoping question and the definitional question. And whenever we are talking about security people also, and we talked about this earlier, I can't remember who raised it, but this notion that there's going to be context specific issues. Perhaps things that are, where the risks are a little bit greater where we may need to think about it slightly differently, or it could be useful to have a single notion that spans most of the sectors. And so wanted to turn it over to the body to say, is there, does this graphic, if we are saying, when we talk about what is a bill of materials? What do we want it to be? Can we use this to sort of drill down on where you would like this to land?

>> Well, since I want to make this as focused as possible, I personally would like to have it include all third-party external components to the vendor's products. Sort of in between the all and the [text] service row of components sort of thing. But I do believe all the time issues there are viable, doable and necessary and should be included as well as the breadth issues, or the naming and the component related information. I think component naming is going to be the harder part of this. The automated format is not going to be as hard as everybody thinks it's going to be.

>> That's a great point that the component naming, and we were talking about this a little over the break, is a problem that both [SWID] and SPD] shared. That everyone has this challenge. Yes

>> I wanted to, that the 1 inch cube with the first three surface sub area [naught] right now, getting there would be like a step forward. For us to either do coordinated disclosure or understand whether these offer larger project rather than subproducts. So

starting, if treat those if they are 1 inch cubes would be a huge progress from where we are today.

>> I think that in breadth there's this business of dependencies that are not components. So, if you want to install this particular application, you know, you also need to be running, or it requires, and they are not necessarily folded up under, but they are prerequisites for. And so I guess there's a question about, you know, what are those kind of associated applications, packages or infrastructure pieces. Because people can update their core software, but that doesn't necessarily guarantee they are updating at the Apache that is running alongside it. And so I think that's one of those discontinuities that creates gotchas. So how do you understand the stuff on a system level. Not just on an application level.

>> Can you make this concrete for us and I'm going to speak

>> I would say kind of associated or, associated dependencies or dependencies that are not components.

>> Are we talking compiler flags and things like that or...?

>> You know, you may need a particular database. Or you know, so SQL, right? So you know there are I mean especially in a web services architecture, there are components that are necessary to be present in the same system. And so I don't know how we really deal with that because people can have an initial install when they buy something but then they only update the core application. So there's all this peripheral stuff that is a dependency that needs to be understood as part of the same system and I don't know how to deal with that. But it's definitely something that should be part of the situational awareness of what you are dealing with.

>> Josh?

>> So I'm really intrigued by this model. It makes me want to go dig up some old notes. There are some parts that are snagging me and I can't put my finger on. I was going to propose that maybe a working group would be to flesh out kind of like a turn of the crank too to something like this but I'm also intrigued at something you said about what is the unit of response time. So, something like what is in it probably needs to be more standardized across sectors, but maybe how often you do it is the way you differentiate yourself as the maturity level. This is one of the ways they rank hosting centers is like, can you do a patch in production, patch with downtime, you know etc. etc. So I don't want to codify this as truth at a glance. I'm snagging on a couple things. I will say though that known vulnerabilities tend to adhere to versions as opposed to this idea of a component name ID. Licenses adhere to project, vulnerabilities adhere to versions. Discrete versions. So, there may be natural ones and when I said let's do a survey of existing practice at banks or in regulated industries, one of the reasons is I bet we can map a heat map as to which altitude on all three of those existing practices live on.

>> Tom, you had two fingers?

>> I wonder if there's room, this is thinking out loud, but I wonder if there's room for trade-offs along this space, such that if you cannot for whatever reason provide minor version information or patch level information, you then should provide snippets for comparison purposes. An edge case that has come up in discussion was the vulnerability that ended up being traced back to stack overflow answer. So it had been copied and pasted into knows how many projects throughout the world.

>> Further thoughts on scoping? What do we mean when we say S Bomb? Jim, this is your slide. Can I put you on the spot and say is there a, would you draw the volume on this set of space?

>> Yeah I would, picking up on what Josh said, I think it may actually be that two of the dimensions get fixed and the third dimension is the one that is allowed to vary and I think Josh was suggesting that perhaps it was the time dimension. And that might be a useful model for us to work on.

>> Okay. Kent?

>> Just so I'm understanding here, the time dimension from a vendor perspective is when I publish software. So when I send something out I make a change to my software I should update that file for whatever reason right then and there so that there is an accurate depiction of what's on that system when it is installed or in that package when it's delivered. So from that perspective, at a patch, when a patch occurs, yes absolutely. Any updates of any type, a hot fix or the like, absolutely. At a major version change or a minor version change, absolutely. That's not real time. But that's accurate reflection of what I'm putting on that device.

>> Just to clarify...

>> One, two...

>> I just want to respond to that point. I think the time dimension isn't necessarily when the vendor makes the change. It is when the vendor makes the S Bomb available to the world.

>> From the standpoint of at least how I have been looking at this, S Bombs are created as part of your build process. It's not something that is different and distinct. So there is included in the package that goes to the customer. It is included, there's multiple potentials here. One for what's in the install package and one for what's in the deploy package on the machine so you could actually have two S bombs on a machine. One that is more holistic and one that is runtime. And as such they may have slightly different information in them. But that S bomb goes the same time the product goes to the disc.

>> We've got one, two, three.

>> All right and I should of been clearer. I don't know if they have it handy but if you remember my three columns like the inventory itself is a build time thing and basically

the cadence that Phillips does for the MDS 2 reports is every time new software is pushed a new S bomb is pushed. So it's a release cadence. Column three there is they've done some sort of triage to say here are the known vulnerabilities and they don't want to update that in real time because new CDs are reported every day so he's opting for a quarterly refresh of his column three, you know, risk attestation but he doesn't have to do that one at all because this is a voluntary best practices for column one, which is the inventory of parts, not necessarily column three of a triage of the potentially exploitable vulnerabilities

>> Right. If we are able to sort of specifically focus on the S bomb itself and the transparency from the vendors then we can build a lot of tools on top of that information. That will be beyond just vulnerability focus. I can see support issues as well, you know if somebody has a problem. Tell me what's in your S bomb file. Run this little program. It shows you exactly what's in the file. Makes it easy for support, instead of trying to dig out from the customer what it is they are actually running on their network or trying to find contracts to make sure they have the right information.

>> Jen?

>> Jen [Addis] from [Reppert] seven. I have probably shocked the shit out of most people in this room by being quiet for most of the day today

>> And for those of you who are curious...the favorite did win.

>> I'm sorry yes , anybody who [fair games that] more for you. I have a question that's probably a stupid question but I'm going to ask it anyway because I'm apparently here to embarrass myself. Do people issue release notes? Is that a thing that people do or is that just [rapid 7]? other people put out release notes when they put out an update to the product generally speaking. I guess my question is this why is is not part of the release notes process, like providing the update is not just a standard part of that process.

>> A good question. I'm going to give Kent a very quick answer and then we will go

>> Well, release notes are human readable and they are not format and structured and we want machine-readable so that we can automate for vulnerability management tools or other security automation capabilities.

>> Bruce, and just as a reminder if you're listening on the call bridge hit star one to join our conversation. Our operator is sitting by.

>> I would agree with the release notes just answer that point, but the point I wanted to bring up is there's deployment options that happen on many software and a lot of these things won't get deployed and if you want to know, so for instance you may have the Swedish language version instead of the English language version of something and only the Swedish language version is vulnerable. So part of this has something to do with the deployment options and there's many products or some products at least where

you can install different versions and it will pick up different versions in the same source to get you there. And I think Java was that we at one point for example. So that's a consideration if we are going to be comprehensive here. That should be put in.

>> I have a two fingered response.

>> Just to unify that comment and the release notes machine readability comment, it would be really good to create some either carrot or stick or best practice that release notes actually are machine-readable. Because the only way to resolve the deployment issue is to have some kind of explicit and formal description of some vulnerability in some deployment in a machine-readable way so that people who are parsing machine-readable release notes can understand what's what. And it would be of tremendous benefit. So as we talk about formats, you know beyond SWID and SPDX can we come up with an industry perspective with some kind of shared understanding of what a set of release notes looks like so the customers can act on that information more efficiently.

>> CSAF

>> Sorry, can't is a just a one off or something that we should…?

>> There's standard formats for security advisories that can easily be leveraged into that type of thing. That's a bigger push for vendors to update I think and most people to do. Release notes have not historically been in any specific format. I don't disagree with you. I think it would be a great thing if we all started using it. But I think that's beyond the scope of what we are trying to talk here.

>> Chris?

>> Especially with release notes were talking but on premise software we are shipping delivery of something to the customer. What about SAS, what about an API. Most people in this as we get to the real dev ops world when you have API you are updating every day. One day I'm a consumer of that API. I might be vulnerable because of a component there. The next day I am not. So I just don't think the release notes model fits into that world.

>> And you just put something new that I don't think we've talked about, which is non-on Prem software.

>> He did have it on his slide. Some thing to talk about.

>> I think what we are talking about here it's already a common practice to include links for example your bug tracker that has a list of all the issues and that may actually be dynamic anyway and it's out there for posterity for somebody to come back and take a look at what was actually fixed in this particular version. Right, so in that sense the bug tracker issue is basically machine generated at the time you want to produce it if you have a system that's producing the bill of materials and you should for all the reasons we talked about, attaching that year otherwise human curated release notes should be a no-brainer, just something you are basically already doing.

>> Yes?

>> So going back to my earlier comment of starting with the inch cube is really if you did start with the very minimum of all three dimensions, could doing time dimension on a live is not very difficult I feel like. If you started with something very basic, just saying can I create this software today to find out what components have been added as a differential should be very, not very difficult. So I feel like if we start with something very basic like that to target, the time dimension is one of the easiest ones to solve. You can always create, if you had a template, say whatever [EXON] looking template or JSON. I'm not going to get into that argument. But you get into some format and then you're able to online query it to find out, you can solve the SAS problems, the past problems, all of them, but live querying to find out what is the version of today's come all the components sort of

>> So this is, keep this data at some fixed point server side on the vendors in the vendor's website?

>> I'm saying give interfaces to query this on every software that you deliver, you have all the components already identified now. Just give a way to update it on the software if only one component was updated when you query it you basically get all the information about open SSL version is this much higher than where we started.

>> Bruce?

>> I think we should decide if we are going to limit this to on premise or not. I mean if we are going to do both, that's, they are very different. And I think we will make a lot more progress if we go with on premise and then later maybe extend that to clout or whatever you want to talk about. If you're going to do cloud you should be able to just have an online API that says give me my inventory of what I'm running. But that's a long ways from where we are at right now.

>> Important scoping question.

>> I have to agree, Bruce. I think it makes it easier and better for us to focus and make some successes first and then move past that.

>> Okay focus and on Prem, I want to allow someone to argue and say there's, we should include the scope of having SAS cloud, something in that space. Anyone who wants to sort of argue and say that we should try to include that?

>> Well the world is hybrid, right? Like your IOT device talks to the cloud. Your mobile app talks to the cloud. The majority of development these days is both. So I don't know how you can just ignore the back and that might have a vulnerability that's exposed through an on premise piece.

> The cloud native companies are also much more like Sunil was adjusting where this is a byproduct of this STL and I was whispering to him like micro services are these

complex matchups where you don't even architect the software. It's just some interactions they could machine generate their machine readable build materials.

>> Okay yes?

>> Thinking about cloud software services stuff might get us into the headspace of imagining S bombs as like a process automated dynamic thing as opposed to a static thing in the first place and that might elevate the discussion.

>> Okay, thank you. That's a good point. I want to go to the phone. Steve?

>> Hi, Steve [Spring]. I'm one of the project leads over at OOSP. And I just wanted to make a few points that I think in order for an S bomb specification to be successful I think it needs to be simple. We really need to make this effort successful in the free and open source community. We want it to be adoptable. I think we want it to be expandable and let the commercial vendors innovate and compete on their differentiators. Initially I think we really should keep the focus there a narrow. I also want to, I'm not a big fan of the S bomb because as we've heard earlier there are vulnerable hardware. And hardware is shipped with IOT devices. And I think that should be part of our vernacular.

[Laughter]

>> Sorry, the comment you missed as you might have helped coin the term H-bomb and I think there is consensus that we should avoid that one.

>> I agree. And my third point is really about being lifecycle agnostic. And whatever specification we come up with I think really needs to have a decentralized scope as really part of its core.

