NTIA Meeting -September 12, 2017
1-Welcome

Thank you, operator. Thanks, those of you who were able to make it into Washington today. And, of course, thank you to those of you who are watching online and listening to us from the ceiling up above. I'm very excited to see all the progress that's been made in NTIA's multi-stakeholder process on patching and IOT security update ability. This is something that really depends on the hard work of all of you, and I think it's actually a good sign that we have sort of shifted from lots of contentious discussion to basically just sitting down and writing and doing that final document, editing and nitpicking, because that means that we're coming down the homestretch and going to be able to make some progress.

So, today's meeting is going to be all about looking at what we've done, making sure that we all like where we're going. A few of the documents, I think, are pretty close to finished, and so we can talk about what we want to do with those. And the second part of the meeting today is going to be devoted to saying how do we make sure that what we've done has an impact; that it matters, because all of you worked really hard to make some serious progress. I think the documents that we've put together are fantastic. But it's not just enough to write a document. For some reason, just the existence of a government document does not magically make the world better. And so, it's going to be up to us to say how do we take this out to the community, how do we take this out to industry, to consumer organizations, to advocacy organizations and make sure that we all really take a look at these complex problems, that here's one piece that we can all agree from different perspective that we've made some progress on.

So, before we jump in, I would like to turn things over to my boss, Evelyn Remaley who keeps an eye on the big picture of things, and she can tell us a little bit about where we are in the process.

Thank you, Allen. First of all, I just want to welcome you all. Thank you all for being here today, those who are here in the room and also those who have called in today and are looking at the webcast. I hope that everyone's families and friends are doing well with the events in the South, and that it's nice that you could all make it here today. I know that many of your companies and the civil society players play a role here in response and keeping people connected during these disasters. So, we thank you for still making time for this process as well, and for all that you do to keep people connected.

So, let me just jump in. I heard someone out in the hall say they were ready to get multi-stakeholdering, which I think is very appropriate, so we're ready to jump in too. Thanks for the work that you've been doing for the last 11 months. We first met back in Austin in October, and here we are 11 months later, and we've been really pleased with all of the work that you've been doing, and we appreciate the commitment.

As I said time and time again, NTIA believes that an open consensus-based process that brings stakeholders from across the digital ecosystem is one of the best paths forward to addressing security issues in a realistic and timely fashion. As we come down the home stretch of the drafting phase of this particular process, I thought it would be good to acknowledge how far we've come and place this work in a broader context. This process began last fall. NTIA had been hearing from stakeholders that IOT represented enormous security concern. Left unchecked the wide propagation of insecure device could undermine not just the rapidly growing IOT landscape but the broader digital economy. At the same time, many of you were very concerned about an overly prescriptive regulatory model. Nobody wanted the government to decide what could and couldn't be hooked up to our network. NTIA chose to focus on the question of patching and updating as a means of making meaningful progress in the discussion of IOT security.

At that first meeting we had a constructive, if at times contentious, discussion about how to scope and orient the work in front of. We haven't covered everything from that first meeting, but as a group, we have addressed a wide range of issues. The documents we're talking about today deal with the technology and the policies, and speak to different aspects of the ecosystem from the manufacturer to the end user.

At the last meeting, a virtual meeting in July, we found consensus around the work that the communications working group produced. Two other groups are in close to final versions of their documents, and we'll have similar discussions on those today. We'll also hear from the capabilities working group, which has been making solid progress. We understand that this can be slow work, but

careful deliberation allows us to make sure we're capturing the consensus from the entire community. We have allocated a lot of time today to talk about how to maximize the impact of these documents, how to spread awareness and adoption, and there may not be easy answers, but hopefully we can collectively brainstorm and take advantage of the important communities to which you all belong. Where can we promote these ideas and who can we engage? These are questions that we hope to talk about today.

Many of you have heard about the cybersecurity executive order, which was announced in May. One key component of that initiative is on botnets and other distributed automated attacks. Obviously IOT security is a key part of the evolving threat we face from botnets. NTIA issued a request for comments to help us understand the evolving threat and heard from 47 respondents, including many of you in this room.

The importance of securing devices and endpoints was probably the largest theme across the comments. Many comments highlighted the work you've done as an important way that the community can work together to address these issues without regulation. We want to hear from you today about next steps in the IOT security space. As we heard the response to the EO, there is still a lot of work to be done. How that can community using these stakeholder-driven processes make further headway on this topic? That's also an issue that we want to dive into today.

Securing the Internet of Things remains a critical issue across the government. The work that you're doing has attracted real attention and we're confident that this approach can have a substantive impact on IOT security, as well as security and trust in the broader ecosystem. Furthermore, as everyone here knows, IOT security transcends national borders. The issue also has the attention of other governments and organizations around the world.

Those of you who have actively engaged in this process are working hard to demonstrate that solutions can and should start with collaboration between the experts in the private sector, the security community and civil society. We thank those of you who have contributed thus far and appreciate your continued commitment to this effort. And with that, let's get started. Thank you, Allen. Thank you, Allen.

Thank you, Evelyn.

Okay. So, for the company, that we were actually were working exists standards tools and initiative workgroups. The goal was to go out and to identify and gather information related to existing standards that were already created out there to help the other workgroups in their endeavors. So, during this process, we wanted to obviously avoid duplication so that we weren't off trying to recreate something that had already been recreated, identify the needs of the various workgroups and be able to bring that research material back in.

We did this in a global aspect. We didn't focus just on U.S.-based organizations. We looked at any and all organizations that may add value back to this process. We also even dug into and looked at specific maybe companies or individual organizations that we typically would overlook. We dug into a lot of those, trying to identify any one of them that may be producing information related to patch and patchability that come back to this overall workgroup effort. So, also looking at -- I'll go ahead and jump over here.

So, in this effort, we went ahead and put together a catalog entry description. It's kind of laid out there on the screen there we can see, where we document the organization, organization's URL, a summary of the information, then individual documents or group of documents that may be of value related to patch and patchability. This was at least a very time-consuming effort. A number of people put a lot of work into this. We went out and proceeded to identify every group organization that we could imagine and start doing research, and this actually involved going out and reading a lot of documents, parsing out a lot of documents, looking for anything related to patch and patchability.

The unfortunately aspect of it is, I'd say probably in the 90-plus documents that we looked at, the information that was gathered stated we should patch, and that's about as far as it actually went. There were a number -- a small handful, maybe three or four organizations that went a little deeper, and those kind of focus -- there happened to be one organization, Alliance Internet of Things, which was a European effort, had a little more information discussing around patch and patchability. And then also industrial automation organizations obviously had more defined information around patch and patchability. But other than those two key organizations, we found very little, unfortunate, which was somewhat disappointing. So, we continued documents this information for the purpose of gathering everything, and it's in the document that's available online. That's online now; right, Allen?

Yes.

Okay. That document is online. So what we wanted to do is we presented all the material that we look at, so any organization that had any kind of reference around IOT, IOT security, we wanted to put into our document so that it could be used, hopefully, in the future, and we can go beyond this organization with usable information by combining this into one structure, where we could easily go in and search and identify other organizations that had discussed IOT security in general, and that's kind of where the document is right now.

And then this brings up a number of questions; okay. And it comes down to, from this document, I don't know if everyone's gone out and looked at this yet or skimmed through this, but where do we take this from here? Obviously, I hate to see this effort just be throwed to the wayside, so we kind of propose possibly taking this document and continue building upon it, basically creating a clearinghouse of information around IOT, IOT information. IOT security information is kind of where we want to go. So, we kind of proposed that question out to the group, where do you see this possibly going in the future, where would you like to see it go, and just to throw a couple ideas out there, we had actually discussed making this basically a web-type documentation, where people could submit information to this using the standard form.

Now the document that we produced -- that we put out does not contain all these fields. I actually stripped it down just down to domain accessibility, because we weren't good at gathering a whole lot of reference material between beyond that, so the current document contains information down to that point, and hopefully this would be a document that, if someone was wanting to do further research around IOT, IOT security topics, they'd easily be able to go to this document and find further usable references, because,

obviously, IOT security concepts are not going to go away. We're always going to be building upon that, and we need this source of information.

So, I kind of propose, actually, putting this somewhere and creating a web interface where people could come in and fill out these key pieces of information, then we could vet it, which would make it fairly simple, validate this is valid information to IOT and IOT security topics that would benefit everybody and create this as an ongoing document that we could maintain, making it possible for further research. So, that's kind of where we're at.

I hate to cut this thing short. And I'm interested in any kind of feedback to this group, to this workgroup on what you would like to see. So, I propose everyone go out there, look at this documentation, think about how you would like to see this move forward, and that's where we take it from there.

Or, the other thing, and we've had this discussion also, is there anyone already doing that out there that we're aware of? And I know there's a couple small organizations that we with found, that we've heard about, we'd like to identify them. Maybe we can work with them, combine all this information with them as a possible solution. But we see this as an ultimate goal, that all this documentation is put in a single clearinghouse place where we can get access to it and put into a form that we could actually continue to maintain and grow without a lot of effort, because obviously this is process was very time consuming and we definitely don't want to see it become old and date it. So, we have to put together a process and find a place that we can host this from with the right web forms, web support to continue maintain this. This kind of where we see this going forward.

Excellent. So, first, we want to see if Kent has anything he wants to add, your co-chair. And Susan, can we open up Kent's line, and we can also move into Q&A mode.

And, sir, your line is open.

Well from the standpoint of -- this is Kent Stanfield. From the standpoint of really trying to decide how to move forward, that sort of discussion that we're hoping to really have, you know, where does this -- you know, we have as a working group, understand what we think would be valuable, but what do others think? I mean from the standpoint of trying to locate someone who is already doing something like this, I actually was, at one point in the past, pointed in the direction, but never received the URL after the fact. I think it was at an earlier meeting, the one before, in April. But we haven't been able to locate that site. We do need someone to take this information, and if anyone has a good idea, whether that be an existing facility or where we should take it within the effort, we'd greatly appreciate that.

Kent, have any organizations been suggested?

One was, but, like I said, they said they'd send me a URL of the site, and the organization, and that was a hallway conversation, sadly, and never received that. But there has been some discussion about NTIA probably taking, you know, the responsibility of putting up a web dictionary, catalog, whatever you want to call it, of sites like this so that we can combine some of that into a central place. But, you know, if there are better places, that's really what we're trying to look for.

Thank you. So, I think now, Susan, can we open up the call line to Q&A mode, and if you're listening on the call, hit "*1" to join the Q&A queue, and I think now we can have a discussion about this if anyone in the room has some thoughts about what we can do with all of this data that we've collected, and how we can make sure that community can continue to use it and build on it. Hit the mic too.

Okay.

And just for the first few minutes, introduce yourself when you are speaking so that everyone knows who we are talking to.

Yes, hi, John Banghart. I'm one of the working group chairs for working group four, so you'll be hearing some more from me in just a little bit. Kent, I missed the beginning. I came in a little late. So, I apologize if you've already discussed this. But have you considered whether or not it would be a worthwhile effort to go through these documents and start to identify common elements across the various standard efforts that are out there? And, granted, that might be a heavy lift. But it might be useful if we had a sense of where are these various organizations, regardless of whether they're government, private sector, international. Are folks leaning towards sort of common ways or common standards around this?

Yeah, John, that's an excellent question. From the standpoint of taking it, really, a step deeper into the examination, initially, our effort has been really focused around trying to identify, locate, read through for applicability these documents, and that's been reasonably time consuming across a scattered set of people, yourself included. And it makes a lot of sense to try and go and look at those that do have the specifics around patchability, what are those common threads, and I like the ideas myself, but what do others think?

Excellent. We have a question on the call, Tim Thatcher.

This is Tim thatcher, USA, and apologize in advance, had some trouble logging into the Google Group, so I'm not quite familiar with every single piece of the content. But my question relates to are we considering integrating privacy considerations into the IOT standards, and if so, what does that look like?

So, Tim, that is a fantastic question. I'm going to take the moderator's prerogative for a moment. On one of the early discussions this community had in January, it was a virtual meeting, and someone suggested should we think about privacy as well, for the purpose of this discussion, and talked about it for a little bit and decided that, no, it would be better to focus on security updates and patching for this perspective, that if we wanted to expand the conversation over time, then we can do that in the future. But we were trying to focus it on patching. But on the standards side, I will now turn it to Daryl, the co-chair, who will answer further.

Yeah, in the current state of the documents that we have out there, like I said, there was only a small handset that was patch patchability related stuff. And to jump back into John's question, I think it would be good to possibly break this down a little further. I'm not sure if we could get down to that point without putting a large amount of effort into it. But I do like the idea of the possibly breaking this down.

Now we broke it down based on industry. I tried to, you know, whether it was the documentation based on industrial. Was it based on automotive? Was it based on consumer-type stuff? But there may be some other categories that may be of some value that could potentially be added there, including does this document talk about IOT privacy, as an example. So, we may be adding another category down the road to this that may add some more commonality so we can go, hey, if I'm doing research and I'm interested in, let's say, privacy, or I'm interested in, you know, firmware upgrades or I'm interested in some other specific topic related to IOT security that we may be able to put some kind of tags also in these documents that would actually narrow them down. Of course, that's going to take some more man hours to go in there and review these and try to break it down to that point. But I think that's possible and maybe even practical.

And if we put this documentation online and start growing it and create a form-based structure to it, then the people who want to add something to this document standards could easily already know that piece of data or gather that data initially and put it in there, making this more defined and more specific, where somebody could actually narrow their search topics down to those specific categories.

Thank you, Daryl.

So, this is John again, if I can just react to that. I think that's great. One consideration on how to scope it, because I agree, I mean, that's a big effort. You guy haves found a lot of documents. You know, would there be utility in scoping it around, well how many of these standards, how many of these documents say that patching is important, and under what circumstances; right? I mean that's one of the things that we've

struggled with in our own working group is trying to figure out, well, what's the incentive to build patching in versus what are the barriers? And so, getting a sense of sort of across the universe of folks that are thinking about this issue, yeah, we think it's important in this circumstance. We think maybe it's not so important in this particular circumstance. And I don't know if there's risk there for that, but it's one way of maybe scoping it that may have utility but doesn't require kind of going all the way down into each individual recommendation, if you will.

