20170426-ntia 1-part-1

ALLAN FRIEDMAN: Welcome everyone to the third meeting of NTIA's Multistakeholder Process on the IoT Security Updatability. We're still working on getting updatability entered in the dictionary. I know a couple of you reached out to us. That's the kind of work we try to do at NTIA. But while we're working on that, we're also trying to help with the broader security of the IoT ecosystem. And thank you so much for those of you who were able to come out today, and thanks to those of you who are watching remotely. We know that travel is really hard, and giving up a whole chunk of your day to discuss this issue is difficult. We really appreciate all the time you've taken.

We're going to go over the schedule and get into the presentations in just a little bit, but first I'd like to pass it over to my boss, the Deputy Associate Administrator at NTIA, and our fearless leader on all things cybersecurity, Evelyn Remaley.

EVELYN REMALEY: Thank you, Allan. Let me just second Allan's welcome to all. It's really nice to see all of you. This is actually one of my favorite parts of my job, actually getting together with all of you who are actually making real difference on security in the ecosystem. So, thank you. Thank you for all coming. Thank you for all committing to this process. I know that some of you actually volunteer your time, and your companies and organizations volunteer your time, and we appreciate it very much and we appreciate the work that you're all doing here.

I usually spend my days in a lot of secure conference rooms, so when I can actually get out and see all of you and see what you're thinking about, and how security is actually affecting your day to day, I really appreciate that. So, thank you again. Thank you for your commitment to voluntary processes. We, at NTIA, are very committed to that as well.

So, let me just jump in and give a little bit more history about the process as well, and talk a bit about our expectation of our partnership here, and talk about where we're going. NTIA believes that an open, transparent consensus-based process that brings stakeholders from across the digital ecosystem is one of the best paths forward to addressing important security issues in a realistic and timely fashion. Since we launched this multi-stakeholder process last fall, four working groups have been toiling on their chosen areas of focus. The goal of this meeting is to share your work and collect feedback from one another. Now is also the point in the process where we begin to develop a shared idea for the outcomes of this process, determine the best audiences for those outcomes, and strategize on how the outcomes can have the greatest impact.

Following the publication of the Department of Commerce's Internet of Things green paper, which I'm sure everyone has read, we put forth an RFC requesting comment on the paper. Several of our multi-stakeholder participants contributed comments to that RFC, and we thank you for your insight. We have been reviewing those comments and considering next steps with our leadership. Securing the Internet of Things remains a critical issue across the U.S. government.

We, at NTIA, are working hard to coordinate with our colleagues at NIST, the FTC, DHS, and across the government on how to address this large and growing issue, and exploring how to give security experts and industry leaders a strong voice in identifying and developing solutions. Furthermore, as you no doubt well know, IoT security transcends national borders. The issue has the attention of other governments and organizations around the world, and we've been working hard to collaborate with those constituents as well.

Those of you in this room and those of you participating remotely 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 that have contributed thus far and appreciate your continued commitment to this effort. And, with that, I'm very much looking forward to hearing where we are. So, thank you, Allan. And I just want to acknowledge the great NTIA team who has worked on this as well, Allan Friedman, fearless coordinator; Megan Dosher [ph]; and Travis Hall. So, thank you. And let's get started.

ALLAN FRIEDMAN: Thank you, Evelyn. So, I see some new faces in the room. That's fantastic. The goal today is to try to get as much feedback as we can on what we're -- what we've been building, and figure out how we can move forward quickly but with full consideration of every respect. So, our approach to technology policy is that we need to hear from every part of the ecosystem. And we have in the room great engineers, we have pretty good lawyers, we have some fantastic policy experts, we have advocates. And the solution to this issue isn't going to come from any one of us, but from all of us together. We think that we can make some real progress today.

So, don't be shy about chiming in, about weighing in on what you think. Those of you who are on the phone, we're going to work very hard to make sure that you can engage. So, we have two ways of remote viewing. One, there's a live webcam, which, if you can see me, you're watching. Thank you for that. There is also a call bridge. The details are on the NTIA website.