>> Those are fantastic points. I'm not seeing folks, other than the point that understanding cloud development practice is going to be useful, not a lot of people seem to be saying that we want to from the start actively try to include non-on Prem software. And I think one way to cleanly divide that is if there are folks that are interested in off Prem cloud SAS stack things that can be a particular separate working group. That's great. I think that's a great way to make progress. But I'm getting the sense that for the folks that are emphasizing let's do this from a proof of concept, start with the easy things first, we will focus on on Prem software as well as some IOT component or medical device component. Further thoughts on that? May I request you put your mic on?

>> Sort of irrelevant, I was going to ask if we could see the list on the screen.

>> Great. We are going to go back to the notes. Okay thank you. That is the, Eric would you introduce yourself

>> Eric [Winer] from Cisco. I was going to say that if you are going to accept this idea which I think makes sense of starting small testing and then seeing what's valuable moving forward there was a comment earlier on about trying to figure what problems

you are going to try to solve. So I think that figuring out if there's a core problem that you think you can solve with this kind of an approach, testing it and seeing whether there are other places that it makes sense to expand that model and in other places to solve similar problems.

>> Good point. All right, yes?

>> I was going to say I think focusing on the on Prem first as opposed to the crowd helps clarify I think why most of the room really wants to do this. Which is when you receive something from someone else you don't inherently know what's inside it. So that bill of materials or the food label helps you understand the ingredients, whereas if you had the ingredients for the cloud and it's buried way down inside what are you as a consumer going to do with it anyway. Hopefully the team running that service actually has it and is responding accordingly. And I think that's the difference between these two cases here.

>> You want to respond? And then we will go to Jennings and then we will go to the phone.

>> Which I mean I think comes back to why you're trying to figure out which problem you're trying to solve because you have to need to know who would find this information useful before you decide it's worth trying to produce that information and push it up to somebody.

>> Jennings, who would find this information useful?

>> I would. And I think part of this is also as a customer or potential customer of a company understanding their basic security hygiene. So even if it doesn't help me with incident response and vulnerability management in my data centers I want to know that that SAS provider actually gives a rip about security and actually documents these things. So there's a host of reasons. There's a whole lifecycle management piece that has to be kind of considered.

>> Great. First I want to go to Jeffrey Snover on the phone and then we will go to Kent. Jeffrey?

>> I wanted to say I think the conversation about on premise hybrid cloud is actually masking the deeper issue. I think the deeper issue is supplier, deployer, securer and then consumer and I think where it makes, I will highlight that I think the idea of a software bill of materials from someone who is supplying something gets delivered to someone who then consumes it, deploys it and is responsible for securing it. That is one set of issues. When you then say that same information should be exposed to the people who consume it, whether it is the user of an application or the consumer of a micro service etc. I think that is a very different set of issues and much more fuzzy and complicated and really quite an order of magnitude more difficult.

>> Thank you. I've got a two finger from art and then over to Kent.

>> It seems to me if we are going to get as far as producing the S bomb, providing it to anyone is pretty much trivial at that point. So I'm not sure we need to worry about the distinction as to what anyone's role is. You have it. You can make use of it or not basically.

>> Yeah. Kent?

>> What he said.

[Laughter]

>> We have Kimberly on the phone.

>> I think that the comments that have been made about scoping and the problems we are trying to solve our right on the money. And in that sense is a software bill of materials to inform customers of Z [lib] in the word processor, they can't update Z [lib] they can only update the word processor. Like how much benefit is there in that. While on the other hand we have a very very clear benefit to the car manufacturer who bought a piece of technology, integrated it into the car, the need to know what's in that technology. Me as the car owner I don't need to know that there's a component in that entertainment system but the car manufacturer does and I think those are some of the scenarios of the software bill of materials is most beneficial to defenders and is easiest to potentially test in the smaller scope. It does need the sort of on Prem. It is very very specific health and safety related and then we can take our best practices from that to how can we expand that further. Cars, healthcare. Whatever you were talking about. I think supply-chain is a really really compelling argument for software bill of materials. If we are using software bill of materials to basically push vendors to level up there security maturity for third-party components, I think we are using a hammer when we need a screwdriver and we are taking one tool to solve an underlying problem around what is the tooling, what is the update pattern, what is the vendor culture and responsibility and hygiene around these third-party components that they are delivering to customers. And I think there are other tools we can apply there.

>> Thank you. We have a response in the room.

>> Right, so I think we want to be careful not to fall into the slippery slope of saying users can't defend. You know I think in the case of the hospital the legacy device knowing that there's a vulnerability there you may be able to sandbox it and safely use it. That's clearly not the case in every example but that wouldn't be a reason not to provide it.

>> That's a great point. Yes?

>> I think we just need to make sure we distinguish who the user is because the user is both a secure and the consumer. Right, and just to use another metaphor, you have a food manufacturer, you have the grocery who wants to have organic foods, you have the parent who buys it and you have the kid who consumes it. The kid does not care

what the ingredients are for a bag of potato chips but the parent does. So I think in this case it's really ending at the securer. The bill of materials is probably most relevant for the securer but the consumer is not going to care. They are both users though.

>> Steve Lintner on the phone?

>> Thank you. I'm sort of running behind here because I'm trying to watch the video and then, which runs about 10 minutes behind the audio from my phone. And then by the time I get called there have been four or five more comments since I hit the request. I think the usage scenarios are the critical piece to understanding what ought to be done in this bill of materials space. Assuming something ought to. I've heard things all the way from understanding the suppliers process and getting convinced that the supplier actually has a security process through a user organization being able to defend themselves in certain scenarios can maybe, I'm not sure I really heard individual users defending themselves but I suppose that's a possibility or at least gaining confidence. And I think being explicit about what the objectives is, what the objectives are is just super important to deciding what needs to be done if anything. And one other point I guess two other points, you know a developer you know, producer ought to have command of their third-party components as part of building a secure product. There are lots more about things to do about building a secure product but that is sort of a must in today's world. But getting that confidence may not require may not require releasing a bill of materials as long as the developer has it and is actually using it to stay on top of what's happening with his components and patch them or replace them or stop using them as necessary when something goes wrong. Sorry for the long-winded response.

>> Thank you I appreciate that and forgive me for citing you in this but Steve Lintner in safe code actually I have a fantastic and fairly brief document on tracking third-party components in the software development process that if you have not seen is a great resource. So we've been talking a little bit about scope and I got a sense that there's sort of, we can have some simplification and some targeting by looking at on Prem. I know that a number of people here are very concerned about medical devices and perhaps by extension have some expertise in the broader class of embedded systems. Do we see that these are compatible to think about on premise software and software that's on devices? Are these things that we can think about at the same time?

>> I fear if we don't we might end up with the very thing we want to avoid which is two incompatible formats.

>> Yeah I haven't heard anything that would exclude medical devices or any other devices from conversation we've been having.

>> Excellent. So this is, I think we have heard this morning that we need to think a lot about scoping. I'm hearing that at least we want to start small. We want to take advantage of existing tools and maybe it is time to open that particular can and see what's inside for existing tools. And now I'm going to call out Kent if he wants to. I'm

putting you on the spot but you can decline and talk about how you thought about the existing tools and standards that we have.

>> Okay, well I'm not going to make the open source folks happy. The reality is a lot of what we've been looking at is to use what we leverage, what we can leverage right now in our build processes. One of the things that we don't want to do as a community is try to leverage a lot of heavyweight kind of processes on vendors because the reality is they probably won't adopt them. And adoption is critical to this kind of solution. CPE was not a good approach to naming devices, mainly because it required the vendors to actually do something that was out of the processes. It meant to they had to send that information to a central location, NIST and have that information incorporated into the NVD related information. That never really was successful. So we want to really look at how vendors themselves, software producers, I'm a vendor, so I say vendors I mean the software development community, to really put this as part of their integration and their build processes. So when you are doing something regardless of what we do here it comes out as an automatic artifact of a normal build environment. It's then up to the software producer to decide whether they want to ship it to somebody or not. That's a different story. But they should have a standard format, a machine-readable format that is incorporated into their build processes. So this information is actually developed. The one that we have is SWID today because we use SWID today and other large vendors do as well. Even some smaller vendors do as well. I'm not saying it's perfect. I'm not saying it's the end-all be-all. It's not. But when I talk to the developers about you know, what it would take to incorporate component information they said it would take five print deaths. So you know, that tells me that they are not too concerned about how this is going to be added into an existing mechanism that many vendors have, although most are still learning how to spell it. But I think whatever we are looking at, whether it is SPDX, whether it is SWID we need to come up with something that is reasonably adoptable, reasonably deployable and reasonably lightweight because the reality is we are not going to have the luxury of coming up with something that's going to require vendors to re-implement their build processes.

>> Great. I'm going to go to the phone first and loop in Steve I think he's going to talk about the open source perspective and I also want to just make it clear that this in the room today is probably not going to be where we resolve standards fights. But I think it is useful to help us understand the scope of the landscape and see whether this is something that we can address or at least tee up for fairly straightforward machine translation. Steve?

>> Yes thanks. So I also looked at SWID and I also looked at SPDX and there's definitely some support for the SPDX especially in the open source community. SWID is really not mentioned too much for various reasons. But as an O-OS person I'm interested in security and open source. And I didn't see anything out there. So about a year ago I actually created a quote unquote specification called cyclone DX and it's open source. It's my interpretation of what a lightweight bill of material specification

could be. And it does support, you know, applications, libraries, frameworks. It supports hardware. Being able to specify those as well as licenses. And it absolutely can be integrated into builds. There's a node module. There’s a maven plug, a maven plug-in, there's support for other things coming in the future, but regardless of the specification I think the open source community is definitely open to trying to help and assist with a lightweight bomb specification. Whether it is cyclone DX or something brand-new is irrelevant. But one thing that could be very useful, which, whichever specifications we come up with, is really the package URL specification. So what cyclone DX does for example is it actually includes the package URL as part of the native specification and because it actually does integrate with node and maven and all these other ecosystems, it uses those ecosystems' native package managers to standardize what the resulting package URL could be. And I think that's really really important when we start to care about where these components come from. And how can I then query those components repositories to get out of date component information, for example. So, I think there really is an interest in the open source community. I know there's many organizations that have already adopted cyclone DX, whether it is good or bad is irrelevant, but I think there's a lot of interest in doing some kind of work in the open source community and I'd be more than happy to help with that initiative.

>> Excellent. We will almost certainly be taking you up on that. We've got Brian, then we've got Todd on the phone.

>> So, in responding to Kent I think I'm going to end up amplifying a lot of what Steve just said, but you mentioned the CPE largely failed because it required other people to do stuff, which is a really apply a new name that was not native to what they were already doing. This is still largely a problem within the C/C++ ecosystem that have really old build systems, really old and reliable. I did that a long time ago. But any of the build systems that have come along since like 2004 this is just a native thing. Every build system is already using very specific, deterministic coordinates for how they select and manage their dependencies. So really there's no extra process required in those modern build systems to produce this bill of materials. And further we need to make sure that whatever coordinate system we use is precise enough to carry the very vulnerability data that we are after. That is one of the fundamental problems with the CPE is that it can't. And any of the other ones that we end up having to map to probably will have the same problem. The only way to be absolutely deterministic is to use the native coordinate systems of the various packages and something like Perl actually is a great wrapper on top of that.

>> All right, we've got Todd on the phone and then Jim in the room and then Taki on the phone. Hey, Todd we can hear you.

>> Oh perfect. Cool. Okay so I just wanted to throw out there like there are a lot of approaches to finding components and listing those all out. I mean honestly as a defender or like just as someone who does asset management for all of my IOT stuff if I could just get something super duper basic like an OS version and a minor number and

kind of leave it at that, like if I had just that, that would be head and shoulders above where I'm at today. Like, I know that we are all, we all have some passing familiarity with vulnerability management and doing these scans and knowing which versions of [inaudible] we have an [inaudible] open and all that but if I just knew that this hunk of IOT has Windows XP in it that's a fantastic starting point and something we don't really have today. And so I'm wondering if like it would be useful to start with something terribly terribly basic like that and kind of go from that, or if we really need to solve all the problems first with component versioning. Or if I'm just being very lazy.

[Laughter]

>> We can start small. Jim.

>> Yeah so, this may be one area where there's a difference between software vendors and device vendors, because much of the information that is necessary from a bill of material for a device doesn't come out of the build process pretty comes out of the platform. That the system is built upon. Because that's included as part of the product.