Great. I have one and then two.

Good morning, Elaine Newton with Oracle. I'd like to suggest that a multi-stakeholder organization be the host of any future web-based effort. I think it's important that a U.S. Government Agency set a good example for other foreign counterparts and make it clear that this is a community effort. It has input from all sorts of stakeholders.

Thank you. Katherine.

Hi there. Thanks Allen. Katherine Gronberg with FourScout, and I was part of the working group. You know, just as a broad brush of what the findings were, is that the vast majority of organizations didn't really go to much fidelity in terms of prescribing or stipulating, or even recommending circumstance for patching and updating. The vast majority of them simply recommended it as good practice. A few of them -- I note the more industry-specific groups -- had somewhat divergent recommendations, and, you know, for obvious reasons, concerned some of the more specific considerations for their industry. For example, noting where things were air gapped, and, thus, would or would not be necessary to patch or update.

So, I do think, like Daryl said, we could go probably one level deeper to ID those organizations that went farther than simply recommending it as good practice. But it starts to split out pretty quickly for the ones that did get specific.

Further thoughts about how we can use this database, and perhaps equally important where to use it? I have Joe Jardenbeck [ph] on the phone. Can we open Joe's line.

Have you already had the discussion about which standards bodies you'd like to see this resident in, such as either IETF or Oasis, as good examples? And with Oasis standing up new technical committee, you can just present this document to them as a starting basis.

That seems like a -- there are organization that is are in the process of doing this. I think it would be very helpful. Anyone in the room have thoughts or have worked with Oasis on this front before?

They recently started a technical committee that's a user council. They're not actually using standards, so that's one possibility. And I'd throw in IIC, or maybe talk to someone at IEEE.

IIC is the Industrial Internet Consortium, and I know that you guys are kind of the pretty active working group member from IIC. Kent or Daryl, do we know, does he have any opinions about whether or not the IIC was going to play a role in this?

[Inaudible].

Okay. We did not. [Inaudible].

Well, IIC is very instrumental in helping to get standards out there and is not a standards organization.

Sorry, there was a comment in the back.

No, there was quite a lot of talk about all three of those organization, and, you know, that might be the useful part of this is to ID the organizations that spend a lot of time on it, versus that those that sort of, you know, note it and move on. There are some that are quite much more active, where we found a much

richer body of documentation surrounding starting with definitions but moving, then, into more prescriptive direction. So, I think that that's a good starting list for sure, and those names came up over and over.

So, perhaps we can continue this conversation a little bit later as we sort of transition to what comes next. But I think two things that we may want to think about are at what stage do we, as a multi stakeholder community, want to say we have done enough, let us hand it over; and then, two, what do we want that hand over to look like? And does anyone have some initial thoughts to start that conversation? What are we looking for if we hand it to one of these alphabet organizations that we just talked about?

Yeah, Allen, this is Daryl. You know, what we're looking for, often, you know, I've seen a number of organizations start something like this and it die quickly, and that's what we want to avoid. If it's going to be of any value going forward in the future, it needs to be with an organization that is going to maintain it and is going to add content to it. It needs to be a living breathing document. Things change, stuff gets old, new things come in, so it's important that whatever organization or ever who takes this on, that it continues to be maintained, or six months or a year down the road it becomes totally worthless, and that's one of the things we need to avoid.

And if you go out and look at so many organizations and so many standards that have been created, they're created and then they die. No one maintains them, and this could be the same way, it just becomes a conglomerate of old data that's no good, and I'd really hate to see that happen. I'd rather it not even be created than not be any good. There's nothing worse than going on the Internet and a doing search and finding a site and going, hey, this is what I'm looking for, and find out that it's ancient data that serves no purpose.

I think this data is wealth of information if it's maintained moving forward into the future, and that's where we need to do, and that's what we need to look for to do that. That's what I would expect this to become.

This is Kent. Can you guys hear me?

Yes, we can.

Okay. One of the things that we have noticed over the last year, and I think in some respects it's because of some of the efforts going on here, we're seeing more standards organizations actually try to take the topic on and look at this from a real development perspective. Oasis, I don't think, is one of them yet, as was mentioned a few minutes ago, a suggestion by Joe. But there are others that are contacting us and that are in our documents. So, that's a positive sign and sort of goes to what Daryl was just saying. You know, we're going to see a lot of change in this area over the next six, eight months, and longer even, and we'd hate to have this information go stale, especial so quickly.

Any further comments in the room? We have Tim on the phone.

Somebody kind of mentioned already, I was just going to mention that they definitely should have credibility and have an international reach, given the topic.

Excellent. Thank you. I think that's making sure that it is an international organization is something a lot of people in this room feel strongly about.

Bill Check, Fen CTA. I think the other thing is following up on, Daryl, what you were saying, that it's really important to look at what resources any organization is going to be able to apply, not just that they can maintain it but are they going to be able to devote some resources to it, either in terms of actual hosting of the site or supporting the site or, you know, some tangible resources that are going to be dedicated to this?

Thank you. Further thoughts? So, I think we can revisit this a little later on today, in terms of moving forward of what, we as a group, want to do that, and how we want to manage that handoff. But I think certainly NTIA is very happy to play any role we can play, but there are strong benefits to having us be

part of something that is, in fact, multi-stakeholder, international, well resourced, and we like to thank the Department of Commerce, as many of those things, come budget time, we want to well resource, but everything else we try to make and play that role. But, again, there's a lot of important aspects in having industry engineering in that approach.

Any further thoughts from the phone? And I know that there are some issues with the phone, we're trying to work them out. If you have a question, I'm keeping an eye on my e-mail. So, if you're watching the webcast and you have an important question, please do send me an e-mail and we'll try to make sure that it gets on the floor and into the discussion.

And, again, if you'd like to ask a question on the phone, please press "*1."

Thank you, Susan. And so, with that, I think we will come back to this for a discussion about what comes next and what we as a community want to do with the work this working group has been work on.

On to the next working group, which is the technical capabilities group, and unfortunately, due to a variety of reasons, including, of course, the ever-present weather that is affecting America, we have not been able to find someone from the working group who is going to be able to make it today, so I am go to present the deck. But there are a few folks on the call who are going to help me. So, operator, Susan, can we turn on Chris Gates' line.

His line is now open.

Chris, can you hear me?

I can, Allen.

Fantastic. Thank you. I'm going to do a very quick walk-through of this deck and then I'll turn the floor over to you to capture all the things that I have wildly misrepresented. Does that sound fair?

I'm sure you'll do an excellent job. Thank you.

So, very briefly -- that's right, we have a touch screen. So, the goal for this working group was to really -- the current goal was to have a shared understanding of what an update means. We think this sort of complements a lot of the work that's happening from the other working groups, you know, what are the standards, how do we communicate with the end users, while, at end of day, what does an update mean and how do we keep them secure? And so, the current draft, which there are some copies outside, walks through the basic steps in over-the-air update process, and for each of the steps says, what are the risks, what are the mitigations, and what's the basic implementation for the security of those mitigation for each step, as well as acknowledging some of the residual risk?

So, the goals here is we're trying to make sure it's voluntary, we're trying to make sure it's nonregulatory, and we try to make it -- there's a lot of discussion with stakeholders, saying this is about objective guidance, so what are some of the tools that we have that come from existing and known standards, a lot of the calls to NIST's special publication?

The audience here is primarily, for shorthand, the working group uses manufacturers, but that really refers to solution implementers, system integrators, and anyone who is involved in producing IOT solutions. On the consumption, side we think more in the level of procurement, so if you have the technical sophistication to say I am acquiring a solution, what are some of the things that I need to make sure I have if there is going to be updates that are going to be updates that are going to be provided. How do we make sure they're not producing further risk?

The working group had a number of discussions about saying, should we be looking to communicate to the end consumer? Can we offer some kind of spectrum or guidance or metric? And at this point they said, you know, the first pass, that's not something that the group felt that they could do easily and cleanly, and rather than designing some sort of a metric that we would hope people would understand, for the first pass, we had the working group that focused on communications to the consumer, and so this is pitched slightly different approach.

So, the desired outcomes, a shared understanding of the component steps of an update and how you secure them. This is pretty similar to what was presented last time. The summary of activity briefly, the working group took a little bit of an exploratory phase to say what can we do. Initially they were looking at capabilities, looking at some of the lower-powered, lower-resource IOT devices, and I think after a little while, they said focusing on those isn't going to take us where we want to in the community, especially because a lot of things are now being deployed outside of industrial space, we can make more assumptions about the techno capabilities that are there, and so let's look at the nature of the updates. So, what are the steps that we'd expect in an update across the board, and define them as connected, remotely addressable so the working group spends a little time saying, well, what about sensors that are embedded on the concrete, that are disposable and you cannot connect to them? Well, we're not sure that should be something we should focus on for updates.

So, the other thing the working group did is a few participants raised, well, how do we develop the update, and they said, you know, again, for the work that this working group has done to date, that's out of scope. And so, how has the document evolved since July, since the last time we talked about it and you had a chance to read it? They're fine in motivation in the audience in the working group, so really making clear that this is not about the consumer explicitly and trying to offer some more explicit caveats, and rather than sort of having different layers of security, saying what is the basic security of limitation, once we have -- we're looking at the risks, we're looking at mitigation, basic security implementation, and then what are some of the residual risks people should think about?

So, I'm not going to walk through all of these steps. These steps have been in documents for the last two versions that you may have seen, but this just helps you see what are the different steps of an update? Some of them are explicitly security focused. Some of them are not but have security components. And others are neither security-focused nor do they have -- at least according to the working group -- strong security limitation. So, for this this step, the judgment is there is no security here, and that's okay. The trick is to identify what are the risks of each step.

And, very briefly, here is an illustration of what this looks like. Obviously, the text you have in front of you is in more detail. But one example is for the signed step, which is pretty early on in the process, the risks are on the sign code or insecurely sign code, they don't allow third party to maliciously push code to your device. That's usually seen as bad, I think. We have a couple security, Daryl, Thad? Thad; okay.

So, the mitigation says you should use cryptographic signatures. You know, just using a simple non-cryptic cache, that's something that toweled be easily defeated by most determined adversaries these days, so use cryptographic signature, and the basic limitation was to say, hey, you should follow a signature guidance from a NIST special publication. Stakeholders in the working group drew a distinction between signing your code and encrypting you code, because the risks are different; right? What are the risks of not encrypting your code? Well, the attacker can learn about your code. And if you're trying to keep that secret, that's important. And similarly, the attacker might be able to get some of the valuable intellectual property you have embedded in your code, and so that's important to you, then you need to worry about map.

So, the mitigation, of course, is encryption and the resources are to use some of the application layer NIST series. And if you are very determined about someone accessing see your intellectual property, then you may worry about having your code exposed on the device, so in your updates, if you have a full image, it hits the device. If it's encrypted but stored in memory in the clear, the memory isn't protected, then you may have to worry about that, and the document will offer some guidance on that first.

So, those are just two examples you can walk through, the sections are not completely finished. The remaining work is to finish the security guidance for each update. Stakeholders also said there are common areas that are across a number of the update steps, such as team management, which is always super easy. I'm led to believe that key management is something that most people have solved all the time.

A number of stakeholders have said, you know what, we've been working on this, but we want to show this to some people in our peer network inside our companies to make sure that we can do, that the technology and the recommendations are correct, and, of course, then, you need to do the full editing. There's still plenty of work to be done, although, again, the document looks fairly close to complete, and so, please, let me know if you would like to join this working group.

Chris, can you add some further commentary on the work that the working group has done?

Yeah. I think one of the things we've got to make certain we clarify is that this is not necessarily an approach for Legacy products. One of the things we took out of scope was this is for going forward, using the latest technology that's coming out for embedded devices, and what you can reasonably expect to find in your devices today. Highly resource constrained sensors or devices, there's not a lot that can be

done, and those literally have to be replaced. In fact, that's one of the areas in the medical device arena that they're talking about now, is how do we get rid of the old Legacy products so we can bring in the newer more secure products.

Thank you, Chris. So, is there anyone else on the call who is part of this working group? I'm just trying to scan the list of names here who would like to add about the work that this working group has been doing? As a reminder on the call, hit "*1," and if you are on the webcast and you still cannot get through, please send me an e-mail. We are trying to fix this.

I'm somewhat we haven't gotten a question about the encryption. I expected that to be a topic of conversation. One of the things, I'm a security researcher, I have over 40 years of new product development, and one of the things that occurs here is when I attach something, if they have a former update capability, I love to go after that, because I can then reverse engineer their code and lick the problem.

So, any thoughts on this work so far? What do we thinking about the direction this working group is heading? Yes, hit the mic and introduce yourself.

Yes, Chuck Powers Motorola Solutions. I think the work that's going on is great. I'm just kind of curious, in the working group, has the discussion come up of kind of the impact of a couple of these proposals, particularly encrypting the update on use of open source software? Because there are certain areas, especially if you get to GPL Version 3, you know, not letting people know what your code looks like is a no-no. And so, encrypting it -- I think signing it would be great, but encrypting it to prevent them from seeing it, I think that may be a path to open-source users may not be able to follow.

Chris, you wanted an encryption question, you got an encryption question.

It's a good thing. As a consultancy for new product development, we work, obviously, with a number of clients, and over the years I've done that. I don't know of a single manufacturer who rolls in any GPL license, and, in fact, there's a lot of effort and scanners in place to make certain you don't actually introduce a GPL license or a library. You try to avoid them like the plague. So, if you're going to talk about this serving all customers, no it's not. But as far as serving manufacturers, I think we're in safe ground in saying GPL is not something we roll in. All right. And that's apparent.

I mean, that's a fair point. I certainly am familiar with some developers who are using GPL code, you know, for better or worse. But just an idea that there may be certain users who might be interested in this, but there's certain things they can't do. That's just an observation. I mean, I don't think it should stop in any way, shape, or form the direction the group's going.

Absolutely.

And, obviously, going in and being able to reverse engineer something like that, or even close similar to a GPL or open-source project, that's a huge advantage if you're attacking the code, and if you know that there is an existing flaw that exists on that, I mean, partly you can exploit those. So, this is something you definite will want to avoid.

Fair enough.

I want to make it very clear for all of our friends in the FOS community that NTIA does not have any position on the merits of the open source line. Derek, on the phone, can we open up Derek's line.

Yes, sir. Thank you. Derek, your line is open.

Thanks, Derek Adkins from [inaudible] RS Corporation. Just if in terms of the last comment, I would say that I don't think encrypting over-the-air updates would violate, in any way, GPL. GPL just requires that you have accessed to the code but not necessarily through the transition. So, you can go back to the

manufacturer and say, hey, I want to get that code, and they have to give it to you. That doesn't mean the updates can't be encrypted.

Otherwise one has [inaudible] things like that. But that's notwithstanding, I think it is important to have updates be encrypted. I don't necessarily know it's necessary for the code to be encrypted at rest on the device itself, but I think the over-the-air part should be encrypted. And there's multiple ways of doing that, in both public key -- or key management, as well as on top of AES or pick your other favorite next generation, you know, decipher. But I think the signature is definitely a must. And I think for over the air, encryption should be a must as well.

And I should also point out that I think the document explicitly calls out the importance of if you're not encrypting the update at the application layer using transport layer security as another potential tool.

And that's something we should point out, by the way, because the focus is traditionally on an MIS IT perspective. If you're dealing with embedded devices, ethernet may not exist to you. You may be working over blue tooth low energy or some proprietary network, RF network over to a dedicated box, and maybe it goes out of a Wi-Fi, or it goes out of ethernet. But you have these stage unequal levels of transport security, so don't make assumptions that you have internet capabilities like CAs and stuff available when you very well may not. So, we very, very, very pointedly make this standard agnostic so we didn't constrain this, and this would work all the way down to sensor, all the way up to the large box sitting on ethernet.

Thank you. Further thoughts on this document, where you'd like to see it?

And, again, on the phone, if you'd like to ask a question or make a comment, please press "*1."

Please.

Just had a question about any potential future plans for a consumer-oriented addition or follow-on to this? I'm just thinking about the document that was adopted back in July. It did have a consumer -- or did include a consumer orientation. So, is there value new in continuing this work in order to kind of keep the two documents, or keep all four documents in scope?

Chris, you have opinions in terms of next stages, revisiting the approach to a metric, or something that might be consumer facing.

Ah, well we're getting a little ahead of the agenda. And I think, as you well know, Allen, I think one of the advantages is to encourage. This is a voluntary standard, and to encourage manufacturers to adopt this, I think something like a metric, where you could actually socialize this and advertise this and say, we are of a rating ten or five, or whatever it is that's good in this metric and this rubric to say, see, we're good at this.

And the problem is, rightly so, all manufacturers have a problem with claiming to be secure, because the second you do that, you become a target for everybody. And so, but coming up and saying "Oh, no, we're achieving this metric or firmware capability" really gives them something they can socialize and market and make, potentially, competitive advantages in the marketplace. This is a good incentive for manufacturers to adopt this.

It's also a great way for the end consumer and the purchaser to know is this okay to use in my garage? Is this okay to use in the surgical theater? Is this okay to use in an air traffic controller environment? Maybe I have certain standards that I need to hit, and it's not exactly communicated. So, you say you do update; great. There's a lot of ways to do that. Maybe I'm sending out completely unsigned, unencrypted, plain text out to these devices. So, this allows you to communicate this.

So, yeah, hopefully it's a follow-on activity. We will approach this and figure out ways to communicate this to the end user in meaningful and very simplistic way so they don't have to understand the cryptography or anything associated within it.

Thank you. Thank you. One thing I things we want to make sure we can do is loop in the folks who didn't focus on the consumer-facing communication as we did that. John.

Yeah. Hi. John Banghart again. I would like to take Cleat's comment even a little bit further and tee this up, maybe for conversation in the afternoon, which is, you know, we've touched on in other meetings -- our groups talked about it, other groups as well -- that there's a pretty natural Venn diagram between all four working groups. I think that there's some natural informative activity that goes on between them. I don't think that we have fully explored that, and I do think, you know, my recommendation will be, I think we need an effort from all four groups to come together and figure out how does our work inform the work that the other groups are doing. I think that there is an opportunity there to help bring the message together. So, I would just recommend we talk about that this afternoon if there's time.

Thank you. I imagine there will be. Any further thoughts on this document viewing the steps of an update, how to submit it? Daryl.

Yeah, I like this document. I like this a lot. I'm often doing testing and work for companies, manufacturers, and stuff like that, and, to me, besides this document working interactively with the whole other workgroups and what the end product is, I think this document can stand alone on its own, and it's something that, literally, I can put to use today. So, I'm looking forward to when I can actually start doing that. This is some really good work.

Wow, thank you.

Elaine.

Elaine Newton, Oracle. Has there been any consideration of proposing this to a standards organization?

So, I think, in the group, they occasionally touched on making sure we're using standards. Chris can weigh in on this. I will say one of the things we're going to talk about this afternoon is IETF is standing up a new organization, a new working group with the slight unfortunate name, Fud, Firmware UpDate, and that's something that we hope that we can gauge. And it grows out of their 4108 crypto work, so I think it's going to have a strong cryptographic sense, and certainly we're going to make sure that we engage, and the working group that is going to engage as well. Do you have other thoughts about how it can?

There are probably infinite possibilities, or at least hundreds of places that you could potentially go. But, I would -- my general advice on this is to -- if there's a group that's already doing similar work and the experts are already convening, that's a good place to go.

That's when we turn back to getting on John's point about the intersection. We turn back to Daryl and Kent you say is there a group where you think this work might be able to go that you've seen?

Both IETF, as well as ISO are addressing areas right now, or beginning to. So, it depends on pick your flavor.

That's fantastic. Kent, what's the ISO work going on in the space?

It's just getting started. There is actually a IOT-related area. I can get some specifics and send it out a bit later.

Thank you. We'll follow up and make sure the working group can connect with some of those. We may even have some participants already as part of the working group.

Sounds good.

And if I can chime in, I think that's great, and I think we should harmonize with some of these activities. But bear in mind, we're working at a much faster pace than most standard bodies do. And I say that as somebody who sits on about half a dozen different working groups with different bodies. It's an extremely slow process. And, so, I think that's fantastic if we're going to do that and harmonize with those, let's not abandon this effort, or give it up to that space or development.

Agreed. That's one of the things that always frustrates folks like us who need solutions today, but at the same time, have to wait two years, or longer, the get to something they could have gotten in six months with a little focus.

Yeah. Yeah, I have spent multiple hours debating a single bit in a Bluetooth special interest group, working group, and it's like this is really painful. So, I do appreciate the agility we displayed in this working group with NTIA.

And we will allow the rebuttal in defensive standards from Elaine Newton.

No, I want to be in defense of doing quick drafting through groups that are less formal, and basically expediting the standards process by getting a document that's created through a multi-stakeholder process. And you also have a document already to fall back on while it's going through a more formal standards process. The pain is it helps multinational corporations implement those and do it one time.

We try to. We always try to work closely with our NIST and former NIST friends.

Totally agree that that's the best way to go. I really do. And I get this, and a lot of this was informed with personal experienced with clients. Manufacturers need help. They don't necessarily need you to tell you how to do it, but they need you the best way to approach, it and they can tailor it to fit their comfort level, and so that's kind of part of what we adopted is, we created this.

Speaking of NIST friends -- oh, go ahead, Kent.

I was going to say one thing to note, to that point, in June we attended the first conference and gave a talk, a few of the chairs. And it was amazing that after the talk, which was well attended, after the talk, we had two manufacturers come up and talk to us and want to know how they could get a copy of where we were, because they were looking to try to implement today.

Speaking of our good friends at NIST, Dave Waltermire on the line. Can we open up David's line. Hello? Hey, David, we can hear you.

Great. Thank you. Yeah, I just wanted to speak up about IPF firmware update working group. I'm going to be chairing that working group, and I wanted to mention that the work that we're trying to do there is really fairly narrow in this space. We're working on trying to develop a manifest format to allow for integrity production, identification, and applicability of a firmware bundle. And, as a result, we're not going to be doing things like, you know, developing process guidance and a lot of definitions.

It seems to me like there's an opportunity here for, you know, multiple standards organizations to work on this problem, and that, you know, through some combination of efforts we'll be able to adequately cover, you know, the space, and that the IEPF is not intending to -- at least through the firmware working group, we're not intending to fully cover the space.

Interesting, David. And I do want to give you some insight. One of the things you may want to look into is patents. There's 46 patents I've identified that deal with updating your firmware, and they break up pretty much between optimizing the transfer speed by patching and compressing and doing differences things. And the other one is man manifest, or an inventory ahead of time. And while in engineering, your mind goes to that, the first thing you should do is inventory the system and figure out what pieces need to go

where. Be very careful. Check those patents so you don't look at patent infringement as you go down those lines.

Thank you. Yeah, we'll take a look at that.

And I will connect anyone who wants to with David. Further thoughts on this document?

And on the phone, if you'd like to ask a question, please press "*1."

Let me point out one area I think we also need further work on is we kind of made a nod toward it as we were doing this document, but we didn't go into the detail, which is, when you update these systems, they are just that, a system. They are not a single server updating a single CPU somewhere. They are updating a system of systems, and so you have multiple programmable elements, both processers and potentially other things like FPGAs and CPLDs that are programmable, that are out there, that can be updated.

How do you roll back, in the case of failures, across inside multiple processors, inside a single box or single device, across multiple devices? How do you handle these kinds of failures? How do you notify and how do you back out so you do not wind up breaking the system? And we've taken some shortcuts in the document to make certain we didn't bump up against that too hard, and we also allowed for that kind of growth for the future in this document, but we didn't directly cover it here, so I think that's a potential area for future growth as well.

Thanks, Chris. Thank you. Anyone else in the room have last comments on this working group document? So, I will say, Chris, in terms of getting this to the finish line, you think a month or two more?

It seems reasonable.

So, again, not too late to weigh in. Please reach out to me if you would like to participate, or if you know anyone who should be participating in this group.

No further comments on this work. I think we can move on to the fourth working group on incentives and barriers. Sorry. Let me load this for you. John, did you give me slides? When did you give me slides; this morning? You're going to have to give me a moment, and we're going to start off without slides. Sorry about that.

No worry.

You have a mic though.

Perfect. Thanks. I'm just going to walk in circles around this pillar for the remainder of the day. Well, hello, everyone. My name is John Banghart. I've been involved in this effort now for several months, as one of the co-chairs for working group four. Our goal and mission was to look across the existing space, look into the future a little bit, hopefully learn a little bit from history as well, around what motivates putting in patchable or patching capabilities, upgrading capabilities into IOT devices, and what are the barriers? What prevents organizations, producers in particular -- and when we get the slides up, I've got a chart we'll be able to see. Allen, if you've got the old one, I can probably use that one too.

[Inaudible]. Sorry.

That's okay. So, it's an interesting challenge; right, because on the surface when the group first got together and we started to think, okay, how do you incentivize people; right, and we were in a meeting and a guy from one of the telecoms who was participating in our group, he said the answer is money, now what's the question; right? His point being, and he was being a little facetious, but he was also right in the sense that most commercial organizations are motivated by either incentivizng them through tax breaks, other types of mechanisms that make it cheaper or more, you know, cost effective to actually build the capabilities in. If it's too expensive, then they're not going to build those capabilities in.

So, let's look at an example that just came up. And I wish that I had thought to update my slides with this, but I think last week we saw the pacemaker, the pacemakers that needed a firmware update. Did everybody see that article? A couple people. So interesting use case here; right? So, this is a case where you actually have devices that can be updated; right? So, the FDA said these pacemakers, about half a million people have them, I think. It's a particular brand. The FDA said, you know, these devices are vulnerable. They can be hacked by commercially available equipment that costs anywhere from $35 to $3,000. That's a pretty wide range. I'm not quite sure exactly why you would spend $3,000 for the piece of equipment if you can just get it for $35. But that's what they said.

So, just to finish out that story, so, you can go now to your doctor or somewhere to get this firmware upgrade. It's not over the air. You have to go in. But, oh, by the way, getting the firmware upgrade could break your pacemaker. So, interesting decision point here, if you're somebody that has a pacemaker, do I not get the update and risk getting hacked, and what is the likelihood of that? What's my risk as a user here? Or do I go and get the update and risk, potentially, being put in a situation where my pacemaker fails and now I'm in the emergency room, maybe I'm having surgery, whatever the case may be.

So, the reason I bring that up is, it's a small sort of example of some of the things that we thought about as part of our group, around not what capabilities building in necessarily. Other working groups are talking about that, like working group three, which we just heard about; right? They've gone and talked a lot about what do you need to be able to do about that more granular level. But, rather, what's the decision-making process around do you put the capabilities in to patch and upgrade or don't you.

We heard a gentleman earlier talk about the fact that some devices are just going to be designed to be replaced; that they're not going to have that capability, but who makes that decision, and is it the right decision or wrong decision? So, coming up with a framework to think about these problems was really where our group ended up going. We didn't want to make policy statements. We didn't want to make recommendations around regulators should do this or should not do this, but, rather, let's focus on a way of thinking about a challenge that can be informative to policymakers, to users, and, in particular, to users.