>> That's very helpful. So perhaps the person who has lost the most sleep and is talking to us from the furthest, Taki from Panasonic. Who I believe is talking to us from Japan.

>> Yes, good morning.

>> Good morning and thank you for joining us.

>> No problem. Just wanted to add to Kent's point I guess on the lightweight part. I apologize if somebody said this but lightweight as in easy for vendors like us to implement, but lightweight so that it's small enough so that it can fit into small devices especially the IOT devices that don't have a lot of memory or storage space. Something that I believe is very important.

>> That is a fantastic point and one of the challenges that, we were having this conversation with one of the experts in this field, Dave Walter Meyer from NIST because he's up at the IETF working on this issue, but Kent can speak to what he's working on.

>> One of the things that's been developed in IETF right now is a specification called code SWID which uses a [C bore] kind of approach. It takes the text out and makes all the attribute textual indices. So it greatly reduces the amount of size that the SWID file would have to be for resource constrained devices.

>> Great. Thank you. Josh did you have a comment?

>> I almost said this earlier and I wish Eric hadn’t stepped out for a sec. Cisco pushed in IETF a completely different standard called MUD, manufacturer usage description. Oh, there he is. Basically the minimum viable product for it is an IOT device would advertise this is the port I'm going to speak on and the domain I'm going to speak to and

if you ever see me talking to anybody else it's anomaly detection baseline. Like, you must be misbehaving. That's really lightweight. When I saw it I was kind of encouraged because with these low capacity low energy devices that may not want to store a lot one could use such a protocol to say oh by the way, here's a web reference to my most recent software bill of materials. You can interrogate devices, take dynamic network security configurations. So is not in MUD right now, but I think from Cisco's offering, they are not the only ones on it, but it's a decent idea for these lower-cost, lower hygiene, lower compute power devices. You want to add to that, Eric?

>> I will circle back with Elliot Lear who is the original author of the standard and suggest to him and see what he thinks. So yeah.

>> So Brian I'm going to get to you in a moment the first I'm going to go to Kate star from the lettings foundation who is on the phone. Kate you are on the air.

>> Hi, thanks guys. I've been following the webinar as I can today. And I have a very couple comments about SPDX so I just wanted to clarify a couple things I heard. Specifically the package URL specification is going to SPDX in the next version as well. There is something right now that serves the same purpose that we thought the package URL is a cleaner story so we are lining up behind that as well. And we've been also looking back and forth with SWID and there are certain elements of interoperability between the two and there's a lot of use cases that are out there. And so people are interested I'm happy to provide more information. About where we are currently with the specification and the adoption of it.

>> That's fantastic that I think actually could you give us the minute and a half to two minute summary of where, what the adoption space looks like, what some of the recent challenges you guys have solved?

>> Sure. Right now we've gotten very widespread adoption of the SPDX license identifiers as a way of summarizing common licenses. And most of the package managers out there as well as packages themselves are using them at the file level as well as the package level. It has been standardized on in some of the European to put identifiers into the source code so that people can machine detect things accurately. We are working on cleaning up the Linux kernel just to have its license cleaned up and use SPX identifiers so that eventually we can just go grit and get an accurate representation of what licensing is there at the file level. The SPX specification has a way of capturing the CPEs in it right now. So if you want to be cross-link into the security databases and look up your CPEs and CWD, you can use CPEID. There's no problem with that SWD, with the SWID in there as well in cross lookup and correlation. So these use cases can all be handled. I did a lot of study a couple years ago with SWID. The reason that the open source community has not understood it or embraced it is because of the specifications behind a pay for firewall. And that has been part of the problem I think. The SPDX specification is all open but it was very hard for people to get to and was complicated on initial view. So these are all things that need to be improved. So

whatever mechanisms come out, making sure that it's very easy for people and companies as well as people on the open source communities to pick up and work from and generate to, we have open source tooling now able to produce and consume SPDX documents and so the interchange is finally starting to happen. There has been various tool vendors in this space that do security as well as doing license analysis and specific component analysis able to generate SPDX documents. Let's see, what else has been going on that you guys are going to be interested in?

>> I think this has been an excellent overview and it was very helpful to hear that there are a lot of problems that are currently in the process of being addressed. So thank you very much.

>> You're welcome.

>> We have Brian in the room.

>> Yeah, good timing. I'll go on the record and say I think that's fantastic news that SPDX is adopting [Perl]. It may turn out to be a watershed moment for the adoption of that format. Because they provide a standardized way of machine inter operating with it but I wanted to go something to a couple callers had said starting with something super basic and I wanted to provide some caution on that. We see this a lot in the cases of tools that basically name-based matching in that you know, it looks like I'm using struts, but stress actually exist with 70 individual submodules and clearly not every vulnerability affects every single one equally. So if you're not careful going to basic to a point that you can be precise enough about the thing that you are using is or is not in fact in your software exacerbates one of the points made earlier which is all those points are calling you asking you to fix this thing when in fact it's not even actually present in the software you're using.

>> It's a really good point. Further thoughts about this? Katie?

>> Apologies if I missed this and Chris Weiss presentation this morning but I've heard this mentioned before about going so granular as to then needing to track what mitigations may be in place an addition. I just wanted to say that as we go forward with this, which it seems like it is going forward, that whatever level of complexity we choose we have to appreciate the fact that just knowing what the component is is not in and of itself an indicator of vulnerability.

>> I have a question on what she is saying.

>> What I'm going to suggest that we do is I'm going to wrap up this discussion about formats and existing tools and then we'll go to the next higher level to exist some of the challenges. And there's one issues, there are two things that we've talked about and I think will useful to clarify in this room how tightly bound they are. We've talked about the formats and I'm very heartened to hear both from Kate and Kent that there's going to be, it seems like the SPDX and SWID play fairly well together or there's a strong potential they might. And is format separate from namespace? The namespace problem

I know a bunch of us have mentioned say no problem, [Perl] seems like a very good tool to go forward. We have common platform numeration, things like that. Can we decouple to solve separately the format issue and the namespace issue? Brian?

>> I think that's exactly what we are sing with Perl and SPDX. SPDX is the format, [Perl] is the namespace.

>> Great, further thoughts on sort of the existing tool side of things? Josh?

>> I said this in passing earlier, but you know, Java is, GABA is very good coordinate system and very adhered to. Some other languages are very loosey-goosey. I almost think it's useful for us to flag, I was whispering like prime directive type stuff. Like do they have work capability for certain organizations. I wonder if there's obviously some languages and some environments are going to be more challenging and less challenging for this kind of approach. I mean most of the financial services stuff is modern languages but some of the older ones can get really ugly.

>> Anyone who[inaudible]

>> I just want to point out that all the static code analysis outputs that come out, why are they not in this format already? Maybe

>> if only we had some vendors who specialized in this in the room.

>> Is there a reason for a different format for them? Or is it something that can be built into anybody who's building software to have this static code analysis like an open system?

>> I don't think it's exactly, it's not really the same thing. Because I mean static code analysis is typically giving the CWE, the class of the vulnerability and then a location and it doesn't know anything about the version or the name of something. It typically has like a binary file or source file but there's no versioning typically.

>> The category that analysts track is software composition analysis with all the vendors in that there's quite a few in the room, they don't even spit out in the same format per se and a lot of financial services guys want them to but what they'll say when you push them is well we are waiting for a standard to emerge and it's just a different output format for us.

>> And I think that is a great way to sort of tie up. It sounds like this group could put together a working group that tackles sort of this basic model of using SWI D and SPDX and what that looks like for this transparency document. Does that sound like something that we would want to have a working group that was focused on using what was in front of us today to get that basic level? Okay. We'll come back to that later when we start to people out what the outputs would be. But now I think it is important that we address some of the challenges that we talked about this morning, that a number of you have raised, of how do we think through some of the complexities of using this data? Is there a metadata channel that we want to think through and start to explore. Is there

guidance that we want to give to vendors, customers, organizations, security tool providers? What does the path look like to sort of addressing some of these very real challenges? We have on the phone Kate Stewart.

>> Yeah just want to say that I'd be delighted to be able to participate in trying to get this SWID and SPDX working together and try to get this direction happening. I think it's a really positive one.

>> I think I just got a wave from Kent. So you guys maybe the cochairs of that working group, given your respective leaderships. So we appreciate your enthusiasm and we will punish you for it.

>> Excellent. Thank you.

>> But now I want to talk to some of the things... Oh, Chris.

>> So, just back on the data format, I think this is maybe what Katie was getting at. The idea that there is a standardized, you know, column if you will of whether you are vulnerable or not, an assertion by the vendor that you are vulnerable or not. Like you know when you end of life the product you'd like to end of life it with the S bomb and all the components and what the final disposition is with those, at that point in time. Is the idea that this format would have that information in it? The vulnerabilityness or not?

>> The vulnerability-ness. Go ahead

>> Two finger on that. I put that in my slide I just did not slow it too too much. One of the working groups I would love to either participate in or even help run especially because I have to do this is, and Chris and I were talking about this as well, some of my older products you might have to use an older version of an API you can't update it. So there's going to be some sort of residual is the phrase I think I used in my slide. Some of the questions I have is how do you maintain your list of residuals and the suppositions across stakeholders and across time? Because the interval that you update them, what's an acceptable answer? You have to substantiate your answer becomes a real operational problem for software producers. And for this to scale beyond a zero vulnerability bill of materials every time which isn't feasible in all cases we need to have a way to persist those dispositions across time and stakeholder.

>> With this cover robs point from earlier about back porting as well?

>> Maybe. I'd have to hear it again.

>> So the issue with back porting is that you have, you're now unsupported. You've got some older software. You say that we can support it anymore. Well we are still supporting it. It's just that we can upgrade to the new version but we can't apply this patch to the bug to a known vulnerability. So you are still using the older version and it's out of support of the original vendor but we've applied the patch to it and so now it is fixed and is no longer vulnerable.

>> Not that anyone here has ever bought or sold a house but there's usually a list of things that have to be disclosed and are accepted and you know, there's a punch list and there's going to be some remainder and residual for software to

>> So, but there is no standard format for that. There's no version numbers. There's no way across vendors like five vendors have applied this patch and there are six names for it.

>> This house may contain lead paint.

>> So let's dive into this. Katie?

>> So I appreciate what Chris was saying there but it wasn't actually what I meant, so I want to clarify what I actually meant. It was about tracking mitigations. It wasn't about tracking whether or not you are vulnerable per se, which I think is potentially a valuable thing as well. It just wasn't what I was talking about. It was talking about format, complexity, depth of you know, how deep is the analysis going to go, you know, in terms of how this looks going forward. There were, just one example off the top of my head very quickly from my past as a Linux developer was we had a Linux distribution. One of the packages was, you know, had a vulnerability in it and the immediate communication from us as the vendor to the world was, yes we will be updating this package. However, you are not vulnerable if you install the default installation because this component is not turned on by default. So, that type of sort of meta-you know, identification of whether or not the component in the item itself is by default, you know going to be vulnerable in the way, and that is just one example of that type of additional data.

>> It's not you are not vulnerable. You are vulnerable. It's a set of contingencies to be complicated.

>> Potentially and it might be a potential place where additional tracking of that data may be necessary to give you a full picture.

>> Any of the folks who are responsible for defending organizations have some thoughts about what you'd like to learn? What you'd like to see from a vendor? Tom?

>> I think that there is, I've been thinking a lot about one of the challenges being the lack of a demand signal in the marketplace for this. When we were starting to bang the drum for structured threat intelligence sharing we had, our greatest success when we finally went around to what I will refer to as sort of the unusual suspects, so some beautiful in the critical infrastructure industries that were typically at sector coordinating Council meetings or were necessarily part of sort of our, the government relations field or anybody else and went to people who are also practical operational network defense types and got them to start visiting vendor booths and start asking for the things that we were asking for because as a government agency it was easy to sort of like sure, you want your science project in everybody's products and is going to cost us a bunch of money and nobody's going to buy it, and they don't care. Then we got people to demonstrate that they cared and it made a very big difference. Because it proved that

more than one customer is willing to break out the pocketbook for this. Here we have a similar problem but we also have a problem of, it's hard to communicate to a network defender perhaps or like some CIOs and CSOs absolutely get this. They are in this room. And then a lot of other ones don't even know that this is a thing that they can ask for. Like, you know, what do you mean I can have condiments other than catch up with my French fries. So I wonder if that is sort of like there's just like with some of the other projects you worked on, Alan, there's a big educational awareness piece for this with the consumers who should be asking perhaps for a bill of materials or some kind of package documentation. And then coaching them up on how to use that once it is in their environment. And I think you can, I mean, you can get them to draw out the dots a bit and to get people to understand it fairly quickly but again this is not something that most people are accustomed to being able to ask for at all.