So, I'll start with this. This is a taxonomy that we came up with, and I think this is an area where some reconciliation with some of the other working groups will help, too, on the definition side. So, we use the term "producer," as opposed to "manufacturer." And we've lumped a lot into producer; right? So, we've talked about software, so companies that would make software that would be used on these devices, the hardware manufacturers. In some cases, it's the same company. In many cases, it's not; right? You may have multiple companies making hardware or software for a single device, depending on how complex or robust that device is. But then, also, service, these are organizations that enable the IOT device to work. It could be a system integrator. It could be an internet or network provider, somebody who sits in that middle ground. So, we've got those three. And then I'll come back to the factors in a minute.

The other stakeholder group that we looked at the users; right? And one of the important distinctions that we made here is that there are human users of these devices but also in some context there are machine users; that is IOT devices talking to other IOT devices. And, again, other working groups have dealt with this same issue of thinking about it's rarely ever just a single discrete device that we're talking about. It's typically a complex collection of devices that could be sensors and hubs, different control systems that all sort of work together. So, we wanted to have a framework that would allow us to consider what about the interactions from one device to another, machine to machine, not just to how the human stakeholder thinks about this.

And finally, we used shorthand here in terms of the term regulator, and you'll notice that I've got both enforcement and voluntary under our category. Most people think of regulator from the enforcement perspective, and so we kind of debated whether to use this term or not. We've kept it because it gets people's attention. When they hear the word "regulator," all of a sudden, they're very interested in what you're about to say. So, we kept it from a pragmatic perspective. But, in reality, what we're talking about here, and that's why we've got enforcement and voluntary, we're talking about any organization that's going to come forth and say this is how something should be done; right? And whether they do that as part of statute, whether they do that as part of a standard, that's what we're talking about here, and accounting for those types of stakeholders in this mix.

And then finally, you'll notice we've got the factors there on the right side; environmental, interactive, and scale. And I took out my definitions in the interest of time. But environmental is what is the context in which this device is functioning; Interactive is how our users or other device is interacting with it as part of its normal function; and then scale is, is this a device that's going to be deployed in five locations or five million locations, because the scale makes a difference to whether or not patching is even viable over a network, whether you're got a constrained network or constrained devices. If it's just a couple, then, you know, patching may be viable from a technical perspective, but, again, if it's in hundreds of thousands or millions, or whatever the threshold is, the threshold in that context is rather, it's going to change the calculus around do we even want to try and implement patching here? If we build the capability to patch into the device, would we even be able to use it?

So, in the document itself, and I'll encourage you to please go and look at it. It it's up on the website. I think it's up there as of today, or yesterday. We're pretty close to being done with as far as we can take it, and I'll talk a little bit about why that is, so we're really encouraging folks to look at it. There's a use case in there that we fleshed out using just commercial grade dishwashers, something that you might find -- a Smart dishwasher that you might find in a restaurant or some other kind of shop. That will give you some better insight into how we think that this can be applied to some of the decision-making across all of the various stakeholders. But we want think people to think of other use cases as well. And that's going to be one of my big asks here.

So, once we kind of got to this point with the taxonomy and said, okay, so with our limited group here and the time we have, we think this taxonomy with the stakeholders and the categories and the factors, we think that that can account for most things, whether it does a good job or a bad job of doing that is certainly a place where we could use more feedback. But we think it is at least useful, if not fully complete or accurate. If we wanted to think about, all right, well what do we do with this? So, let's say we have a use case. We've sort of mapped this out. How do the different stakeholders feel about the patching

capability in a particular device in a particular context? How do we measure whether or not it's going to be a good idea to invest in that capability or not?

So, we came up with a method, a relatively simple method, and I will admit that, up front, some of the examples here are simplistic. We recognize that there's a lot of nuance and a lot of complexity that goes into this, but we think this is a good start. So, again, you can see here, we've got our three stakeholders. This is one example of a question that they might think about in terms of, do I want to build patching capability into this this device? Will I expect to support this device for several years? I strongly agree with that or I strongly disagree with that? The user incentive might be new features are important to me, yes, or no? If new features aren't important to you or the device doesn't need new features, then maybe patching isn't necessarily something, or upgrading, isn't something that needs to be considered? And regulator, you know, is the device going to impact physical safety, life, limb, and property. And, so, yes, I agree with that, or no, I strongly disagree with that. So that's an example of how they might think through that.

So then, and this might be a little hard to see in the room. Again, it's all in the document, and there's some additional diagrams in the document as well. We actually started to fill this in and started to draw out some diagrams here to start mapping them together. So, in this case, you've got a situation where the incentives and the barriers are basically the same. So, the producer is saying, yeah, I strongly agree. I expect to support this device for several years; that is, it's not a throwaway. It's not something you can just quickly replace.

The producer is also saying, providing new features to users is important, strongly agree. That's a decision point. You may not care about providing new features. And then patching could introduce new vulnerabilities; right? So, then it becomes an attack vector. If I can patch good code into it, can I also patch bad code, and here they said strongly agree. So, in this simple example you end up in the situation where the producer, just looking at those three criteria, are saying, well, I'm motivated to include patching but I'm also equally motivated to not; right? So, I'm not going to answer whether they would or wouldn't do it here, but it's an example.

So, let's change it up a little bit. So here, same three criteria with the producers. So now they're saying I strongly disagree. I do not expect to support this device for very long; that is, it may be a throwaway. Providing new features to users is important. Nope, don't care about that either, because of the nature of the device. But patching could introduce new vulnerabilities. So now you've got a circumstance where the incentives to include patching are not very big; right? Excuse me. The barriers are not very big, but the incentive to do it may be there because of the potential risk to users.

And then finally, a slightly more complex example, where we bring regulators into the mix. So now you've got a producer who is a weak barrier, I think is how we have this one. Yeah. So, producer with weak barrier, regulators with strong incentive, so you start to see the alignment.

So, what is the point of all of this; right? Our hope is that, as this gets built out, it can become a way of starting the discussion. So, you've got a producer, somebody manufacturing the devices. You've got a regulator, whether it's an FTC or a standards body, or whatever it is, in thinking about what do we want to do with particular kind of device or class of device, whether it's a thermostat or a refrigerator or a pacemaker. Let's have a conversation about what is the real risk here and do we want to have patching in these devices or not. This is a slightly more systematic way of starting to approach this problem.

So, the more you build out the nuance in terms of questions -- I strongly agree with this, strongly disagree -- it starts to tease out how the different stakeholders might be viewing the problem differently, which is a really great place to start any time you're trying to deal with these contentious issues.

It's very easy -- and those of us in this industry, you know, we're very good at scaring people. We can tell stories about scary pacemakers and we can say someone's going to hack your thermostat. In fact, one quick side note, we were at a meeting out at Black Hat, I guess a month or two ago. It's really hot in Vegas in July by the way, just to give you a head's up on that. But, so we were in this meeting and we

were talking about this issue a little bit tangentially, and there was a very smart, very well-meaning researcher in the back of the room that said, "Well, hey, why don't we give researchers the ability to remote disable devices and make it legal for them to remote disable any vulnerable device that they found. And I turned around and I said, "So, your notion is that we want to give a researcher sitting in sunny California the ability to disable my thermostat in Norway in the middle of winter because he found that it was vulnerable?" And he's like, "Yeah. Why not," right?

So, the point being that different people approach these problems differently. They've got different goals in mind. If we have a framework that we can work with and we think this is a reasonable starting point to start having that conversation and start understanding, well, how do you view this issue versus how does somebody else view this issue? What are the factors that are involved? And, again, do it more systemically or systematically so that we're not just telling stories. It's not just anecdotes. We're not just scaring each other or trying to sound smart. We're actually starting to break this down in meaningful ways that we can start to measure, and that brings me, too, to what I think is so important about bringing the working group's work together.

So, if you think about what I'm talking about here, think about what working group three has put together around these very specific capabilities and the associated risk. That's informative to some of these kinds of discussions. If we build whatever -- I don't remember the list of all the capabilities, but if we take capability one and we build that in, here's the risk that we introduce. Here's the risk that we mitigate, and so on and so forth. That should be informative into decisions like this. It should be a risk-based decision. It shouldn't just be making policy decisions because somebody got scared because there's a big scary story about how risky a device it. We need to have a more systematic way of approaching this.

And if this isn't the right answer, fine; right? Come and talk to us. Let's come up with a better answer. Let's figure out how could this work that we've done integrate with other work that may already be being done out there along this spot. But, ultimately, our group thinks that we do need to find a way of characterizing this, bringing it to decision-makers at the producers, helping users to have a voice in this and understand what do the users care about, and don't care about. But then also how do the regulators feel and the standards bodies feel?

So, that's the long and the short of it. You know, what we need is the same thing, really, that most of the other groups need. I would like to get this down a little bit more concrete. You know, we've got one example in the document. I think we need to get some more producers; that is, the manufacturers of these devices at the table or thinking about if there's side meetings that we can do to sort of get a smaller group together, whatever it is, to start putting real data in here.

What does it cost you to build patching capability into a thermostat versus not building it in? What's the real cost associated with that, not just in terms of the manufacturing cost but your long-term maintenance costs. Let's get some real data behind this. And how much do users really care? I've got a connected thermostat. I don't know if they're updating it or not. I actually do know. But if I was a regular user, I may not know. But if I don't care, if it does what it does what I wanted it to do when I bought it, then maybe I don't care if it's patchable. So, if I don't care and the producers don't care, well, should the regulators care? I don't know the answer to that; right? But everybody's got a perspective here. I think we need to start taking this framework, making it better, and start actually putting in real information.

So, if you are a manufacturer or producer of any kind, certainly want to hear from you. We're all users, so we can all contribute to that. Regulators as well. And, again, as I said, we'll not just talking about the enforcement side of regulation but also that voluntary side, folks that are working on standards that, you know, so much of what the working group, I think working group one has uncovered. We want to start bringing that together and focusing on this and turning into something a little more concrete just to see if it works, or if it even has utility. So, I don't know if I went over time or not, but I'll stop there.

Reactions? Thoughts? Comments? Phil.

Hey, thanks for presentation. I like the direction that that you've gone in. I had a question on stakeholders, the list is broken into major ones, and then within that there's several others. I didn't several on there that I would probably have expected to, like investors who drive, you know, in a lot of cases, whether a thing even gets made; retailers who have a lot of influence over what gets made, whether or not it has certain capabilities, how buyers perceive it, as distinct from regulators, something like legislators, so people who are making new laws or just convening hearings and things, that can have some drive in the ecosystem.

And then, difference between buyers versus operators, I don't think I see in there. Sometimes the two might be distinct. So, in hospitals, for instance, physicians are the operators but the hospital procurement system is the buyer. So, there might be different drivers. They influence each other differently.

So, no, it's a great point; right? And I mean, there's a certain boil-the-ocean problem here too, right? So, it's deciding what is the right level of granularity to start breaking this down. I agree with every single thing that you said; right, that there are a much larger number of stakeholders that we could start building this out to. I think, as part of any future effort, what I would suggest is that maybe we take a couple of those that you just mentioned; right? I think they fit somewhere into the producer or user or regulator would be my argument.

But I think, yes, let's build out a few more categories, and let's do a use case around retailer cares about this thing or that thing. Regulator cares about this thing or that thing. Manufacturer cares about this thing or that thing, because manufacturers and retailers aren't always going to agree. So, let's pick a use case. We can pick out some of those additional categories that you've mentioned. And let's try and turn it into something that is, you know, real; right, a more real example. So, I'm not disagreeing with you, but I also don't know how to get to that next level of granularity if we don't start proving out what we have.

It might also be a timeline thing. As I look at this, a lot of these seem to be devices that already exist or are in the pipeline rather than devices that are farther out. So, if, you know, you've got a company up in Boston that's making potential healthcare equipment and you can't find venture potential capital, that product will just never make it to market. But that's a very future-looking thing. But it will shape the market of the future. So, that could be that different of these have different levels of influence at different stage, and so that might be a way to kind of shape this so you make, like, the superset rather than the subset for today's devices.

I like that as well. And, at various times, we have discussed that exact fact, that there is a timeline here. It's very easy to look at this, and this, the way that I've presented it, is very much a snapshot, because that's really as far as we have gotten. It's like, can we even take a snapshot. I think you're a hundred percent correct that there are temporal elements, because things don't all happen at once.

Again, the question is, what does that timeline look like in any particular use case; right? What are the influencing factors at any one particular moment, and which ones should this group worry about versus what other groups should worry about; right? One of the things we were very conscientious of was trying to stay away from overthinking the policy side of this; right, and the legal side of this, because you can go down that rabbit hole and never come back. We tried very hard to stay away from that and try and stay focused on are there discrete elements that we can identify that won't get people's hackles up but that will still provide some meaningful value. So, I'm a hundred percent on board with you, Bo, I really am. But I don't know how to get to that next step if we don't get some other people involved, whether it's yourself or others, with that viewpoint to help flesh it out.

You want to come forward and find a mic. Remind folks who you are.

Seth Carmody, U.S. Food and Drug Administration, so I am familiar with the pacemaker example. So, a question: Where was the consideration of liability and players that enforce, say, monetary penalties for lack of security? I can see a regulator slant on it. Any discussion around that?

Yeah. I mean, so we sort of generically. And it's shorthand; right? We weren't ignorant of the nuance, but we used the shorthand around enforcement, regulator enforcement, as being sort of a catch all for things

like that. It could be the FDA, the FTC, whatever. But we sort of threw that all into that bucket. Just as with Bo's comments, you're right, there are levels of granularity and nuance there that are important; right? You can't just gloss over them, because it matters. It influences the outcome.

But, again, to my mind, it's let start with something simpler. Okay, we've tried this out a few times, it seems like it's working, now let's make it more complicated; right? Let's bring in specific regulators. Let's bring in other types of potential influencers here, figure out where do they fit. And if they don't fit, and if we decide that they really are impactful and need to fit, that's an opportunity to update the taxonomy or update the way that we're approaching it, but it's a phased approach, I think.

Thank you. I thought that may be the case. And then, just a clarification around what you mean by "regulator voluntary?"

Yeah. Sorry. So, again, we cheated; right? And I probably just need to go change that, because it gets confusing. Regulator voluntary, what we did, in order to simplify our approach, was we took any organization that would, with some level of authority, whether it could be standards organization creating interoperability standards, whatever it may be, we lumped that all under one thing; right? The reality is -- and that's probably an area that most immediately could use some adjustment -- is we probably do need four things in here; right? So, I think regulators are a distinct category -- excuse me -- stakeholder in the traditional sense. When most people think of regulator, they're thinking of enforcement; right? And then maybe a fourth one, which has more to do with standards, and we've talked a lot about standards bodies today that are engaged in this; IETF, Oasis, and others.

So, we've gotten that feedback before. We haven't done it because, frankly, it's been convenient shorthand for our group to just lump them together, because we see the outcome being somewhat similar in terms of the decision-making process. Think about it this way, so, if I'm building a device, I care what the FDA might say, because you're regulating my medical device, but I also care about interoperability standards related to my device.

So, from my perspective, as a manufacturer, I've got two things that I have to build to; right, because if I build the one but not the other, or vice versus, then my device won't work or I'll get in trouble. So that's why we grouped them together, because from our perspective, it was the manufacturer has to meet certain things in order get the device out the door and have it meet its intended purpose and not get in trouble for it. But it was convenient for us. I think it's less convenient as we roll this will out, just from a terminology perspective. So, I hear you loud and clear.

Rudy Brioche with Comcast. Just to follow up on the questions, I guess one of the ideas presented earlier, which I don't think you followed up on, on the role of retailers, considering, play such a critical role as far as interacting on both sides, particularly with consumers you know, and in discussion with, you know, incentives and barriers, seems to play a pretty important role. Was that purposely not included, or is it, you know, too big of a nut to crack?

We didn't have the right input to be able to define that; right? I mean there's some obvious examples that you can go to, but it gets murky pretty fast. So, Amazon, are they the retailer or the manufacturer; right? Are they the hardware producer, the software producer, the service producer? Yes. They're all of those things. So, how do you treat the Amazons of the world? Where do they fit into the decision-making process, because they're basically making all of the decisions; right, because they control the entire supply chain for themselves, more or less. Other companies not so much; right? Other companies are relying on other manufacturers. It could be overseas, and then they're building the software and they're packaging it and marketing it.

So, when you open up that door, it gets really complicated really quickly, because it's hard to lump everybody into sort of neat categories at that level of granularity, which is why, again, I think if we start at this sort of higher level and just say, yep, we all admit and agree this is an oversimplification, but let's start and see what happens as we try to apply it? And we'll either determine it's way too simple to be useful, or it is useful in this current form, in certain circumstances, but we need to build it out, and maybe it

becomes the retailer's take this and build out their own model. Maybe it becomes the manufacturers take, something like this, and build out their own model. I don't know; right. It could go a lot of different ways.

The point, ultimately, that we wanted to drive home was we need more system systematic ways of thinking about these problems, because it's not enough. None of us want to get in a situation where something really bad happens and suddenly we're legislating and regulating without any real context of what the costs may be and what we might be really asking for. So, again, let's put a model together to help us make some intelligent decisions moving forward so that we don't make bad decisions, if that's possible.

Further thoughts? Susan, is there anyone on the line?

Thank you. Once again if you'd like to ask a question, you may press "*1." Christopher Gates, you may go ahead.

Love your approach. This is some of the stuff we kind of kicked around not nearly as good a format as what you're proposing here for doing this. But we've kicked this around in the technical capabilities working group, so I really love what you're doing and going forward with it, so I think that's a great opportunity and would love to interact moving forward with this.

One thing I would point out that's kind of been already beat together while I was waiting here, which is the liability side of it. I mean, we're going to see that. We've already seen bills by Senator Warner introduced. We know what's coming, where suddenly the board is going to be responsible.

So, let's say you take your connected dishwasher, in your example, and you've got liability. If that reaches out and takes down [inaudible], so it can't make money, you're liable for that. And while it's not right there today, it will be tomorrow, and so I think that's something that really has to be put into these metrics. This really helps to be able to go in, because no manufacturer, medical device or otherwise, wants to put money into something that isn't needed. So, if you can walk in with these kinds of metrics to back up your position, say, you need to do this and here is why. Here's where your risk level is. If they're comfortable with that risk, great. If they're not, then they can put money down on it. So, really do appreciate the work and think it's a great first start.

Yeah, thanks, Chris. Look, you know, we all agree that liability is an issue here, and we think about, you know, what is congress going to do or not going to do. I used to work for the Department of Commerce, so I will channel my inner commerce on Allen and Evelyn's behalf and say that I'm quite positive the NTA does not want to take the position on what is or is not good legislation. And, so, we tried very hard to steer clear of something that might get us down that rabbit hole as part of this effort, which is not to say that it is not a critically important question. It absolutely is.

Our feeling was, this is not the forum to have that conversation. It needs to happen in other forms. This work and the other work of the working groups can be informative to those conversations. We did not want to take any sort of position on something that might touch on legislation too closely, for a variety of reasons. But I appreciate your point, Chris, and thank you for the compliment. I do appreciate that.

Susan, is there anyone else on the line?

Our next question comes from Kent Landfield. You may go ahead.

Yeah, I just wanted to say that I like the idea of trying to work the combination of a couple working groups to sort of accentuate and expand on what you've done. I think what you've done is, potentially, extremely useful. But we need to dig into a couple more use case, a couple more examples that might be much more directly tied to what we're producing in other areas.

Yeah, thanks, Kent. Agreed. You know, I teed that up earlier. I think we're going to talk about it this afternoon, about more ideas on how the working groups can start bringing their work together in meaningful ways.

Further thoughts in the room? So, John, I know that, as with all model discussions, we'll just use your model and say, oh, but we could add this to it. You sort of said, no, we want to validate it. If we have another meeting, a virtual meeting, in a month-and-a-half, two months, what do you need to have and what does your group need to have? Because this document is fantastic.

Yeah.

But it's pretty similar to the last one we saw in July.

Yeah. Nom not really though. The reality is -- thanks for bringing up that we didn't get anything done over the summer, Allen.

You're welcome.

I appreciate that.

Decide to work on it.

I was trying to weave around that. No, look, the reality is we started out and we've had a very -- it's been a relatively small group, a lot of really good engagement, but it's been relatively limited to people who do not come from manufacturers of devices. We haven't had people who are writing software for these kinds of devices, and so it presents a challenge when you have, you know, people like me and people from trade associations and others who have a lot of really smart ideas but sort of just a perspective; right?

And, so, what we need more than anything is, we need folks that are involved in manufacturing, you know, anything, really, under the producer group and expanded producer group to participate and help us understand what are the costs associated, what are your real incentives and barriers, and don't just say, "Well, make it cheaper for us and give us tax incentives," or, "Don't regulate us," right? I mean, everybody knows all of those. That's sort of the obvious answers. We need the less obvious answers to help us manage what is the risk associated with doing this or not.

So, if you work for a manufacturer of any kind, again, whether it's software, hardware, or if you're providing a service where you're specifically touching on the interaction between devices and you've got some insight into that, that would be really, really helpful for us to make this more concrete. So, that, ultimately, I think, is what we need to make progress with the team we have today. I can tell you, I think we've carried this as far as we can carry it. We need new voices into this.

Now, my hope is, by integrating some the work with the other working groups, that's going to get us some new input; right? That's going to bring some new voices into the mix. I think that will help. But, again, if you work for one of these companies that are developing devices, we would love to have you participate in whatever way you can. I think that's the voice that we need to hear.

John, can you pull back the slide with the use cases, the couple of use cases that you were talking about use cases. Perhaps there's some folks in this room that may have some other suggestions for use cases that you may have on the line.

Oh, yes. I'm sorry. It's back up here. Yeah, so, I mean, the one that's in the document, it does relate to the dishwasher. I don't remember why we picked a dishwasher. You know, we knew we were supposed to deal with consumer devices. It seemed a relatively harmless one to choose, and we knew that there was business harm, potential physical harm and so on. But we also talked about sort of supermarkets doing inventory checking, things like that, trash can that tells you when it's full or not full, you know, simple sort of consumer things.

Any other use case that fits into that consumer market -- you know, we're trying to stay away from medical devices. I cited that example earlier because it's sort of interesting. But we're trying to focus more on the consumer ones. I think thermostats are really interesting. They've been around for a while. They've got a pretty good deployment model. We've talked to folks at Amazon to see if they'd be interested in coming and talking to us about issues around Alexa. Hopefully there's not one in the room that I have to say Alexa, never mind. Does anybody else have one and have to do that all the time? No? Okay.

Not since the discussions about Alexa.

I've got a lot of connected stuff in my home. You've got to learn it if you want to deal with it. No, but my point being that, you know, any of those case uses are interesting. Anything where consumers are engaged now and where we think that they're going to be particularly engaged moving forward, I think those are the most interesting places to have conversations, not industrial controls, not medical devices, fascinating topics, but not for this forum.

Does anyone have some thoughts about use case might be able to help out?

Yeah, so interesting use case might be in cars. Ford, I think in 2016, committed to go all over-the-air update for their systems in some timeframe. I forget all the details of it now, but that was -- it's my understanding that was, in large part, driven by some of the bad press and reputation that comes out of recalls. So, if they can avoid a recall and do a software update instead, that makes it a lot more palatable. And that's something that would have been driven by shareholders, investors worried about brand and brand reputation.

But a competing tension there is at the dealer level, so, now you're cutting dealers out of some slice of the pie. So, some of the conversations I've heard had -- this is not in the Ford case, but if you're going to do an over-the-air update, does that mean you have to pay dealers some royalty or license or -- that's the wrong terminology. But how do you make sure that dealers aren't losing their shirt when you're going for this over-the-air update? So, those are two competing tensions that I can definitely can see as a use case that can maybe help flesh out some of the retailer case and some of the investor case.

You know, I like that. I think cars are an interesting one. We saw recently the Tesla, you know, pushed out that update so that the cars could drive further. I don't own a Tesla, but if I was a user, I would be like, well, why can't I just have this all the time; right? So that creates some interesting tensions there as well. So, you know, you've got manufacturers pushing these over-the-air up updates, but what are the outcomes of that? I like your example. I think there are others. So, I think that's a useful one.

I would love to have somebody who deals with car manufacturing, who actually manufacturers cars actually participate in that, because, otherwise, I'm sort of stuck just piecing together what I can from news articles. But without really getting down to the brass tacks of what's reality here, I don't want to guess. You know, if we can avoid guessing what Ford is thinking or, you know, what Toyota is thinking, I think that's far more useful than if we are just guessing, so, anyway. But thanks, Bill, I appreciate that. It's a great point. It brings some of the nuance that you were talking about into the mix as useful.

Yeah, this is Daryl. I noticed some of the factors in there, and I like the idea that you mentioned scale. Not that it would make a good use case, because I don't know if the information is available, but I did talk to a company, a business now. Obviously, they weren't consumers. But the products they were using were not industrial. They were, I guess, enterprise-type technology in a large organization. And, typically, with firmware updates on embedded devices, they don't patch, they update. Most firmware comes down as one big block. The entire thing comes down. And they literally had tens of thousands of these throughout their organizations that woke up and update at the same time and DOS the entire network.

Right.

You know, so I kind of like the idea that you mentioned scale in there. That was kind of interesting. Often that's not considered in these types of scenarios.

Yeah, that's a good point. I think that's a great example. If you think of a lot of other examples [inaudible] somebody else has thought of, just other kinds of constrained environments, where patching or updating may not mean much.

Sorry. Thanks. So, yeah. No, I agree. I mean, these are all nuances or granularity, or whatever you want to call it, that I think need to be part of the mix, so I appreciate that.

We have Joe on the phone.

Thank you, sir. Joe Jarsenbeck, you may go ahead.

Okay, so can you hear me now?

We can.

Good. Okay, because I was trying to comment. So, John, again, you've heard from others, but what you've provided is excellent in terms of a framework and use cases that would enable discussions both within companies, but within a broader stakeholder community, so I really commend the work that you're doing.

I just wanted to make sure that you addressed the all-hazard analysis, because a lot of times, when people are having those discussions, it's for a much more narrow set, because you have to ask, you know, if the device is hacked because it wasn't patched or it wasn't updated, then what are the risks outside, not just to the user, but could be if it's hacked, then it can reach out and be part of a more global distributed denial service attack. What does that mean? So, it needs to be properly framed in terms of all hazards that would help people have those discussions, which now comes back to what is it that people need to address when they're doing it, and the value of having standards in place, which was from the previous group discussion.

And most of the time -- and you guys already realize that -- government does not seek to regulate until industry is viewed to be non-self-regulating and lets bad things happen. And, so, if you have standards in place that follow that says, "But we're doing this," so as a minimum, we're doing this. So, we're doing our own proactive. We're doing our own due care. Because if you simply rely on the users to say the objections are there, most users are totally uninformed about it. So, to ask the question, well, why should regulators care if users don't care, users don't know, and so there are some who are acting on citizen's behalf why these things need to be done, so just keep that in mind. just because users don't care or don't seem to express that doesn't mean there's not an issue. But again, great work that you've done. You've provided that framework for the discussions for internal risk investigation activities.

Great. Thank you. And I think, in terms of moving forward, captured that we're trying to build out some use case. Some folks have some use cases that I think John can work with. It sounds like, to move forward, John needs a few more fresh ideas from the people who haven't been participating so far, so please reach out to John. And I'm happy, if you don't have his contact information, I'll include that with an ask.

Anyone else have further thoughts about what they would like to see this group as they take the work they've done to sort of finish and it get it over the finish line.

And, again, if they would like to make a comment over the phone, they can press "*1."

All right. So, we now have the point in the agenda we want to talk a little bit about seeing which of these documents are ready. I think the incentive document has sort of a couple use cases they want to have done. The capabilities document still needs just a little more polish. And I think we got the sense from both of those that if we can get a few fresh ideas and one or two more rolled up sleeves, we can actually get those across the finish line in the next month or two.