>> One, two, three.

>> Some of the executive branch agencies were guests of that but House energy and commerce convened a roundtable with the subject with a bunch of stakeholders for medical and one of the initial answers from hospital CSIOs was we don't have the bandwidth to read this and we don't want it. Then about 10 minutes into it they're like oh my gosh this would save so much trouble and cost. So there was a very small learning curve. You were there too. A very small learning curve but then it went very well. I almost wonder if like a roadshow across the [ISAC] would be an interesting little roundtable per stakeholder group.

>> Let's do it.

>> I'm game

>> I will flag could there's two major finance sector events today as well as a meeting of the auto [ISAC] board. But those two sectors have expressed strong interest and I think will be probably coming up with further ideas but I like the idea of framing the surround and awareness and adoption working group that is focused may be on writing a little bit, but really emphasizing on raising awareness and promoting adoption. Are there other things that you would like to see as part of that effort or initiative? How does that play with you know, the solving the problem work. Yes JC?

>> I think, you know, speaking as a person who is doing policy work in the government, now selling commercial solutions I think it's very important that whatever comes out here be vendor agnostic. You know, it's just, there's been too many situations where there's proprietary data formats, lock-in, you know all kinds of acquisition bad malpractice, because whatever's awesome this year is not going to be awesome three years from now. And if there's a sustainable value and sustainable security, no matter how fancy something is or cool it is, we have to get away from, you know these proprietary closed and vendor specific standards and formats.

>> Thinking that there's probably strong agreement around this issue and the other thing I will say is that is one of the benefits of a multi-stakeholder model where hopefully we have enough vendors to help and I also flagged that if you see something like this and don't feel comfortable saying that you can always come to us at NTIA as the conveners and will work very hard to make sure that this is seen as a community building exercise and not a brand building exercise.

>> I was going to comment on Josh's comment about the CSOs not, or I don't know how to phrase it but basically I was one of the CSOs saying I don't want that but that was in response to the S bomb being on a PDF. You know, and really it's hard to hear people talking about this as something that is machine-readable and something that could be consumed. I'd love to pull this information to my CMDB as an example and use it for running queries when I'm hearing about the next version of heart bleed or whatever. And so that goes back to what I think is part of we have to do here is simply start doing it and I want to go back to my offer from New York Presbyterian to work with a few healthcare specific entities, and I'm thinking medical devices because there's so much visibility there as well is getting a few hospitals that are concerned and knowledgeable about this like Mass General and others and basically let's try to live through what this might look like so we learn about the challenges with publication, consumption by the consumer, you know just kind of the whole lifecycle that will go with an S bomb, and I think if we do this and it becomes a point we can talk about this, it's something we can share with people and really talk about trying to solve the problem in a tangible practical way and there will be lessons learned that we can use as part of that but I really think it is something we should do is in addition to thinking about the standards, let's just try some things now with what we can do now.

>> Seth?

>> Seth Carmody, US FDA. Thanks to NTIA for convening this group. It's very important things going on here I'd like to jump in and second Jennings here and also offer our support behind anybody who's willing to jump in the ring and actually convene a pilot specifically around medical devices. I know that FDA in conjunction with our miter colleagues have also set up a sandbox environment at Mass General Hospital that may be an appropriate environment. There are some paper works to fill out in order to make that happen to get your equipment and in some legal implications but those can all be worked out but I'd like to put out that offer just as Josh had mentioned this morning that the Commissioner Gottlieb is behind this and weeded out that the S bomb effort, not just with NTIA, but with also healthcare the sector coordinating Council, you know this is something that's going to happen so let's figure out what looks good so people like Jennings can defend its networks and devices.

>> And just for those of you who have not been working with NTIA for a little while, one thing that has happened in the past is for organizations that want to bring deep sector specific knowledge but also still want to have some of the benefits of this sort of open broader community, we have in the past partnered with an organization like first.org

where they brought large vendors and national CCERTs, but staged a sort of joint effort between that and a working group that came out of NTIA so that at least those in the research community that were not members of first could engage. So we are happy to walk through something like that. And perhaps it might make sense to say one of the working groups that comes out of this future to be determined could focus on the medical sector and we can sort of walk-through whether there is enough that's in common, lessons learned for other embedded device technologies or whether it should be sector specific. Thoughts from those of you in the medical space?

>> So this is Jennings [inaudible] again. I really am an impatient person. I don't want to wait for the standards pieces to resolve. I'd rather just throw like Jim can we just start planning something and get a few other groups and start doing this. It just seems to me like there's a problem with people spending a lot of time talking sometimes and not committing to action.

[Laughter]

>> Let's form a working group to try to solve that problem.

>> So I use the analogy of surgery, the first time human being started performing surgery they had no idea what they were doing. By doing that you get better. We were just cutting bodies open.

>> That's going to be an interesting expansion of this role. Policy and open surgery. Let's continue this. What, we have a body here of experts. We have the ability to document what comes off the top of the head. What would this process look like?

>> Well, so, I'm in contact with peer institutions. There are several like Mayo Clinic that are really thinking hard about this. I think between those institutions as the consumers we need a few medical device manufacturers to say we are going to try this with you and we'll identify certain, let's say device types that are deployed commonly across the institutions. Pick a standard or pick two. We could try to. I don't know. And have some of the folks in this room that care a lot about this like I've got a good working relationship with Josh and just physically like I almost envision a whiteboarding session where we start planning how does this thing look like how long to take to do this and get results that we can report back to the community, report to the folks that are not here. You know it is I don't think much more complicated than that.

>> Great, you've described what we would name a working group. Josh?

>> So I want to do the whole improv comedy yes and. From the medical advice we give an attack for support for what HHS is doing with the sector cordoning counsel and what you are proposing we don't need this NTIA process at all. In fact it could slow it down. And I'm very cautious that we don't do something specific to medical that has to get redone or done differently for everybody else because we are all going to benefit from this. So I like the Federalist kind of approach of a really small experimentation. I also like parallel experimentation for other sectors. The way I view the opportunity in this

room and the brain trust on the phone and anyone else we can pull into this later is, can the FDA HHS take medical action and experimentation that Jennings is willing to help with and I'm willing to help with be informed by bigger picture broader use cases from this group? So we can do something awesome for healthcare and I think we're going to do something awesome for healthcare. I want that all something to be transferable to other things and that's the opportunity in this room.

>> Katie, two fingers.

>> So I am all for the idea of running a pilot. I think that will be very instructive and even if it is in a particular niche space. One thing, if you do run a pilot, would be not just looking at you know a hospital or large organization plus some of the vendors who actually have to produce the S bomb, but the integrators and the deployer's. And then what I would also love to see as part of that case study would be time and effort from every single one of the participants, because what I keep hearing is that you know we are doing it already in this space or we are 90% there with the tools that we have. But having that big picture for an entire organization or a hospital or something like that, that is a very valuable thing. How doable is it from a practical perspective over and over again? How repeatable is it? What additional human resources and process resources would need to be developed in order to make this not just a one-time exercise? So maybe echoing a bit of what Josh was saying as the extrapolation of this, of what you learn from doing that being applicable elsewhere. Anyone can marshal the, can marshal for a particular outcome, especially if it's just to produce a report, but if the report doesn't also include the level of effort and additional, you know, potentially additional cost to all of these, all of these players and it, then we are actually missing a huge part of you know, where my concerns are about the scalability.

>> That's a good point. Pilots should try to capture all of those lessons. So I want to make sure that we don't lose also the points that Katie raised earlier about some of the overhead communication that we might need to have in a more nuanced and sophisticated bill of materials model but I want to close out sort of our initial excitement around this healthcare model. Any further thoughts around what you'd like to see or some scoping, some further insights about what a health care and medical device focused working group with a pilot in mind would want to emphasize?

>> I also think the pilot, I wish Sunil hadn't left, the pilot six years in the making and financial services is not thrown away. In fact they measure the cost savings and I think we keep implicitly assuming it's going to be a cost burden. And so let's measure it all.

>> And that might be something that we capture in the awareness and adoption approach of being able to document the lessons learned from those who have already done this. I think that could be a good way of trying to capture that especially if we are thinking about cross sector approach. Jennings?

>> Well, just to make some closing comments about the healthcare piece of this, as a healthcare CSO, one of my pet peeves is people saying healthcare is different. I

continuously push back on my peers when they say well it's different for us and we will talk about medical devices but if you talk to a CSO from the bank they say I have problems of ATMs and embedded software. And you know security problems and security challenges are not unique to an industry. They may be different in some ways but ultimately the solutions wind up being very common at least from my perspective. And ultimately if we are doing something that's a pilot this is something we should be thinking about, the sustainability of this and trying to identify barriers to adoption. But I will tell you that the current status quo does not scale. I mean I have to chase down vendors to understand if there's risk based on a component. In the wanna cry problem Josh mentioned, you know it's still happening in hospitals around this country because vendors aren't managing patches and what not. So ultimately I think it's very intuitive to me that there's value we just have to figure out how does a pilot become something that demonstrates value but also demonstrates barriers and challenges so that we have something we can learn from.

>> We’ve got JC here, but just for a reminder for those of you who are watching or listening, hit star one on the call and we'll see you and make sure you get into the conversation.

>> So I have to say this as someone who has a lot of battle scars from open systems acquisitions. The term pilot is really dangerous and problematic because the pilot, basically whatever mistakes you make in the pilot get baked into whatever you do next and you can't disavow them. So I would highly encourage people to think in terms of reference implementation. Right, so we are going to lay down some axioms for what constitutes best practice which are agnostic and we are going to do a reference implementation that goes in does and goes out does and someone else can do another reference implementation. Different sector. That works fine. You can have a reference implementation for on Prem, you can have a reference implementation for cloud. A reference implementation for IOT. But if you frame it as a reference implementation, that doesn't ossify the idea that this pilot has to become the thing. And that is really really important.

>> I was just going to say at least in my world I wouldn't, I'd hesitate to call it reference implementation. And I can see your objections to pilot. Maybe the way to say it is this is actually a bit of an experiment for, you know I'm okay with calling it anything frankly as much as I think the way that at least my team and I, we run what we call pilots I mean we are not afraid to come out the other end and rip things apart because they didn't succeed. I hear what you are saying. The philosophies are different. It is more of whatever we call this, my commitment is to consider it I think more of an experimental mode to understand what the challenges we are going to face and how do we move forward. Healthcare isn't doing this. Or if they are doing it they are using their own S bomb and we're trying to move to here's something that's standardized and rigorous.

>> So yeah it's a semantics thing of pilot, phase 2 program of record, right, that's the fear.

>> Yeah. Thank you. For framing especially in specific communities is very important to remember. So we appreciate you flagging that. So, past couple hours, since lunch we've come up with the idea of saying we are going to look at standards and formats. We are going to think about awareness and adoption and try to capture some lessons learned. We are going to have the healthcare experiment, or however we choose to name that, the pilot sector specific, the reference implementation. But I want to loop back to some points that raised earlier today and that Katie brought up again, which is, there are some real challenges with using this data, especially if we want to have this in an automated fashion. So there are, there's the question of, you know, vulnerability versus exploit ability. There are some concerns about people saying I will tell you most of what I have but I don't want to tell you everything. Are these issues that you think we should address? That we can address? We can bring a proof of concept, reference implementation that sort of demonstrates that they are not as big an issue as we might think. Or are there ways that we can tackle them to start thinking about even if they don't fit into today's standard we can start thinking about how to include them into tomorrow's discussion. Josh?

>> Maybe a halfstep prior to that on my list of potential work streams, there's been a I have to find it but this has been a six-year conversation and really on there was about 20 furious objections levied and I think 18 of them proved to be unfounded. But they look really good. And even some initial blush responses like Jennings thing all we don't want that, that's too much work. So I had proposed we capture some facts, some fictions, some common objections or an FAQ of sorts because what we really want to do is, we really want to tackle the hard persistent, pernicious things that could screw this up as opposed to spend two to much time on the ones that are maybe answerable. So it's not instead of your request. Stressing let's do a triage of what are the most common concerns and objections. Do we have a good answer or do we not have a good answer. And I think the ones were we don't have a good answer is fodder for more investigation.

>> Michelle then Eric?

>> I just, if we are talking about kind of scheduling our next activities I do want to reiterate a couple of times we've had folks very importantly point out we have two scope and the goal this. Not to death. But this type of thing can go, can expand to all kinds of areas. The making sure that everyone is very clear and having a couple of people just focused in on what that looks like I think will be really important to be able to find an end point to this.

>> And I think that actually ties back to the comment I was going to make in response to what Josh was just saying is that if you have some understanding of what you're trying to achieve, it helps you understand whether or not the objections are, rise to the level of a cost that you would say is intolerable. So you might say certain objections you can brush away because they are not correct or it doesn't reflect a full understanding of how this is going to work. In some cases you may decide there's a cost that comes

along with doing this but it's outweighed by the benefit. So you have to have an understanding of what you're trying to achieve in order to net those things out.

>> Reactions? Katie?

>> Perhaps a place that will help inform some of the costs would be to do a survey of the intended consumers of this information about what their current costs are for deploying patches and the reason why it may inform some of the S bomb efforts is one of the biggest things I think that will be one of the devil details is the frequency of updating it. And the frequency, and I bring that back to the intended consumers of that information and back to one of my original concerns, which is organizations struggle to deal with the vulnerabilities that they know about today in applying patches you know, for the vulnerabilities without the subcomponent additional information. So a survey of the, of some of the willing you know, intended consumers of this information, of what they spend now and what they would like to see in terms of, you know how would this help them, how would this help them with their current picture, because I hear a lot of, there's a lot of cost saving that is talked about but one of the most eye-opening conversations I ever had with a customer when I worked at Microsoft was the fact that they actually spent about $1 million every patch Tuesday, so every month on the scheduled testing and deploying of patches. They wanted to cut the $12 million budget down to $4 million. They asked us to move to quarterly because that is what they wanted to spend and that was within their sort of risk tolerance. So intended audience, survey them for what they are spending now and what they would like to see out of this and that I would very much like to see an analysis about what the cost reduction might be in improved efficiency from having this information.

>> Michelle?

>> Sorry I just wanted to, I think that because of the point we are in the maturity of this process we may need to also factor in the risks of not doing this properly, right? Because I don't know how many organizations actually have efficient and fully vetted patching processes and one of the things we're trying to do is avoid the big, costly consequences of not patching properly. So trying to bake that into that kind of cost metric as well, the cost of having a successful ransomware attack kit at your hospital, things like that or other industry.

>> In terms of metrics for success since we've acknowledged that having like an S bomb as part of your organization as kind of a sign that you are doing other things right and also may be communicating with other organizations right, the benefit of adopting a standard like this could be kind of emergent and distributed across the whole software development ecosystem and not accrue to any one particular organization. And it would be interesting to know if there's a way to get an overall metric of say the security of the ecosystem based on this standard options intervention.

>> We've got one, two. Josh?

>> I don't want to be the referee but every time we say we're trying to protect like an end-user operator I feel like it's the paternalism thing. So I just want to caution they can choose to ignore it, they can choose with the patch frequency is, they can choose if they want to mitigate it. If we don't give them any information, they can't make the choice.

>> You I don't think we've heard a shortage of potential benefits today. But I think we should also beware of what are some of the challenges.

>> One extra additional benefit to follow up to your comment from the industry specifics we are still seeing over 10,000 organizations stoning known vulnerable versions of struts and if they didn't learn from the issue that Josh mentioned from back in 2013 they should've learned from the one that got Equifax and then later additional ones last year. And so as we work to make this more of an accepted best practice like CI, like CD, the inevitable side effect of that is that everybody else will start paying attention to what is in their software and hopefully it will up the game for everybody.

>> Rob?

>> Well you asked if we had something else besides benefits, so I want to talk about the costs for a second. I come from the world of intrusion detection systems which don't work. When I say they don't work it's that they don't work as intrusion detection systems they don't sit there silently until one day it tells you by the way there's an intrusion. That's not what they do. What they do is provide a lot of visibility into the network. They provide forensics data for after an event happens and so on and so forth so they have a lot of value they just don't detect intrusions. And one of the reasons is false positives, that a signature will trigger its accurate 99.9% of the time but you have so many backups, you have 1 billion packets go across so that means .1% of 1 billion packets is still 1 million packets that trigger events. And we have a similar situation here everyone is saying look at the JBoss structural vulnerability, tell me about the habit so I can fix it but what they are not thinking about is the false positives of, I mean we discussed a kind of on the edges but not in these terms of, I'm getting daily information, I get 10 new NVDs that say, that match up with stuff I've got in my environment, am I vulnerable? And I don't know. I have 10 things I have to deal with per day that I basically ignore per day. So the question is can I give you an S bomb you can match with the vulnerability database that's not more false positives than signal, that is not more noise than signal.

>> Is there something that I can, this communication would come from the vendor to say, hey, we know this is going to flag it and it's okay. It's not, this will be a false positive

>> what I mean is if you get S bomb from the vendor and you do the matchup yourself with the vulnerability it's, on the whole it's going to be more noise than signal.

>> I want to bring in Sunil who's been doing this for a little while and then Chris.

>> Yes so what's missing in many organizations is a threat model that connects those pieces together. So yes I actually want to know all the vulnerabilities but the filter that we applied is a threat model that says does it even matter. Just to use another

metaphor, you are vulnerable to Ebola. Right? I don't think anybody doubts that. I don't think you would question it. However is it within your event model that you should be concerned about it and the answer hopefully should be no. Otherwise I think most of us would leave this room pretty quickly. But we know that you already have a threat model in your head that would say is that irrelevant. We don't have a similar construct, or many organizations don't have a similar construct or the threat model is available and thus you can make the decision. Now whose responsibility is it to create the threat model. And it's not the vendors. It's ours.

>> Chris?

>> I think when we talk to the timeliness of the update of the S bomb, if the S bomb has information from the vendor saying whether it's an issue in the component that is in their is exploitable or not the timeliness of the update is going to matter. If you have 300 open source components probably almost on a daily basis one of those is going to have a CBE associated with it or at least weekly. So if the vendor is updating you monthly or quarterly, you have this huge period of time that you don't whether you are vulnerable or not and different organizations might choose to mitigate anyway to Sam going to put some sort of mitigation in place, waiting for the vendor. So I think this timeliness of the update of the S bomb is going to be critical, right? I mean obviously you'd want continuous, but if it's weekly or monthly, is that really that great, you know, is it usable still unless it's a very quick update from the vendor.

>> So this is a world when if the S bomb can convey metadata as well as just the list of dependencies, it can contain metadata, we might need a world where the S bomb is updated more frequently than the product itself.

>> Right. If you're going to go on the path of you are a risk-averse organization and you have to mitigate in some other way than wait for the patch. You'd want to know to put a mitigation in place. Which is what I'm hearing the critical infrastructure and the medical world would want to do.

>> Thoughts on that, for those who are justifiably risk-averse?

>> The answer to your question is no, weekly, monthly is not good enough. If you go back to we want the defenders to be having the same information as the bad guys, bad guys get it as soon as it is out there. They are not consuming their data on a monthly basis.

>> Bruce?

>> The [inaudible voice off microphone] information that comes down and some people understand it and most people don't and the people that don't [inaudible] and we need to stop that at least in the cases where there's random, we need to stop it always but most of the time the random action I've found is known do anything could at least in our customer base. Because they found out I didn't do anything, I haven't done anything for 25 years the number has been or whenever it hit and nothing bad happened. I used

to do things and it disrupted everybody. Sometimes my systems didn't work for three days after I applied the patch and it didn't help anything so I stop that. So we have to address this problem. If you're going to get people to adopt it you have to do it in a way so that they are not going to be jerked around all the time and then find out it didn't matter.

>> But again, I mean I think any argument that you know it's better for end-users not to have information about how they may be vulnerable is just not really going to get much acceptance, because if they want to read it they don't have to read it. They may have a contractor who takes care of that for them. It's just, it becomes indefensible at a certain point to do things like tell system integrators that they can't reveal vulnerabilities in your product to their customers When they know they are there. And so again this paternalism really, it should stop. But getting back to the business process I think the real pain is the shift from batch to continuous process. Right, and in every industry it doesn't matter whether it is pouring steel or constructing houses, when you go from batch to continuous processes there are wholesale changes in the industry you go from you know, chunks of steel to you know, roles of steel coming through the factory and it never stops. And they are, the processes necessary to adapt to continuous monitoring, continuous integration. I mean every single large enterprise is going through, you know some evolution whether it's comfortable or exciting or painful around this and there's a skills gap and NHR problem associated with that. But I think that when you get into continuity and you get into automation that's where these, this information should be there and also becomes useful.

>> I've got one, two, three.

>> Just going back to the title of this whole meeting today is offer component transparency and the fact that I don't know what the harm would be to provide that information. As people have said they can act on it or not but to provide that information if you didn't provide it and you knew it and you did not provide that, then at what point does this become a legal issue down the road of negligence or something of that regard that someone could say you knew this information, you sat on it, for paternal reasons, whatever you didn't provide it and something happened. Why not disclose if you have that information and let the folks decide what to do with it.

>> All right Tom, Josh, Bruce

>> Going, so back to our experience just shipping around threat indicators in a structured format or not a structured format in lots of cases but this sort of like you have to be willing to ship garbage sometimes just to have a conversation with what your users actually want and what people can leverage. If you want more people to achieve the right level of understanding that Bruce, I think you are talking about, first you have to tell them a bunch of garbage and let them make mistakes and then blame you for the mistakes. Which is where we been before. And then you learn from each other, right, and as slowly over time we've learned how to refine how we package and ship

indicators and the degree of context that people want and that there is some stuff that's strictly never useful no matter how bad we might think it is. And I see that I would imagine that this is going to be similar. That again as far as the roadshow is concerned we are going to have to teach people what to expect and what to do and not to do with the information.

>> Josh and then Bruce.

>> That was a good segue but if this is the part where were saying what I'm scared of in S bomb, what I'm scared of is, there are a few, not too many, but if you that expect to have come to the bill of materials. Like no known vulnerabilities at all. And especially think I said this before for the older stuff that's not going to be possible or even economic. We wouldn't want people doing busy work I think is the phrase Chris used with me on the phone at the cost of valuable work. And so I think a risk is if the column one from my graphic of the S bomb itself is only used it to create column two of a list of potential vulnerabilities treated as actual vulnerabilities, that poor education absolutely could cause busywork. That's why I'm pushing for column three, which is some sort of rational analysis or attestation that could persist across time and stakeholders.

>> Bruce then Jennings.

>> I'm not advocating giving people nothing. I'm just trying to say that what people need is they understand it. And yeah, it will take time to get there and it will take time for us to understand how to communicate with the different constituencies so that they can get an understanding, but we are not done when we just say this CBE might be, which is against this competent that you have and there might be vulnerable, decide what you want to do on your own. That's not good enough.

>> So, I just want to again reiterate kind of the importance of this from the patient safety perspective and I've heard some skepticism in the room today and I get it. You know, there are going to be customers who, let's say we gave all the third-party components, there's going to be customers who don't understand this and they are going to be a pain in the butt. You know, I get it. But at the same time, thinking about New York Presbyterian or any of our peer institutions, we are critical infrastructure and when we thought about security four years ago it was HIPAA and is it laptop encrypted but we now talk about it in the context of emergency management, enterprise risk, business continuity and I'm working with law enforcement on tabletop exercises around a blended event that brings down our elevator systems in our hospitals and we can't move patients and during that event maybe we have a public health crisis and we're trying to pivot how we deliver care. This is the sort of stuff that really, this is happening in our country, it's happening around the world where there's really critical events happening, mass casualty events and the technology we are talking about here, the software behind it is used during those events. And so we have to have a security program at New York Presbyterian that scales to having available systems during really critical events that affect our country and it is unsatisfactory to say well there might be

some customers who don't use this, so it's not valuable or there are some customers who, you know, might read it too much into this. We are talking about really important stuff, you know, that needs to be there to help critical infrastructure. And this is important and I think teams like mine can be the sort of teams that actually help us work through these issues and you know, try to identify a path forward for something that's really critical to multiple industry sectors.

>> Thank you. One, two.