From the standards document, that's an interesting dynamic, because I think when we think of NTIA stakeholder documents, traditionally they're sort of finished. Whereas one of the things that the standards group made clear is they don't want to finish, they want to make sure it's a living document. And so, one of the things that we'll have figure out is what does that process look like. We can start with Daryl, or with Kent, if he's still on the line. Do you have some thoughts about, you know, from your working group's perspective? We've got input of the past few months. You know, we tried to sound the gong and make sure that everyone knew about it to contribute. How do you feel about it, in terms of saying this document, when we can find a home for it, is ready to move on to its new home?

So, when will this be ready to move on to a new home? Like I said, it's still moving forward right now. I think we need to start looking for that place right now. That doesn't mean we do not want people giving us feedback and information to improve the document, you know, and the way it's structured. So, we're still open to that.

At this point, I think, from my opinion, it's at that the point getting ready to move forward. I'll continue inputting data to it. If it's supplied to me, I'll continue updating it. But, sometime this year we, in my opinion, we need to find a home for it. We need to figure out what that home looks like. We need to find a home that says, you know, we're going to continue maintaining it. Some of the other things that were actually mentioned in there, organizations, that, obviously, credibility, that we know they're going to continue on with it, international reaching stakeholders continue to be involved in that, and resources are continually available. So, everywhere it goes it needs to meet those general requirements, in my opinion. And at this point, we're ready to move to that level.

But, again, take a look at what where he produced out there. If you have any good solid feedback, I would like to get those adjustments in place before we take to that next level, and find a home for it. And we're also looking for content. So, in the handout that was given out there, there is the catalog entry descriptions. If anything is not in this document right now that you think needs to be in there, in reference to IOT security, make that catalog entry description available to anyone who wants to supply us with stuff. Have them fill that out, and I will continue maintaining and getting that information into that document until we find a home, and hopefully we need to do that this year.

Great. Kent, I know you're on the line and have some thoughts on this.

Thank you, Kent. Your line is open, sir.

Thank you. I'd like to see this become a web-based facility, mainly because it will make it a lot easier and much more automatic. I mean, granted, you're going to have someone active, a mini moderator to sort of check the data being submitted. But nine times out of ten, you're not going to have to worry too much about it after you've done that.

That's a lot easier to maintain going forward and a very like lift, as opposed to what we have been doing, is, you know, searching for these documents ourselves. A lot of these document creators, standards organizations, and consortia, even academia, could benefit from having the ability to make this information available themselves from the crowd-sourcing kind of perspective. I think that would be a good approach to take, because it reduces the load on individuals or organizations and provides a means for updates to available very quickly. We're still nowhere close to that. We need to talk through that proposal.

But, honestly, I agree with what Daryl said earlier, we're in a situation where this has to be manually maintained and manually done by the working group, as we have to this point. It's going to be problematic, and it will degradate, and we don't want that to happen.

So, do you think it is possible, in the next two months, to work as a community of the working group, and we'll make sure that new people that are involved to say what might be an endearing home, or what it would look like to have it stay at NTIA for, you know, the next end months?

That's definitely a topic we can take on and focus on, which, to this point, we've just had a cursory discussion. We haven't had any real focused discussions on trying to come to that solution. But, you know, like you say, it's about time.

Excellent. And we'll make sure that, when we summarize this meeting, that's something that we flag for folks who weren't able to watch today.

Sounds good.

Any other thoughts on sort of taking the standards document and either transplanting it or making it somewhat, on autopilot, a sustainable model, what this document would be useful for?

Allen, just a couple thoughts. So, I like the Wikipedia model. I think that's what Kent was saying in some way. I don't know how you curate that, but I think it's a good idea. I also want to interject that just became aware, I think within the last two weeks, of a similar effort to catalog IOT cybersecurity standards. I think it's the IIC -- I'm not very familiar with the IICS working group. I think it's at NIST NCCOE.

It is. This is Megan over in the front.

Oh, there.

We've actual contributed the catalog from this working group to that document.

Fantastic.

And I can fill you in more that working group afterwards, if you'd like to chat more about it.

So, from where I sit, I get hypersensitive about duplication of effort, so I'm glad that you guys are, you know, at least talking to each other.

Thank you. Yes.

Just a quick comment. I don't think that the standards document needs to be hosted by a standards organization, because it's not going to be a standard, it's a reference report of some kind, or a catalog.

That's a really good point. Thank you. More organizations deal with standards then actually produce them as formal HDL. Further thoughts on this? So, it sounds like we have three groups that are just about there but need about a couple months more to do some polishing and get a little more data integrated, and, so, you know, for our next meeting, which will probably try to alternate virtual meetings so that people don't have to worry about getting to Washington, we'll be ready then. Further thoughts on that? Do we all seem to think that that makes sense? Anyone feel like they need more time or will be ready next week?

Because now we can pivot to two questions that have come up. One is, how do we take the work that's happened thus far and is going to finish and take it out to the world? And we want to make sure that we check in with the folks from the communications working group, which has a published document already. And the second has come up from a number of folks already, which is how do we take these documents and make sure that they talk to each other? What does that look like? Should we work on a tighter

integration? Should we work on having an overarching chapter or frame or separate document that explains how they integrate?

And before we get into that, we can talk about the sort of the progress and the awareness of the adoption of the work that's happened already from the communication working group. So, Harley and Beau.

Thanks, Allen. So, since we got consensus on our working group document, the working group has met on the phone, and we identified a number of different areas like different fora that we can bring our document to in order to brief them about the work that we've done, and its implications. I'm just going to run through the five general areas really quickly. But one is IOT trade groups, we've identified several of those, maybe five of them. Two, we talked about doing something with CES and CTA, so possibly doing a CES panel in January, as well as presenting before a CTA member meeting; three, a list of IOT conferences. Daryl provided three good ones. Four, IOT manufacturers and points of contact at individual companies; five, ISOC, the Internet Society and OTA, so getting our working group document in ISOC's planning for the coming year, and the availability on that. It will be in the campaign for next year, as well as referencing the document in the Online Trust Alliance in the IOT framework.

And then we've also talked with NTIA about putting the working group document out on the web as a PDF or an HTML, and also it integrating it into a blog post or release on behalf of the group, because from the perspective from at least a couple of the co-chairs, there was some reluctance to host that themselves. So, a question for Allen and Evelyn, but where do we stand on the possibility of having an NTIA blog post that talks about the working groups document?

And so, I think we wanted to see how today went. But I this we are ready. We can talk about that very easily.

Okay. So, I think we can have a blog post, and happy to coordinate with both the working group, as well as anyone else here who wants to talk about the communications document and what it means to them. I think having stakeholder voices in that type of blog post always is helpful.

And I will say, also, so, the five areas, I guess six, if you count NTIA, that I flagged just now for follow up, we had previously sort of de-emphasized meeting with government agencies, like with regulators or, you know, voluntary regulators, and part of the reason was because of the strong feelings within the group that the working group document was not supposed to be a template for legislation or regulation, and therefore, are meeting with regulators to talk about the group before meeting with companies was perhaps backwards.

But I wonder -- and I haven't talked with the working group about this, but I've sort of come around lately to thinking maybe that is not the right approach, and, in particular, because of the Gardner, Warner, Wyden legislation on IOT that does include stuff on IOT labeling; that perhaps we should sort of reemphasize meeting with the Hill and agencies and say, hey, this approach is out there. There's, you know, a fair amount of support for it, and so, you know, let's see if we can promote this in a nonregulatory manner, you know, before including it in legislation. So, I guess that would be the seventh area.

And I can go into more detail about, like, which trade groups and so forth that we've identify that we're going to try to target, if you'd like, but that's the overview. Bo, do you want to add anything?

No, I think you had a really good summary. One thought to came to mind as you were speaking. We had some early conversations with some retailers and retail associations, and we probably want to pick those back up, because as we've said here a couple of times, they I can be a powerful ally in kind of getting this out there.

Ultimately, one of the things that we've learned from our research is that one of the big concerns of retailers is they always get asked questions about devices, you know, on the sales floor, and if their sales folks don't have a way to answer those, then it leads to customer frustration, et cetera, et cetera. And it can also drive up returns, which they don't like. So, it would probably be worth working, and with some of

those folks to just see what something like this might look like in an implementation phase at a retailer, whether it's back into education, whether it's, you know, a sales display, whether it's, you know, asking manufacturer's what their update ability is before they agree -- you know, before the retailer agrees to carry. That could have a big impact on adoption across the industry too.

Thank you. Sorry. Forgive me. I was trying to figure out on the surface the settings. The other thing that we have done, and you can't quite see it, is we have set up the website, ntia.doc.gov/iotsecurity, as a way of making sure that the documents we're seeing -- the completed documents we're seeing at a particular place where we could all understand them rather than having to wade through the multi-stakeholder processes.

It's really important for seeing the history, making sure that we preserve transparency and openness. But this allows you to see what is there. And so, we can talk a little later, if you want about what else you would like to see on this webpage and what someone who comes across this should know. How do we make sure that it's clean and light but still conveys all the information they need to? And I will see if I can make the font bigger. This is currently the text on the page.

You know, one thing that occurred to me in looking at our own document was that, you know, in handing out hard copies or, you know, PDFs that's circulated via e-mail or something, I wonder if it would be helpful if we could include a link to our own document in the document; right? So, if somebody has a hard copy of it, they'd know where to find it online pretty easily. And this webpage seems great for that, provided you think that it's going to stick around; right; that is, that the URL is not going to change.

That is one of the reasons we traditionally in NTIAs, not to mention system does URLs, has a year and a timestamp and subfolders; that was, our IT team was actually quite flexible in working with us to make sure that this URL was going to stay. And we certainly hope to make sure that this is part of our mission and not the sort of thing that would be taken down. Further thoughts on Beau's use on outreach? And can you very quickly run through those points?

IOT trade groups, IOT conferences, IOT manufacturers, agencies and regulators, NCIA-specific workflow, and then some specific work with CES, CTI, and the Internet Society, and the Online Trust Alliance.

Any other thoughts for what we can do, for the moment, focusing on consumer communication? Yes?

Hi, this is Vanna Schaefer [ph] from TIA. Out of curiosity, have you talked to any academic institutions or the academic community?

I knew we were missing somebody, but, no. No, we haven't yet. In fact, we've spoken to relatively few people on that list. You know, most of what we did was divide up which parts of the list we were going to gather, and that has been done mostly. So, you know we have the list of people to talk to, but we haven't done a ton of outreach to the folks on the list, so that's a good point. And if you have particular ideas, we'd love to hear it.

Definitely. I'll follow up later, but, yeah.

I think in the first stakeholder meeting, we did have somebody from the University of Washington out there who was looking to do something on updateability. I don't know if he ever participated again.

So, Yoshi, together with Jeanie Camp at Indiana, have a very large NSF branch looking at IOT security and privacy from a consumer perspective, so I think they would be a great target to reach out to. I'm happy to connect you with that team. Elaine.

This isn't a fully formed thought, but given that there is a labeling discussion here, and in the EU, I'm wondering if there's anything we can do to make sure we're all talking to each other, or at least aware of one another.

Do you happen to have a recommendation on who at the EU to reach out to on this?

I can get one to you.

That would be wonderful.

Thanks.

Great.

Certainly, I think there are a number of both government and private sector groups that are spending some time paying attention to Russell's politics on this front. I think it would be good to make sure they know about this venture.

On the consumer advocacy side, have the working group done some engagement on that front?

So, in the interest of keeping it relatively -- keeping our list manageable, and recognizing that this is not the full-time job of any of the folks on the working group, I did put future privacy forum in the IOT trade group bucket. They're not a trade group. They focus not just on IOT, but I thought this would be up their alley and they would perhaps help carry the water on the consumer advocacy side. So, I did try to make sure that was represented but didn't want to come up with a separate, you know, six-group list of consumer advocates too.

Harley, are you looking for more people to help you on the outreach side of things?

I mean, more help would always be welcome. It's sort of unclear, at this point, how much more help we would need, as opposed to what we would welcome. You know, each of these components that I had listed was -- you know, we had somebody in the group who helped volunteered to help put together that list, you know, and I think the actual outreach -- you know, the e-mail that we send to the list or, you know, to those entities to try to establish contact is not going to be that heavy of a lift. I think that we would just have to take a couple days and do it. I don't know, maybe I'm underestimating the amount of work it's going to take, but I think it's probably okay. That being said, if anyone wants to join, anyone wants to help out, you know, please feel free.

Yeah. And we always accept tweets and retweets of our work. That's always a good way to get it out there, Facebook. You know, I think general awareness is a good thing, and that doesn't necessarily have to be centralized and have us as a bottleneck. I mean, I can just imagine somebody so passionate about what we've gone that they take it upon themselves to make sure that they go door to door knocking and, hey, have you heard about this updateability and patchability.

I will also say, though, for places where -- folks who are here at the table or on the phone that don't have particular contacts -- like I don't have very many contacts in the EU, for example, or limited inside into the academic community. But if you have a particular relationship with them, that would be especially helpful. Otherwise, I'm cold calling.

And so, for the next meeting, is there something that we can help you with or that we should look to you to come back with for us?

Well, for NTIA, I'd like to see about getting, you know, some sort of a blog post or announcement on the work. You know, I realize that nobody in our working group, you know, non-NTIA, nobody else in the working group has put out like a formal announcement, so it kind of came out with a bit of a whisper; right? So, I'd like to do that. But, in terms of specific follow up items that you guys can help with, I think that's the big one. And then, you know, any ideas for academics that you think would be particularly helpful for points of contact, but the rest of it, I think we're doing okay. I'd like to talk to this guy.

Sure.

Yeah. Since you're interested in it, and your agency is actually on the list, so.

Excellent. Further comments? Anyone on the phone who has a question or a thought about outreach for communications working group?

And if you do, please press "*1."

One thing that, at the next meeting we may ask about is, as the other working groups finish up and begin to think about the awareness of adoption component, is hearing your lessons learned, as well as any doors that you've already opened is going to be very helpful. So, I would encourage you in the working group to keep track of the outreach that you've done so that it can be further amplified.