>> So it seems like a lot of the concern is how the recipient of the information interprets it and what the best practice of how to do that is. It seems like that's also something we can solve as a use case, as a receiver of this information what is the best practice for how I'm supposed to interpret it? Should I expect that there are zero vulnerabilities or is it more realistic to expect that the vendor has probably investigated all of them and disclose the ones they know about and have told me why they think certain ones are not vulnerable and that information empowers me to do what I want with it. But I think as we publish the standards we can publish the expected standards for how it is interpreted at the same time.

>> And I think that may be, I'm going to jump in, we have a number of you who wanted to focus on what can we do with what we have today and then perhaps another area of focus can be okay, how, what does transparency look like tomorrow. As we sort of build out so the folks who are using this, how can we add an additional layer of metadata on top of this that can help organizations use it and make sure that they are not inconveniencing the vendors as well with further complexity. I had a point here and then Rob and then Eric.

>> I thought at one point we were focusing on bill of materials which my understanding is a statement of some software producer saying this is what's in our stuff, the list of ingredients. But it sounds like we are also talking about the things saying you know, warning, aspartame causes cancer in rats. Maybe you should be concerned. And that's a different function. And I want to bring it back to an original point that Ray which I think was duly shut down but it's like if we are talking about having data available about what components, under what conditions are or are not exploitable, what is the incentive structure around building a common knowledge around that, such that we can use that to inform decisions about risk and mitigation.

>> So, I wanted to jump back to the point on understanding versus just having raw information. And that the raw information is better. What we have 30 years of experience now with full disclosure, where this issue has been constant that we gave out the raw data of a vulnerability in the full disclosure process, or do we try to give understanding. And we've had this constant problem where vendors sort of corrupt their data. Like is this a critical vulnerability. Well, they have marketing reasons why they might want to soften that and tell customers it's not so critical. So the understanding from the vendor is immediately that they have other concerns then what we have as the

consumer so 30 years of experience with full disclosure is the idea that get the raw data out there first, that's the most important thing and understanding sort of comes later and similarly we've had 130 years of that with crypto. Everyone wants to cover a crypto stuff and the end user doesn't need to know the algorithm details. We can cover that up. And in fact you find you get the raw details out there. Because what you are hiding to try to communicate understanding is any alternative perspective. Your friends may have a different perspective on it and you're hiding it from them so therefore they can't get it. So maybe the hospital can deal with the raw information but yet the understanding comes from the community from other companies, from other sources, other than the vendor.

>> I like that idea.

>> Can I respond? The hospital can. Not all hospitals can. One of the things here is I think we are assuming every customer is the same. But my hospital, hospitals like mine all the time we review the crypto's used by the vendors and we are constantly telling them hey you're using export ciphers or you're using TLS 1.0. We want you to upgrade to 1.2. It's part of why want to see the asked mom is because we make it part of our procurement process and part of the lifecycle for managing the vendor. And the benefit of having big enterprise hospitals like mine doing this is I think there's trickle down to smaller community hospitals who don't have those resources and capabilities. So that's part of I think the same thing will happen if medical devices or other software can be, the electronic medical record that we have the ability to drive the conversation into affect basically product design and support and benefit the entire industry, not just our large hospital.

>> I had a two finger from Kent.

>> I just want to sort of push back on the myth that vendors have a tendency to twist the truth when it comes to issues like this. Quite the contrary. We want to get this out as fast as possible because we have a liability issue if we tell you something untrue. It's an integrity issue from us as a vendor as well. So this myth of the vendors will tryst the truth is, you are dealing with the wrong vendors to begin with.

>> Well we have some conversation here. I don't want this to devolve into the full disclosure debate. We wandered into that one already. But I do want to get to Jen and JC.

>> So I'm just going to say like I agree with that point about you are dealing with the wrong vendors. I think there are absolutely vendors who do this. They are absolutely vendors who don't. I think not all vendors are created equally and we could all probably agree on that.

>> Oftentimes it's not their vulnerability as written. I mean most people, 80% of the software in a commercial product is open source. So if there's a critical against some component there, it's not like they are just pulling the score out of the air. You know, where they have a fudge factor around it. Like it is, it's there. And so it would create like

horrible regulatory and legal problems for them to change that. You know, I think that the disclosure issues become problematic when people either don't disclose what is there or they prevent others from disclosing what's there.

>> So I didn't want to debate full disclosure but I do want to point out that your statement disagreed with me agrees with me. Like one reason why you might distort the information is because of your marketing reasons. The other reason might be for regulatory reasons, that you've distorted it the other way. It's like Josh's statement that he made earlier, this house may contain lead paint. They don't know whether it contains lead paint or not but they are making the warning because they have to and so the same sort of thing happens for risk analysis is that you have to go the other way and maybe say it's more risky than it really is because if you don't you'll get sued. So what I'm saying is that the needs of one is not necessarily the needs of the other.

>> We do that [inaudible voice off microphone]

>> We have a request for you to use the mic if you want to say more than...

>> We do that. We always go higher. If there's any doubt we always go higher. Always.

>> All right, we've got Josh and then Eric.

>> It's really a question not a comment because I've known you long enough to know when you're sometimes being Socratic or whatnot. Are you saying with your point about the 30 years of disclosure without having disclosure, are you saying we should give the fullest amount of information? Or are you saying we shouldn't? Because earlier it sounded like you were advocating for opaque. Now it sounds like you're advocating not you, Bruce?

>> I'm not saying we should or shouldn't. I'm just saying the argument that it is too, that the raw details are inappropriate is never the argument in our community. We decided that our community needs transparency. That's the name of this group. We've decided transparency is good. There are other flaws, to what detail we gave this information, which is the cost versus the vendor. How much use will be, there's lots of other questions. But the one question we should all agree on is transparency is good.

>> Eric?

>> This is I think maybe a question for further thought based on what Josh was saying before but you are talking about how a lot of times there is a belief in advance that this is going to be a net cost, and yet there are benefits that exceed the costs. How is it that you measure the benefits of the use of this in a way that will help us to understand what costs we should be willing to bear.

>> I think per stakeholder because you and I are speaking very similarly, per stakeholder, what is the current pain of the cost of operations to call every vendor. So you are a hospital operator like Jennings have to call these people and they are you,

are you are you vulnerable that is having a cost and efficiency in the meantime to resolution. One of the ones in the room, I'm hoping the Aetna guy will speak to this but Jim [Ralph's] saved millions of dollars of reduced unplanned unscheduled rework and he measures it with engineering KPIs, like very proven common things. So I think per stakeholder group you could look at current cost burden, emergent cost burden, that kind of thing. I don't think it's going to be the same measurement across the stakeholders though.

>> If we have examples like that that prove out the model that I think it will be a lot easier for us to, you know

>> This gets back to the point earlier about trying to understand some of the costs and benefits. So as we are coming into the home stretch of today, I'm very impressed at some of the common ground we have found. You guys have figured out that one may be tackled the standard set of thing and we have the independent software vendor and the Linux foundation coming together and that warms my heart. There's some real interest in part because there have been a lot of view participating from the medical sector to say let's really work for understanding the implementation in this sector. I think those two efforts I hope will work on coordinating them. There is the issue flagged of this awareness and adoption piece, which I know Tom talked a lot about sort of first taking this on the road and engaging sectors, more organizations, building a bigger tent. I wonder whether you all think that the discussion of understanding some of the costs and benefits, whether that is the right sort of grouping to sort of think about awareness and adoption to tackle some of the data-gathering, whether it is anecdotal or quantitative. Would you like to see those, this is the point where you start to think how much work am I willing to do to actually find good answers here? This is where we start making eye contact and making everyone uncomfortable.

[Inaudible voice off microphone]

>> So we are going to flag the awareness and adoption piece. Do you think that is a similar question for understanding sort of the organizational mechanics? Or do we think that should be a separate issue. And the second thing I want to propose to you is, should there be a group that is not focused on saying what we can do today, but trying to tackle some of the longer-term visions of what does transparency 2.0 look like that we can start thinking about now so it can be standardized in a year so it can be rolled out in two years? Do we want to sort of go down that road and try to tackle some of the very hard cases that Katie and Chris and Rob and some others have brought up art?

>> I don't have an answer to your direct question but looking at the provisional working group ideas I would suggest that the SWID PDX1 be slightly more genericized to be, to existing inventory standards review what is currently being used, is it working, how much do they talk to each other. That's probably useful to know before you make an uninformed decision about which one to pick. So okay, thanks.

>> Good framing, thank you. Kent, you like that? Yes?

>> Hi, savanna with TIA. I'm sorry what?

>> Remind us of your name

>> Savanna Shafer with TIA. I really like Josh's idea about pulling together the FAQ of sort of current conversations about S bombs and I don't know if that fits under the awareness and adoption piece, but I would like to make sure that's kept in.

>> So who is going to do the scoping and goals? Is that a group or…?

>> No, that is an excellent question. In the past something that we've encouraged is that is the first job as a working group comes together is to come up with a statement of purpose of some kind and figure out how they are going to address the task.

[Inaudible voice off microphone]

>> And I think, no, it's a phenomenal point. So how would you tackle the scoping and goals question?

>> I would say for the medical device experiment, which we will come up with a different name because that sounds kind of glib

[laughter]

>> It sounds problematic at so many levels but I would say that we would define, we find some key leaders and we define what are the scopes and goals and we would be transparent and share that. I think that is really probably is across each one of these. It is, awareness and adoption is

>> Sorry I'm not going to put the microphone I think we are talking across purposes. I agree that every group will define its own scope for the project that that group is doing but I think that the original point and I'm sorry I'm terrible with names but I think the point that you are making Michelle is that we haven't actually agreed to scope for S bomb is, and therefore having subgroups working on different elements of how we would apply it or what it would look like or how we would adopt it means that we are all going to be running in different directions and not speaking a common language.

>> Can I, just about the medical device piece. I would imagine let's say Jim [inaudible] Siemens are helping we've got some others, we would maybe look at SPDX and SWID and say what we want to adopt, what seems to make sense for medical device manufacturers right now and it is an experiment. We can pivot. If those things become completely harmonized we can change but let's pick something and see where that fits, you know? Does that make sense

>> I'm just going to respond to this really quickly. That to me makes sense but I think there are some really foundational things that we need to create as basic parameters to make sure that anybody involved in any of these working groups has a common understanding of what we mean when we say S bomb. Particularly as you know to the point again and I'm terrible with names I apologize but you made the point earlier on

that we've have people in the room talking about S bomb as basically just a list of components and we've had other people talking about it as a list of vulnerabilities. And so while there is I would say pretty broad spectrum of discussion around what this term means and it's still relatively loaded that it's going to end up being a situation of I think like relative chaos unless we nail that before we split into subgroups.

>> Kent.

>> Okay my understanding and this is just mine, could be mistaken, my understanding is we are looking at third-party components to software packages and identifying those. The vulnerability aspects and all that other can be use to build on top of that foundation but initially because we want to look at just focusing this we are looking at third-party components to vendors or software publishers product.

>> Art, Seth, Josh, Jim.

>> As I sort of laid out in my slides I personally like having the component relationship and vulnerability mapping but I do agree with Kent that the first layer of that foundation needs to be the inventory. So I'm reasonably happy with minimum viable product being the ingredients list. The word third-party concerns me. I sort of know what you mean, Kent, but just all components. I don't care that they are third-party or not

>> Third-party is just for my focus read anything the vendor didn't develop themselves [inaudible incorporate from open source.

>> And I want things that the vendor incorporated in things the vendor created from the final recipient I want all the parts. So I want McAfee to include all the stuff that you put into your stuff and the stuff that you create first whatever, first party.

>> So just, sorry just so I understand you're talking about you want source file names, you want that kind of stuff because that won't happen.

>> No no so abstraction is important here too, but it can go a couple layers above that. You know, you can give me, the S bomb I get from you can Sam going to make a product name I can't remember anymore, McAfee antivirus version 4.71 83. So there's that and bundled with that is open SSL and some other stuff. So I don't need your file name level but I need your something, what you call a product.

>> You get the product information at a higher level from the standpoint of the product name, product version, any dependencies and then third-party components either commercial or open source.

>> Sorry, I want to keep the flow but I also want yes, I just want to...

>> So I find it very interesting the conversation happening between you two and this guy is going to be needing whatever you are producing to act on it. So I feel like from my perspective at the FDA's perspective we are using S bomb to rally around and sort of say oh, this is a concept but really in actuality what it looks like I don't care. As long

as Jennings can use it. Jennings, do you know what you need right now at the moment? So that we can properly scope this or is it something that would come out during a pilot. My point is that is it something to be figured out or is it something we can define right now before we leave the room? Great.

>> So that was the, we have the existing standards, we have the pilot, that will tell us what we can do today, or sorry, the reference implementation and then I agree with you that definitely from an awareness adoption perspective we are promoting awareness and adoption of but I think we did a good job or you guys did a good job of sort of saying well we are going to limit it to on premise software for now and that is something we can also add going forward. But I think the scoping is not going to be solved in the next 45 minutes. We still have spent the entire day sort of talking through what are the benefits and how could this work. I have got, what was my order there? Josh and Jim and then we will just go around.

[Inaudible voice off microphone]

>> Regardless

>> Well, for the today.

>> I was going to, I think if you look at your according to the disclosure multi-stakeholder process we sort of naturally fell into time horizons so my instinct, and I've never seen this in yours before is Jim's strawman initial you know, draft of a three-dimensional thing, my instinct is like a very quick turn of the crank that is useful as a platform for every other project could basically map the best practice in horizon one and then just what is the heat map of what people are actually able to do not theoretically able to do. And then we have the ring just outside of that is what, you make best practice common practice. So some of those tangible, and then maybe the aspirational stuff you call transparency 2.0. But let's do a capture of current, a capture with minimal effort and maximal reward what is just outside that. Because if we just look at what is, to your point, the scope could kill us if it is too big, right? You could easily under scope this thing, you could easily over scope this thing. We are both trying to future proof the thing and also make sure we don't take forever to get there because hospitals are actively being attacked. So I don't know if there is a way to do like a very quick project that enables the rest of the scope and use cases and exit criteria to be good. I don't know.

>> We've got JC and then

>> You missed me.

>> Sorry, Jim

>> I just want to be clear in the scope on top. I don't want to pick apart words, but it's more than software packages. And I think you captured devices already there, but it's not just a software packages, but devices.

>> This is why I'm going to strongly suggest that the working groups were going to actually be churning forward focus on that scoping and as we move forward we will be conflict that process. JC then Art.

>> So ion channel has an open standard called the [CEVA] for what's in it and stuff about it. And nobody schema is going to be the be all end all but I was happy to share that with anyone so that people can knock the stuffing out of it and say well, what it's missing or what else would we need. Not even to use ours, but to say well, something that we would use what have this but it would also have this and like oh, that thing is completely unnecessary and why would anyone think this was useful or whatever. But I can just throw something in the ring to murder board and sometimes it's better not to start with a blank sheet of paper. So you know we can send that to you guys and you can take it apart and I'd love to hear what's awful about it.

>> Art?

>> I'd like to cling to some hope of a little bit of scope coming out of the ring here. This is maybe the last time I'll try it. We just got into, we must not down the rathole of what level of granularity, I was, Kent was sort of suggesting lines of source code and we asked the end-user what they would want, we're not going to solve that today understood, no argument there. But even to say we are only doing the list of ingredients and it is box product and that can include devices, even if we could agree on that, which I'm not sure we can but if we could do that today in the room we are a lot further off, down the road then otherwise. That's I guess I will put that as a proposal.

>> So we are going to have you repeat that.

>> I will speak slowly. A proposed high-level scope is I'm just going to say box products to include devices. So services are out and what else did I just say?

>> A list of components.

>> Yes we stick to the list of ingredients, list of components and I will delay my wish for component relationship perhaps and vulnerability mapping. As add-ons. That's a proposal. I'm not saying done deal. So shoot at that

>> On that scoping, Jen, do you have a thought on that scoping?

>> I have a question about the scope actually. It's very specific to this. Is there not going to be any discussion of how this is shared? It's just saying this is what a component list looks like? Because it seems like there's more to this. Because it's, I guess you're going to get that in the standards and how it's written, but, so if I understand what we're saying, we are just creating a format to create what has previously been called an S bomb. But we are not creating any way of sharing that or compiling that or any, I'm just asking because I've heard

>> So what does the action of transparency look like.

>> Are we stopping at a template or is there going to be some process involved.

>> Great question. I think you want to have Kent, you got two fingers high there.

>> Okay so part of what at least was thought about before this in some other forums was to have both a format and a suggested way that we could distribute this. The suggested way to distribute it would probably end up being a working group because there is some other pieces that sort of had to be brought into play to make that available. So that, thank you for bringing that up. That was one thing that we did want to try to think about from the standpoint of creating a working group around distribution of these and availability of these. Normally though, the intent of the box product is, this is incorporated in the box. So that bill of materials goes with the product and it's always there and it's always updated. When changes occur.

>> Jim, Bruce, Josh. Anyone else, and sorry. You keep doing this to me. Sorry.

>> So, to Arts definition about the scope, but box products, in our cases they are going to be really big boxes. Okay

[inaudible voice off microphone]

>> But to answer what Seth was saying before, I agree with Jennings that we could, if we sit down for a day with a whiteboard we can get to the answer of what we want to do.

>> Jen?

>> So I have two requests. One is that, can we get some like specificity of what we mean by a list of components, like is that just what's in it, is it just what version it is, is that, like just a little bit of specificity about what that means or like capture it as a question that needs to be answered by the working group. And then, that would be my second request, is that I get that we don't want to import a scope right now and that we want working groups to come up with them but maybe what we could do is look at Jim's slide and agree a set of questions that the working groups are all going to answer in their scoping so that we can make sure we are all at least scoping to the same requirements.

>> Which slide of Jim's?

>> That one right there.

>> So all working groups should directly refer to that slide

>> Maybe we could pull out some questions that come off it and capture the questions so that the scopes all address those questions.

>> Okay a start

>> So sure some of them you've already discussed around things like is it devices or software, is it stuff that is on Prem or as a service and like you've already addressed

some of those already. The time frames I think is a critical one. I think like what information is being shared. Like is it versions, is it known vulnerabilities, is it whether or not a thing is still supported. Like that seems like a pretty fundamental thing.

>> You want us to go back to the discussion to resolve now what information should be shared?

>> No. I'm not saying we need to answer those questions now I'm saying what I think would be a sensible idea is if this group agrees a group of questions that the working groups will then make sure are covered when they come to scope so that at least everybody is scoping on the same requirements.

>> I think that's a great idea. We don't have a list of working groups yet but I think that's a great idea. We should come up with both of those. Josh has thoughts.

>> I don't know if I was supposed to be next or not but I was trying to answer with this model a single sentence scope statement, now we are kind of changing it when we say boxed stuff, but if I were to say what I see happen pretty routinely in financial services on the part of some medical device makers it's all software components for the depth dimension, pretty routinely. It's component name major and minor version for the breadth one. Pretty consistently. And it is with each update pretty consistently. That is so if I were to heat map it instead of just talking about heat mapping it the heat map I see is that intersection as a common practice. So that could be a phase 1 scope. I didn't say the trio that you are expecting me to say for Josh Korman bingo.

>> Inaudible voice off microphone]

>> Sorry, Josh, can you narrow that down to a single sentence we can see our notes anymore.

>> If we only use the 3-D solution space which I told you I wanted to improve but the current heat map of common activity is all software components on the depth dimension, component name with major and minor version on the breadth continuum with each update. So that is the any update middle of that line for the time dimension. That is what I see as the most common behavior for current S bombs.

>> And I want to go to Michelle and first we have Steve Lintner on the phone and Steve I'm sorry I did not see earlier.

>> Actually I, it was like 15 or 20 minutes ago that I hit star one. So I think I may be well out of sync. I just, at the risk of taking what was referred to as the paternalistic perspective, I think the high-priority, and this is consistent with what somebody said, one of the user folks said, I think the most compelling scenario I have heard this morning was the person who said that he asks his suppliers to demonstrate that they have a software bill of materials for the software that they are delivering to him and if they don't then uses that as a negotiating point because he knows he's going to have additional risk and additional work to do downstream if he actually buys that software.

And by the way, not buying it might be a pretty good idea. So I feel like it's a very compelling use case and scenario. Sort of beyond that, I get confused about what folks are actually going to do with a bill of materials if they have it. Maybe in some cases they can protect themselves. I think a pilot is a good thing to demonstrate the value of the bill of materials to the end-user community.

>> Thank you. Sunil?

>> So Steve, that was Sunil who, made that comment in the me follow up with that. I sent Megan to your email address and diagram, I'm not sure if you can show it. So, sorry, the diagram I created for Megan was one that there is, imagine just for the sake of easier being able to see this a little easier, imagine just a two-dimensional diagram for a moment and that two-dimensional diagram will draw a box that basically represents what the vendor is willing to offer as it relates to some of these parameters. Okay. But then what the buyer wants is bigger than that. All right. The size of that box that the buyer wants represents our minimum risk tolerance for some system that we care about. And that box may be bigger if the impact or the criticality of the system that we are buying is of sufficient thresholds. So there is a certain box that represents the volume of how much we care. Okay. And in theory the vendor should exceed that. But oftentimes today they come short of it. So there's a smaller box in terms of what the vendor offers today that creates a concern for us because we do not have the information that we need as it relates to the software bill of materials and so on and so forth. So the difference between what the vendor offers and what we are asking for, that's the opportunity for us to drive concessions from the vendor as it relates to, since you can't meet our needs, this is what we want you to concede as far as the negotiations are concerned. Main thing I wanted to point out the was the size of the box that is expected from the buyer is really driven by our minimum set of expectations around what the impact of a system. So if there is a system that is truly, if it goes down our bank goes down. Then we're going to actually ask for a lot more, just because it is so important to us. We are going to want it in real-time with every possible attribute

>> There's a lot of context. Not all software is equal.

>> That's right. So know that the variable set. I think to Josh's point about what is the minimum expectation he I think hit it right on. The minimum expectation is what he mentioned. Any update, major version, all software components. But know that from the standpoint of our risk tolerance for certain other types of applications it may be much greater than that. But you know at the same time we may say you know what this piece of software really doesn't affect us that much and we may want to have a smaller one. And so it is going to vary. But to Josh's point, that is a great minimum standard that we should start with. It's going to change.

>> Thank you. Michelle.

>> I just want to go back to Josh's proposal. I agree those things are very important and actually I like this slide a lot. But if I want to come back to what we were discussing,

which is the scope, I would caution against trying to incorporate time if we are just looking at a template and a method of delivery. Unless the time is how often you are delivering an updated S bomb for lack of another word, previously called S bomb. If we look at what the scope of any initial project would be, the depth and breadth, if you start bringing in how often you are going into patch, that often becomes a, you look confused.

>> So, just the time seems to be coupled with the method of delivery. But on this chart it is, it is either in real-time is independent and everything else is coupled with this type of delivery. It is your slide. You can

>> Is this the delivery of the patch or the delivery of the updated S bomb? Because I thought it was delivery of the patch.

[several voices]

>> Okay now I understand. Thank you.

>> I'm confused because I thought the time was anytime the software itself was changed on the system which would then include the S bomb. So, at initial delivery at major update of the product, when it is patched, all of those are times when you are going to get new software and a new S bomb.

>> So this is how often to update the S bomb, delivery of software, updates of software real-time. Fair interpretation? Happy? Yep. Which is to say are they going to be coupled or independent and I think that's an important thing to acknowledge, but from a scoping perspective may be something that a group would want to tackle, you know the 2.0 versus what we have today. Further concerns about scope? Bruce?

[Inaudible voice off microphone]

>> I was going to give up on components with in components which he calls relationships or something that I think we ought to keep that one, and that's based on our experience in building these things internally because sometimes you'll see that a component like log [4J] is putting itself in the product and sometimes you find out that it's inside something else and if you just say log for Jay you don't know that it needs to be updated multiple times or not at all because the component, when it already went in and figured out that it wasn't exploitable or something like that.

>> Yes I mean at this point a full transitive dependency tree is something you can have pretty easily if you are in a CICD pipeline and you have a platform behind it. It's like a solved problem now.

>> Should we leave that as a potentially included. Excellent. I want to go back to the list of ways that we are going to tackle this. And again the way we think about working groups is, this is the tentative, this is the initial approach. Folks can say hey I'm we thought we would go, do work on this but it turns that we don't want to. We are too busy. People may come in three weeks from now and say before the next meeting, and say

we think this is an issue. So this is not definitive. We are not bound to this but it is how we can start getting our feet under us on this particular topic. Katie?