That's good advice. Sure.

So, on the schedule, we're due to break in 20 minutes for lunch, but I think it might be useful -- sorry. Do we have a name? Ah, so forgive me. Can we open up Michael Eisenberg's -- I don't see him on the call list.

I don't see a Michael on the line either.

So, forgive me. Let me check. Michael, we may catch you after lunch. But let me check, if you sent me a note. And Michael suggests a couple of organizations, such as the NANOG IOT working group, and we're engaged with NANOG, RSA, and I've talked to a number of you about that, and the ABA IOT National Institute in D.C. Ah, I'm sorry, that is not NANOG. That is the NAAG, which is the National Association of Attorneys General. And Michael, I believe, mentioned that at our last in-person meeting. So, Michael, there is, if you're watching on the NTI website, there's a dial-in number, and --

I can give you the number over the phone if you' like.

Can you say the number out loud, operator?

Absolutely. It's 1 (888) 205-4638.

Thank you. And our operator is literally standing by, so we hope you can join.

Call now.

Always embarrassing when you're upstaged by the voice in the sky. So, I think what we can do is to start the conversation of what integrating the work looks like, because I've heard from a number of you the importance of saying, hey, this work, nicely dovetails. We have technical components. We have standards components. We have user components. We have incentives. All of those seem to hit very important and complementary approaches, so what might integrating those documents look like? And, John, you raised this issue first today, I think, so do you --

No, I'm happy to chime in. It's just my thoughts. There's probably better ways to go about it. I think that, you know, notionally, like you said, I think each of the documents has some core pieces. If you think about it -- so obviously I think about it from our working group's perspective, where we have sort of this broader framework, there's less detail there. So, my sense is that, at least for the work that we've done, digging deeper and working with each of the other three working groups, and I think it's all three of them, because we have user stakeholders; right, which, you know, the working group on user communications has talked about. We have this idea of what influences or gets in the way of the producers; right, which are more of the technical elements that that working group has worked on.

We've got a sense of, you know, what do standards say around what do people have to do to even achieve those things. So, you know, I think, from our perspective, I'd like to see our group work with the

right people in the other groups -- and I'm happy to take that on -- sit down, and let's actually parse that through a little bit; right? So, I know that's sort of a soft step, but I think we need to actually spend that initial step of saying, okay, you've heard about my work, I've heard about your work, now let's actually sit down and spend some time together and think about, virtually or otherwise, how does that inform this? How does that make the work that we've done better, or vice versa? Or how could you see the work around incentives and barriers sort of either dovetailing or sitting on top of and providing some additional structure around the work that you've done in your group?

So, I don't have a lot of clear answers on exactly what that would look like at the level of detail, because I haven't done the analysis, but I think it's that analysis is the first piece we need to do to get from, you know, that makes sense and sounds like a good idea to, yeah, here's actually what that would look like and what we would try to achieve if we did it.

Further thoughts about what this might look like, because I think sitting down and having that discussion can be useful. But a lot of us are here, we can start that now, or perhaps after lunch. Any further ideas?

All right, I'll come back in, since you're keeping the demand full, I'm here. So, I think, at a minimum, what I would like to do is, you know, I already mentioned earlier about looking across the current body of standards work; right? So, I think that's an important first step. You know, we talked about, potentially, different levels of granularity on how deep we might go. I would like to do some analysis across what are the standards that have been identified, the guidelines, whatever, what are some common elements, who says what and where, and then take that and use that as an input into our taxonomy, and say, okay, here is sort of the overarching view on yes, it's good, no it's not good. Here's where we think about it. Here's where we don't think about it, and put that into the model that we've come up with, see where it fits. And if it doesn't fit, create a spot for it, and then use that as an input to, all right now let's pick a use case.

We'll use our dishwasher or something else. Maybe the car is a good one. I kind of like the potential there. And let's use that as a use case. So, let's very specifically say what are things that standards say around how you should implement this in an automobile, if anything? If they don't, we pick the next closest thing and we take that as an input. I think, from there, we can build on top of that and take the input from what's the consumer outreach look like? Are users saying that they care about this or not care about this? Why should users care about this or not care about this? That becomes an input into, again, the working group four model around -- because that's a stakeholder, let's use that information and what we're communicating to users to determine how might that influence them on that scale, strongly agree, strongly disagree with this, that, or the other thing in a particular use case?

And, then, finally, I think it's working group three. I always forget the name of it. But the one that we saw right before mine, which has the detailed sort of capabilities. That is a place that I think helps bring together that idea if we can get some additional producers, manufacturers engaged to say, oh, I see these 12 things that you've done. That's really hard, that's really easy, love it, love it, hate it, hate it, hate; right, that becomes a discussion starter that then feeds into our model to say that, in this given context, this manufacturer looks across these 12 or 13 item and say's here's how much it's going to cost me to do it and here's why I would choose to do it or not do it. So, now all of a sudden, I've got inputs from all three of my stakeholder communities that we've identified in our group, minus the regulators. So, I know we've got FDA here. I think FTC has been involved in this effort in the past two. Would love to get them in the mix, too, to think about how are they viewing this.

So, that's sort of my notional view, because I've thought about how I would work with each individual group to provide input into our model. But I would love to hear from the other groups on whether or not they think that's a worthwhile exercise and how they might see the value that they've produced sort of injecting into that process, or vice versa.

Fantastic. Thank you. Further thoughts on -- and we have the sort of incentives and barriers working group that said, hey, these can all inform the work they're doing? Other thoughts about how they can be a little more integrated if, indeed, they should be?

What if it was really simple, and you just had like an introduction that tried to synthesize the work of the groups into sort of a more coherent statement that, you know, encompassed the themes and findings of each the working group, as like an introduction, and then you just had the working group documents unchanged after that? That would be pretty easy; right? And I will tell you that, like, considering the agonizing that went on for our working group, it would be very difficult, I think to --

We're not going to open yours again.

Well, you're not going to open ours again, but, like, writing about it and then trying to get the consensus on that will produce more agony, I think; right? And, so, in the interest perhaps of keeping it simple, I think that should be a possibility at least; right? I mean the working group documents, so far, have been worked upon as sort of self-contained units, and I think that they do work as standalone documents. But if you had an introduction that synthesizes them, then you can have them all kind of sort of a compendium. It would also make it very handy, you know, for the website; right? You could have the introduction as HTML, or as a separate PDF, and then just have the working group documents underneath it.

Yeah, so I don't disagree with that. I mean, I think writing an introduction and to try to synthesize, I think, makes sense. I think that's the first. It's almost -- it's not quite a vision statement, but it's like, hey, here's why we did this. We knew why we started to do this. But now, you know, a year later, or whatever it's been, here's what we think we've learned; right, and put that together all into one statement. I think that's smart. I think, too, that if I'm being honest with myself, I'm probably projecting a little bit around the fact that, you know, what -- our working group has been a little bit more amorphous in terms of the output, and so I'm trying to figure out is there a way to take what I view as more structured output that the other workgroups have created and somehow use that or leverage that to bring more structure to what we have done? And that may not be the way that we need to do that. I think the use cases are one way to do it.

But I wasn't, in any way, suggesting that we change the document. So, I wasn't necessarily saying we merge it into one gigantic sort of, you know, manifesto about IOT patching. I don't think that's doable. But, again, thinking creatively around how do these things inform each other and maybe starting with that introduction, and just building that may give us some insight into how we might be able to take it a step further.

I think it certainly would help your working group's output to get insight from manufacturer, trade associations, and so forth; right, on how they would implement or not implement and why. I think that would be challenging; right? And I'm not sure that the folks who are members of the multi-stakeholder process are, you know, even going to be able to get those answers. Like, you're probably going to have to get them straight from the source to be accurate; right, get them from the trade association or get them from the manufacturer, and then you have to hope that they're giving you their honest answer and, you know, not something they know is going to be replicated in a public document. And, so, I think it would be a worthwhile document if it is successful, but I think it would be challenging.

Yeah, no question. I agree. And so, it raises the question of whether or not the timing is right. Those conversations are going to be had; right? Whether they're had in front of congress or they're had before that, those conversations are going to be had. So, my view is, if there's a way for us to, off of this work, start figuring out how do we have some of those conversations to get some honest answers now, it may be in our best interest in the long run; right?

But, I mean, we've all been down this road before in other areas, and it may just not be possible to get the kind of answers that we need in order to say something truly concrete around what is the risk and how do we deal with it. I don't have the right answer to that, other than I think the more proactive we can be now and help control the conversation earlier than later, it seems like it's better for all of us if we can find a way to do that.

So, like the call to say we need to actually demonstrate some power and some potential of this approach. Certainly, it's very near and dear to NTIA's hearts when we're looking for the concrete way of how we as a

group can do that. We have the introductory chapter, which I think came up at the last in-person meeting, and we may talk -- pass the hat to see who wants to help engage on that front and help lead it.

I don't mind. Harley, will you help?

For you, John.

Thank you. All right. So, I'll sign up for that; right, because I'm making an issue out of this, because I think it's the right thing to do. I think we have agreement that we want to do something. So, I'm going to need, you know, a little bit of time, but I'm happy to kind of drive that a little bit, and, then, you know, I'll work with Harley. Other folks that would like to contribute to that, even if it's just to kind of look it over afterwards and give us some insight, sure would appreciate that. So here in the room, on the phone, please reach out and let us know if you'd be willing and able to help out, frame some of this vision around the four documents.

And I'm happy to circulate John's e-mail, or if you like, everyone can route through me. Are there things that people want to see in that document, other than sort of an overview, as you've listened today. Both John and Harley have been thinking about this problem and this process a lot, but I wanted to make sure that we capture all of the insights that are in the room today, about what that document might look like, what are some things they should keep in mind, the group should keep in mind as they begin to flesh that out? Yes.

Well, just some thoughts around perhaps -- and I mean, these have come out a little bit, but maybe it could be kind of collected and articulated, would be a little bit of context surrounding patching and upgradeability in the larger scheme of things, because there have been so many efforts, including the EO, that have come out that have framed what we're specifically doing out in the context of other efforts, and so I think a little perspective on what patching and upgradeability itself represents in the grander scheme of things might be good, maybe in the way of introduction.

Thank you. Anyone on the phone have some thoughts about what you'd like to see on the sort of overarching perspective?

Again, press "*1" if you'd like to make a comment.

It's good thing you're a good writer, John. Yes, please.

[Inaudible] from Wilkerson, Barker [inaudible]. Just, per my earlier comment, I think it could be helpful to articulate where some documents -- differences in scope of some documents, particularly the communication document is aimed at, I think, if I remember correctly, all end users, including consumers, whereas the capabilities document is focused, at this point, on enterprise procurement. So, it might just be helpful to explain that difference and why the maturity level.

And we do have a comment on the phone as well.

Oh, fantastic. Joe. The thing that nobody's mentioned is the insurance industry. They're the ones who have driven a lot of change nor the safety and security issue. So, I would suggest, if nothing else, just annotate that they need to be brought in at some point.

Fantastic. Thank you, Joe. I may reach out to you to see if there are some folks from that industry that we should engage.

Okay.

Any further thoughts on this notion of interactivity? So, one thing I will say is that the capabilities document cites the communications document a couple of times, and it's always good, I think, to have some cross citations. And now that there is a convenient way that we know there is a sort of canonical

pointer at ntia.doc.gov/iotsecurity, you can have a way to make sure that we can track it across the different documents. So, perhaps that something the different documents can use to sort of use to say, hey, this document will be here, even if it's not fully published.

Further thoughts on making sure that we're all helping each other in the different efforts? So, the last thing on the agenda today is to say, you know, next steps for the multi-stakeholder process writ large. We are currently due to break for lunch, but if folks are okay and they need to stretch a little bit, do we want to spend a half hour now having that discussion so that we can get the rest of our day back? Would that be a useful approach? We have consensus on that. Fantastic.

The big picture that NTIA has -- and I'll let Evelyn chime in on this as well -- is, you know, we really did hear that IOT security was a priority, and that this was something that had to be driven by industry engagement, but not just industry, one cross sector, making sure we heard from all different sectors, but also civil society, academia, et cetera.

One of the things we've tried to do was to scope it so that here was a particular aspect. So, we weren't trying to solve all of IOT. We weren't trying to secure everything. So we focused on patching. We focused on consumer, or at least, you know, not administrator devices. As you've seen this process happen, are there other areas that you would like to say, all right, when we get these documents accepted, the next meeting will have, hopefully, four different documents that will all be heading off in different directions, and we'll still be working with you to make sure they have an impact. But that doesn't mean that we can stop working. And so, if there's work that you would like to see continued, a pivot to a slightly different area of IOT security, using this non-regulatory model of multi-stakeholder driven collective expertise, we'd love to have your input. You know, we have a few ideas.

Evelyn mentioned the request for comments that we just had as part of the executive order, where we got some great ideas there. But a few if you have further ideas, we'd love to hear them. Evelyn, is there anything else you want to say on this?

I would just say that, you know, at NTIA right now, it's very difficult for us to host more than one multi-stakeholder proceeding at the same time. But we, you know, believe and we hear, daily, how many challenges there are in this area right now. And we want to be able to continue to move the work forward, but we do think it's helpful to be a little bit strategic about where we go next.

This work has been moving forward very well. We get questions about it daily from our government colleagues and others who are interested in watching this closely, interested in the progress, and it's helpful for us to be able to map out where we see progress going next as well. The ideas that we do just try to take on things that we can actually accomplish something in a short period of time under, or around, a year, I think is something that has been attractive to many, that we're not trying to take too much on, and to track progress as we go along as well, and to make sure that we're evaluating, even after we develop products, to make sure that they are having an impact. These are things that many have given us a thumb's up on on these processes.

So, when we did the RFP, just recently, as part of the EL process, as Allen said, there were several things that bubbled up there that could be a good next step. There are things, you know, that we think might be easier to accomplish than others. Again, especially in making sure that we can do it in a reasonable timeframe and show progress. But we're really interested in hearing from your all, because it's really the stakeholders that drive these processes. It's your ideas. It's the commitment from you and your organizations that make this work. So, we're really open to hearing from you today on next steps.

This is your blank piece of paper to say, hey, NTIA, we think you could make some progress on this. Any thoughts?

Allen, this is John. So are you looking for -- the answer's probably going to be yes to this, but I'll see if I can just get the conversation started. I mean, are you more interesting -- maybe it's not you. But do you think it's more interesting to try and identify sort of those broader brush issues? So, you know, patching and upgrading, that's a pretty broad-brush issue; right, in the sense that it is the related to most IOT devices, in some form or another. So, we could look for other broad brushes used, or you could look for more specific areas. Maybe it's been industry. Maybe it's by environment, where there's not a lot of work being done; right? So one comes to mind where there is aa lot of work being done is in the auto industry. There's a bunch of groups working on that, so probably we don't need to spend much time there.

But what about just the Smart Home concept. What does a Smart Home mean? What is the consumer risk? What should be the kinds of things that consumers need to think about, folks that are manufacturing devices. Expand the security argument a little bit of sort of that one issue of patching to what are the

broader security issues. Now, as a risk guy, because that's my job, I want to tackle those issues; right? I want to get right into the middle of.

However, I do also recognize, because I've worn policy hats before, they we don't want to necessarily get too much into the mud, where we start spouting off about how risky all this stuff is and people shouldn't buy these things. So, I understand that there's a balancing act in there. But I'm just trying to frame up, in my mind anyway, those are sort of the two options. You either find another broad-brush issue, or you find some specific environment or specific industry where there's enough multi-stakeholder interest to actually do something meaningful.

That is a fantastic framing of the kinds of ideas that we're talking about and looking at, so thank you.

Hey, Allen. One of the things we talk about FDAs Center for Devices is, while upgradeability and patchability is certainly a big issue. In your case, if the economics just aren't there to maintain the device -- John was talking about, you know, whether a producer has an appetite for maintaining something that's already been purchased, in the absence of that, what is the minimum level of security that we're willing to accept that will basically last or decrease risk enough through the duration of its lifetime that it's adequate? So, if it's a two- or three-year consumer product that's going to be upgraded, and tossed into two to three years, what's that baseline that will get us two to three years without an update?

That's a great idea. That's important problem that a lot of stakeholders that have recently talked to us about, so thanks. Just out of curiosity, at the FDA is that something you've seen explored in the industry?

Yeah. So, honestly, I think it's whatever dollar question is what's the minimum amount of security that's adequate, and how long is adequate for. You look at efforts underway to determine what, you know, what is that baseline, so you have other programs that have been accomplished. I think DOD and NSA, the intelligence communities have the NIAP program which is seeking to, you know, some assurance level of security. You have sort of device centric, medical device centric, like UL, trying to establish that baseline of security. So, I think that is the efforts underway. And FDA is always interested in, you know, both putting out policy that describes that, but also leveraging the power of the community and what they're doing, so, like, UL for example, and other efforts that are underway to describe what a baseline security is. We're not necessarily defining it ourselves, but we're leveraging the power of the community.

Beau.

Seth, that's kind of adjacent to another idea that I've heard and thought of floating around. It's a little bit almost if you look at that on the side, which is what is a reasonable supported support of a lifetime for devices, and then what happens after that. In other words, you know, defining what is an acceptable level of security and how long can that last, is one way to look at it. A different way to look at it is how long is an acceptable lifetime for it, and then when that lifetime ends, you know, how do you know when it ends? Is there some way you can predict it up front, or is it a matter of, you know, the security model expires, or is it a matter of, you know, it's replaced by something better? If people want to continue using that, especially an issue in health care, what must they do? You know, does accountability shift from manufacturer, at that point, to the operator or the buyer? So, there's a lot of potential things that could be brought up or brought out from that type of process, looking at the timeline and establishing something there.

Yeah, I have to second that effort end-of-support, end-of-life discussion, tiered to, like, a consumer level versus, say, medical equipment level, which we're really getting at is risk. But, yeah, that's a topic that needs consensus for sure.

Excellent.

I'm sorry, Allen. Just thinking broad-brush topics, you know, what about things like we actually -- it came up today a little bit, you know, the fact that encryption can be challenging, and maybe that's more of a research kind of project than multi-stakeholder, but encryption is an interesting sort of concept when it

comes to IOT. What does that really mean? Authentication is another one; right? What are the authentication challenges or requirements around what should devices do to authenticate themselves? Is it okay that anybody can walk into my house and tell my Alexa to do whatever they want it to do; right? You know, should there be other types of authentication mechanisms? And I'm only picking on Alexa, by the way, because I love it. I own three of them now. So, please don't misinterpret my comments.

But my point is, is that, you know, because I've interacting with these devices now for several months, you know, these are the kinds of challenges that I see. And I wonder if maybe it's not those, or maybe it's a collection of those, if there's a way of taking these sorts of other interactions that we have with these devices and turning that into a multi-stakeholder project of some sort. I'll keep pondering it, but those are the things that come to my mind, because they're old security challenges, but what do those old security challenges around encryption and authentication, what do those mean in this world with all of these devices? Is there something more scientific, if you will, that we can do as part of a multi-stakeholder approach beyond saying, you know, this is hard or whatever. I like that.

Thank you. And I should also point out that our NIST colleagues are doing some great work right now on lightweight encryption to address this particular issue from a technical perspective, and maybe it's a good time to start thinking about it from a policy and business perspective. Chris Gates is on the line.

Yes, sir. Thank you. Chris, your line is now open.

Hi, Allen. I wanted to address a couple points that were being made here, one of which is thresholds. I really want to advise against any sort of thresholds for this. I mean, there's two parts of it, one of which is a good example, Target was PTIC payment card compliant when they got hacked and breached 90 million payment card information and pharmacy information. Those kinds of things lead to a sense of false security. And the second one, the thresholds, is business motivation and limping into this. They go, great, we're going to make it just to the point where we're just going to make that threshold, and this happens certainly with the FDA, when they become the standard, when they should be the minimum standard not the maximum standard, and so I really worry about that a lot.

And then, lastly, to John's point about encryption, you know, this was once a case when we were all dealing with 8051 micro controllers out there and old, old, old 20-year-old components. Today we're all dealing with componentry that runs off of coin cells that can do AES-256. The libraries are all for free out there. You can download these. Anybody can. That are high quality encryption libraries, hashing libraries they can be used for government-level, state-level attacks. I mean, you could implement the Whisper Systems protocols on these devices without any problem at all, and all of that while running off of a coin fill battery. So, the argument that we no longer have the resources to do is it not really there anymore. It's a matter of the will and motivation to actually put this into place in our devices. That's it.

Thank you. Really good point. Anyone else on the phone who would like to weigh in on other areas, whether they're broad crosscutting issues that are fairly well defined, or specific sectors or applications, where this type of progress can make some progress?

And, really quick, we do understand that there are some technical difficulties for new people trying to call in right now. So, if you have some other points or questions and you're having a hard time with the phones, please shoot us an e-mail. I think Allen has e-mail up just a little bit ago, and we'll hopefully be able to get your questions that way.

And, also, if you don't mind, I'll repeat the number to dial in. It is not 1 (800) but instead, 1 (888) 205-4738.

Thank you. I appreciate that.

So, I wanted to make one quick follow-up point they think underscores the, like, focus on timelines and into why what's reasonable, is to Chris's point, I think it was Chris on the phone. Today we do have those capabilities, but just like we have different timelines for different devices, in 20 years, when some of the things we're building today are in the field, we'll say, oh, gosh, we have these great capabilities today, 20

years from now, in 2037, if only we had had these back then, I think it's going to be kind of a perpetual rolling issue of technology increases, landscape changes, et cetera, et cetera.

So, while we do have these capabilities today to do things, there are two potential kind of corollaries to that, which is what we did 20 years ago that got instantiated into products that are still being sold today is way, way less than what we can theoretically have the capability of, and just like we see Windows XP on a bunch of different systems or older operating systems, it's not that Windows XP was bad, it's that we have a lifetime of devices that exceeds the underlying software components and hardware components capabilities for what they're being asked to do today, in today's environment, et cetera. So, in 20 years, we're going to have the same issues we have today, so it's not going to go away, which, you know, makes me think that maybe something around timelines, not necessarily thresholds, but timelines, might be a good something good to at least have some consideration around the next event.

Yeah, I'm not sure if this was said already, because I was messing with my phone earlier. But, you know, since we started this entire process month and month and months ago, I don't think we've had a meeting where someone didn't stand up and go, well, what about privacy? So, you know, privacy within the area of IOT and consumer products is an area that I think should be looked at. Like I said, I don't think we've ever had a meeting where the topic didn't come up, so.

Thank you. We do spend a lot of time at NCIA speaking about privacy, especially Travis, who is our privacy point person and runs some of the multi-stakeholder processes on privacy. Final thoughts about where we might be able to pivot to next, building on some the successes we've had? Are folks generally supportive of this approach of trying to tackle this issue? You're allowed to shake your head or send up skeptical e-mails too. I should say we have heard some enthusiastic e-mails as well. So, if you feel strongly this is not a good use of time, please let us know, either publicly or privately.

Allen, this is Michael, if I could --

Michael, you're on.

Thank you. I've got one, what now may be a stale comment, which was citing a couple of candidates for the conferences. Folks probably are very much aware of RSA coming up in April of 2018, which would certainly be an important opportunity to get the word out. But the ABA has now, for the past two years, run a national institute on IOT policy with several hundred attendees in not only the legal profession but policy and technical experts, and we'll be running another one in May of 2018, the third institute.

And finally, I would commend to folks' interest, as a possible additional stakeholder, for a variety of reasons, not only the fact that they run some fairly impressive conferences but because they have shown an interest in the development of security policy, and that's the state attorneys general.

I have spoken on IOT, along with Naomi Lefkovitz from NIST, at their technical conference in Charlottesville in April, and then I was on a panel with Attorney General Rosenbloom of Argon at their annual meeting in Bozeman in June, and now they've got another conference coming up in November. And they have shown a particular interest in challenging federal preemption jurisdictionally in areas where there's federal regulations, such as connected medical devices and vehicles. And they're particularly concerned with the possibility that the regulatory structure in place for many IOT devices fails to address the security risks inherent in them and leaves consumers vulnerable to injury without any remedy because of the existing federal preemption posed by the regulatory structure. So, the attorneys general seem to be ramping up what may be a greenfield of opportunity for interest and participation as an additional stakeholder.

Thank you. I really appreciate that, and I'm glad you were able to get in, and I apologize that we had such difficulties earlier. Joe.

I was just going to answer your question earlier. Yeah, I think this is a worthwhile effort; right? I mean, I don't know how else we can tackle some of these issues without having some mechanism to collaborate;

right? We don't have to solve all the problems, but I think we've demonstrated the value in this and the outputs that we've created over the last year. I don't think there's any question about that. So, regardless of where we pivot to next, I would just encourage this collaboration and the multi-stakeholder process, absolutely.

Thank you. Any last thoughts before I ask your input for scheduling the next meeting? So, just glancing at a calendar, I think it might make sense to think of sometime in early November to have a virtual meeting. We've had two of them so far, and I think they've been fairly productive. We've been able to have some good conversations and good presentations. They also tend to run a little shorter. Anyone have strong thoughts or things that we should be aware of what's going on in early November to plan around. Is there a week-long IOT summit that everyone in this room will be at? Is there a really good party that you haven't invited me to that I should know about?

All right. Well, then we will work on trying to put together a time and date for that. What we've heard today is some great progress from three working groups, and we have the standards group, which has pulled together a lot of data. They've worked really hard on getting this into a fairly organized standardized, if you will, format, and then the next steps there are to say, well, how do we make that sustainable, and they're going to come back with a couple of potential ideas to suggest.

The capabilities group has really managed to focus quite nicely on understanding what the steps are and how secure them. And we've heard from a lot of people today, saying, hey, we want this out there now, and so they're going to work on finishing that and editing that. If there are folks who you think should be engaged at the technical level on that, or also want to help with the editing side, that's wonderful. And the incentives and barriers group is looking for a little more input, where they can actually validate some of the assumptions that they're making and perhaps think of a couple more use cases to sort of demonstrate the value of their model. Is that a fair summary of the working groups?

I think, you know, just reasonable we might expect these to be pretty close to done in two months; yeah? For what we're looking for. This's already, Daryl, we'll ask can he not to do it. He didn't show up this time. And we got some great input on how to take these documents out into the world. The communications group is already in the process of doing that, and they're going to come back and report what has worked and what hasn't. And we going to also talk a little bit internally about what the next steps might be for the broader multi-stakeholder process. Any further comments or addenda to that summary?

Yeah. The introduction.

Oh, thank you.

So, I mean, I would like to plan to discuss that at the next meeting. I think we can have something for people to digest by then.

That would be fantastic. And I'll work you and Beau, and we'll talk about --

Harley.

Oh, sorry.

Oh, did you volunteer, too, Beau? Thank you so much. I appreciate that.

I'll work with you and Harley, and we will see if there are some other folks that might be able to help. All right. Well, as always, it is my chance to thank you. I also want to thank Megan Doscher, who is our other cybersecurity person at NCIA, who does a lot of internal-facing federal cybersecurity work. Travis Hall, who is NCIA's privacy guru, and our fearless leader Evelyn Remaley. But perhaps most importantly, thank you all for your hard work, for showing up, for continuing to engage, if, for no other reason, to show up and make sure that we're not messing up, because I know a lot of you are focused on that side, so that's

great too. We're trying to find something that makes as many people happy as possible, and I think we really are making some great progress.

And a thank you to Allen as well. Thank you.

We'll talk in a few moments. For those who were watching at home, thank you for watch, and please, as always, don't hesitate a time to reach out if you have any questions.