>> Can we go back to the slide before this?

>> Yes. The notes. Do we have the list of vendors?

[Several background voices]

>> Sorry yes?

>> Well because I have a question about it. Okay so those are the working groups. Awareness and adoption, is that working group, because I knew that it was, that working group, I knew what that was for during the CBE multi-stakeholder. But what is that working group for in this context? I don't understand.

>> Kent do you have a thought

>> Yeah my thought is like hers it's a little confusing especially if you are doing a standards review and trying to map the best practices is in a different working group that's part of the standards aspect. So awareness and adoption might be a review of what is actually occurring today with the various formats and options that we have

>> So it was my attempt to try to capture Tom's approach, which is let's have a slightly bigger tent than just the folks who are in the room. The emphasis on understanding lessons learned today from what's been going on, and this was, some folks made the point of you know, people like Sunil have been doing this for a while. Mapping Katie's question about existing costs. Other questions about trying to map existing benefits. Capturing that in the single working group as a catchall for these issues. I'm more than happy to pull those back out.

>> Okay, well then I mean if that is what the awareness and adoption working group is for I think that an additional bullet point should be the attempt to determine whether or not this will actually help people become more secure Based on some of what's, the survey of what is occurring today and existing costs. When I look, there was a recent study it was Kenna security did a study in 2017 that looked at patch strategies, remediation strategies. So, looking at two factors of coverage and efficiency, basically you'd obviously want in an ideal scenario you want hundred percent coverage of applying known patches and 100% efficiency. You know. But they looked at it prioritization based on [CVSS] score and then they looked at prioritization based on just targeting vulnerabilities for the biggest vendors. And they found that actually using a random, random just rolling the dice on which vulnerabilities to patch ended up being as efficient as just a strategy of patching, you know, maybe CVSS score of seven and above or something like that. So the whole point if that's what awareness and adoption is we should be examining the question of will this make a difference. Will this actually make people more secure

>> No, I think that Mike [Vareko's] work on showing that patching is a function of using either a companies special sauce or just exploit in the wild is the best option. Don't want to devolve to a patch a strategy question. Yes?

>> That same study shows that if by known vulnerability in either [meta-sploit] or SPDD was 30 times to be exploited

>> How dare you.

>> Just proving all the great service that that free open-source project in [exploit] provides but efficacy totally matters and I think that's part of what, I mean, Tom left the room, the awareness and adoption discussions per FSI [sacker] per sector is to see which value is being derived from the experimentation or which concerns there are but also to your point, the FAQ so we make sure we are getting past the superficial stuff.

>> Jen?

>> Just trying to recap something that I think I heard, which is that on the awareness and adoption question that while you were trying to get what Tom had been talking about about how do we actually drive future adoption and make it easy for people who don't necessarily like naturally get it and all that kind of stuff, which I think is a really great goal, but what I'm hearing from people in the room is that that's a premature concern for where the project is right now given the other working groups. And the things that you were talking to and other people and are more talking to as being benefits that we could do right now is much more about capturing case studies it sounds like of people who are doing it today. So maybe to create a little bit of clarity and get rid of some of the confusion we just rename the group to being something like a case study group and it's much more about capturing the benefits of what people are seeing today if they are seeing benefits what the hurdles have been and all that kind of stuff.

>> Great. I like it. Yes?

>> I just want to say that I like the fact that we are scoping it to or it seems like it is a fact that we are scoping it to the list of components and not the warning labels partly because my sense of my own experience with the NVD stuff is probably the reason why CBEs are hard to use because the CPEs are really hard to map to anything useful. And since we've already heard that CPEs, two software components are linked in with SPDX, if we solve that problem then we have done something which I think makes NVD more useful.

>> Great. Bruce you have a microphone on. I can't tell if I've been ignoring you for a while.

>> Yes I just want to make an editorial comment about surveys right now. And I'm not saying this to be difficult or anything, but you know, throughout American history in terms of regulating behavior whether it be through industry adopted regulations or I should call it self-regulation or through government regulations, people have tried to

play off two sets of costs. One is social costs against kind of the cost of implement in the technology or something like that. And you know, that was done, use the example earlier today, seatbelts, auto manufacturers talked about the cost of implementing them and the impact it would have on the ability of people to buy cars and all these things and ultimately that was just a way of avoiding doing the ethical thing. And I really want to stress that this isn't something we are going to be able to prove the value of early on in this. People didn't even know what S Bomb is an people patch poorly right now. So this is about trying to change how people do things and change the awareness around information security and practices. And frankly I will speak from experience ramping up security programs at hospitals. It's messy it's ugly and we spend a lot of money that's wasted initially because I'm trying to change a lot of behaviors and things. It's not efficient and it gets efficient over time. And so as we talk about that I'm not opposed to doing surveys and things and looking at current state and looking at metrics but let's acknowledge this is a long game, so to speak. This is not something that's going to take effect in six months.

>> Excellent. So we have 11 minutes left. First I want to make sure that if there is anyone who's watching or on the phone please do chime in. We are going to make sure that we capture it. I'd like a couple more quick comments on working groups. It will be your last chance to throw something on the board and we are going to sort of see if there are folks in the room who want to take a leadership position and then we are going to talk briefly about moving forward in terms of timing and scheduling and all that fun logistical stuff. Seth?

>> Kind of a working group but not within this group I just want to make a shameless plug for the healthcare sector coordinating councils newly announced S Bomb effort, that is healthcare specific. That is healthcare sector specific. So we don't want to, to Josh's earlier point that we want to make sure that that has sufficient informative focus in there that it doesn't miss broader opportunities and just focusing on healthcare. One of the things that we didn't talk about in here that pertains to healthcare gets back to our boxed example is does EHR fall into that category pits of those are the kind of things we don't want to miss out of studying this group just because of the folks that we have that are willing that would get captured in healthcare but will not be talked about in this group necessarily.

>> Thank you. And I think that de-conflict and collaboration is something we can work through to make sure there's productive work going on but we are not duplicating anything. Art?

>> So, sorry, so case studies, proposed notional working groups, case studies, what's going on today, there are some examples we've heard today about what people are doing something and it's working, gathering more participants. Okay. Standards review, what standards exist today?

>> And Kent, is the goal here to see if we can sort of lay out here's how this can be done with what we have today? Okay, so standards review

>> And feasibility. I think I would propose another working group where it might replace the transparency one and I will call this the scope working group. So I still like the idea of having a little bit of consensus today at a high level, but there could be more thought about scope. We haven't got the granularity level yet. We haven't got the size of the box, the 3-D box. There have been like five different discussions about what size the box should be so a scope working group could at least propose some things and maybe where a boundary line is between feasible and what the stages of time you talked about earlier. And that might incorporate the transparency 2.01

>> Scope for today and tomorrow as a Disneyland-esque name? I don't want to lose the thoughts that came out today, which is there are some complexities. But keep going I'm sorry.

>> Basically that's it I think I would maybe call it a scope working group and the way I'm thinking about it transparency 2.0 would be part of that. Again, just talking out loud.

>> Great, Michelle?

>> Thank you for putting that on the board now because I've been trying to actually get a scope working group on their but I keep talking about but I would actually add scope and goals because what happens is after working in standards for the numbers of years I have people conflate goals and scopes all the time. So if you have them both in one working group they can kind of separate them out where they belong. So you have a scope and a goal coming out of the same group of people I think would be really important.

>> All right. Josh?

>> Since Seth's actions are going to impact my business sooner than probably this working group will and since several people have flags and operational challenges like residuals or people expecting a clean bill of health, could we maybe nest under the case studies it's not just case studies but also like a running list of concerns? And in some sides you get triaging and FAQ like oh I understand your concern and here's an answer for it and some of it would be here's a concern we don't have an answer for but I don't know how to label that one. I don't want to wait until phase 3 of this to actually solve real-time problems.

>> We did have the thought of having a challenges and external concerns working group, which was looking at edge cases and some of the problems that we are going to sort of come up with, which may be similar to what you are looking for. It could be incorporated into one of those.

>> In part does that fit into the scope issue of sort of the possible how to address future concerns and complexities? Where does that issue fit, something that's been on the table all day? The concerns that should be addressed.

>> In the transparency to 2.0 because edge cases might drive too much

>> Katie?

>> It seems like scope and goals is going to read the other working groups because everybody's going to want to be involved in scope and goals. So maybe that is literally the only thing we do as next step just as a suggestion.

>> Does anyone want to do things other than scope and goals?

[Several background voices]

>> I do see what she's saying. If we are going to have a scope for all these things you kind of have to define and it's not that the other things can't start, but the scope and goals one needs to happen soon and be done soon doesn't it?

>> Yes I think that should certainly be a priority. I know for a fact that there are people in this room who want to do work now.

>> We are going to do work now. Let's just be very clear about it

>> You can use scope and goals to have a very productive discussion but I'm not convinced that scope is something that unless it is a high level it's going to depend on what we have, the tools if you want to do it today, or how you want to talk brings through in the future or gathering data. I feel these are all separate enough activities but if you think that they should all be conditional and we shouldn't move forward on any of them, suggest it.

>> Well I don't think it's, I don't think it is necessarily conditional I just think that it's going to be a little bit inefficient. Perhaps the case studies could be done in parallel of surveying what's going on right now but that would then inform the scope and goals right? I think may be a bullet point to add under scope and goals of what would be covered would be anti-goals, to making sure that whatever it is that gets created doesn't do certain things. And then the last thing that I would suggest going under scope and goals would be frequency and that is going to be actually quite important. The frequency of doing whatever it is that ends up being scope.

>> So we have three minutes left. We have the folks who are going to do the standards and rebuilding we have our leaders there. Katie would you like to be one of the people behind the scope issues, scope and goals?

>> Sure.

>> Is there anyone else who would like to be the coach or

>> Oh no, you said behind. I was listening to you. Nine mean, here's the thing, I definitely would want to be involved in that one.

>> So forgive me, going to cut you off. I'm looking for folks folks in this room don't have the time and bandwidth to be volunteering to be cochairs that's okay. Is there anyone who would like to volunteer to be a cochair of case studies, medical device pilot, scope and goals?

>> Medical device

>> I was going to say [inaudible]

>> Michelle, Jennings, anyone else? Case studies? Josh, Jim

>> I will go in on medical devices with Jennings.

>> Fantastic. Anyone else for case studies? We will find that. We are running perilously close to penalty time. Can you pull up NTIA slides?

>> Point of order. Just as logistics going forward, in past NTIA multi-stakeholder processes we have had a mailing list that you can then send various information to so that folks could have these kinds of quick conversations we organize, but we organize we create the lists for the individual working groups themselves and whatever mechanism we are going to use to coordinate. So, is that the process we are going to use now, and if so

>> That is the process we are going to use now.

>> If so then some of the conversations about the initial working group setups can also happen on the major mailing list.

>> Yes, that is the plan What I wanted to do in the last minute is to say this is something you want to make sure we can continue the conversation moving rather than scheduling things ad hoc so the next in-person meeting we currently have reserved to be right here, November 6. Before that we will have a virtual meeting the week of September 17, sometime that week. We will be publicizing this, so if there are things going on that week that we absolutely should not conflict with, obviously this is a group of illustrious important people. Nobody is going to be free all the time. But we will try to schedule something for that week. That will be slide share, conference call, probably three hours-ish long. We will see how short we can make it. We have another virtual meeting after the holidays, another in person meeting in the spring. If people say no, we would like a different schedule than this, or you would like to meet in person not in DC we can talk about it. This is something that we want to go where stakeholders are. We want to make this as useful and as productive as possible. But we also want to make sure that we keep moving forward from a progress perspective. So we are going to send out a summary of this, the slides, the description of the working groups, going to reach out to some people who did some of the talking to do the initial refining. Once we build up the consensus, each group will sort of further refine their own mission. But we

are going to make sure that this is something that can happen together. NTIA is here to be a resource for you. If we can help with call bridges or help with document drafting we are very eager to. If you know how to run your working group, that's okay too. We don't want to impose ourselves but we are here to help. And finally I want to thank Megan for all the help documenting things today

[applause]

>> And much more importantly I want to thank all of you for showing up. We don't agree on everything but I'm really impressed at how much progress we made today. So thank you and I hope you feel that you did a lot of good work today. And thanks to those of you watching the webcast.