And when it comes to audience participation time, you may want to call. We apologize. There's about a two-second lag between the call and the video stream. The Internet still is the Internet. So, we're going to work on that, but if you want to chime in on this conversation, it's "*1" and you'll be in the queue. We'll try to get to you as soon as possible. If you're having trouble, please backchannel through someone in the room, or you can email me, AFriedman@ntia.doc.gov, and that way we'll be able to have as productive a conversation as possible.

So, walking through the schedule for today, we're going to be hearing from the four working groups. We're going to start off with Technical Capabilities, walking through, you know, what are the actual steps of an update and what of the -- how do they match with the capabilities of the device. We're going to be thinking about technical standards, what's already out there that we can build on. From the technology side, we're going to pivot towards the consumer approach, how do we communicate this update question. And then, finally, we're going to look at the thorny issue of policy, barriers, incentives, how do we actually make this vision from something that we're talking about in this room to out into the wider world.

So, we're going to have presentations from each of these four working groups. They'll give a short presentation. We've got 45 minutes; that should be plenty of time for discussion. If it runs a little longer or shorter, that's okay. We're fairly adaptable here. And there will be a lunch break from 12:30 to 1:45. There are a number of great places nearby. Some of you who used to work in this area might be able to help point folks to particular places for lunch. After lunch, we'll pick it up with the final working group presentation. And then we're going to have a broader discussion, trying to sort of zoom out and say, okay, based on the feedback we've heard today, what more do we need to do and how do we get to our target audience, how do we sort of think about aiming this towards a wrap-up, and what is that going to look like.

So, with that said, again, if there are any questions, feel free to chime in. If you're in the room and you would like to speak, I'm going to request, and we'll probably have to remind each other to push the microphone button, and that way the folks listening at home can hear you as well as you'll be more audible in the room itself. So, with that, let's hear from the Technical Capabilities group. Shrinaf [ph], do you want to come up and we can load the slide deck for you to talk?

It's not. It should be on the desktop. It's on the desktop. Yes. So, thank you. Give us just one moment. So, yeah, it's on the desktop. And you can -- I can drive for you while we do it from here or you can do it from the podium, whatever you -- great. The floor is yours.

SHRINAF: [Inaudible] technologist. I'm working with [inaudible] group [inaudible] in the [inaudible]. We are working from last [inaudible] months on this particular [inaudible] putting all the categories and the devices and all this stuff, and having a very good conversation [inaudible]. So, we have put together some stuff [inaudible] been working on [inaudible] this is work in progress [inaudible].

So, what is this work group? Background is [inaudible] what we are thinking is [inaudible] approach. It is not like one person presenting and providing [inaudible] and we need to accept [inaudible]. So, it's a shared. You bring your ideas. We will discuss those ideas. And we will see what are the positive aspects of it and what are the constraints if you want to implement that kind of stuff [inaudible] and we will say, for example, the device categories, they're all devices in the field which are computing constraints, one or maybe some of the devices are very critical in the infrastructure where that definitely requires kind of a very secure mechanism to make the updates. Whereas a small device, for example, in the home kind of environment, those kind of devices may not be able to make the updates securely because of the computing constraints and the crypto constraints and the power constraints and all that stuff. So, in that way, we have to -- we did the categorization and then we are trying to say what is called a scalable security approach can be made here.

So, that's the first thing, make a list of all those things and make a baseline for these objects. Then the steps of an update and the necessary technical capabilities, yeah, this is what I have already mentioned in the second point. This is the desired outcome, what we are planning. If there are anything we need to add, we can discuss that. The goals and audience, here it is, it's everything is voluntary. There is no membership, nothing kind of stuff here. And we are not making any kind of a recommendation or it needs to be implemented kind of a thing. And there is no regulatory this one also. So, it's all non-regulated and it is what we call it is a guidance. [Inaudible] you can call it as some kind of a recommendation for the implementation [inaudible].

And the second point is very interesting. So, when we are doing some new -- we bring in new technology and introduce new stuff, that should not pose any risk, security risk. Just to give you an example, okay, now we are connecting all devices into the network. Can I connect all the devices into the network, including the very critical infrastructure kind of a thing to an external regular Internet? That could introduce -- may introduce some security risk. If you want to do that, you may have to address some of the issues and vulnerabilities that may be able to [inaudible]. Come on.

This is mainly -- all this guidance and those things we're covering aimed at IoT device manufacturers, solution implementers, system integrators, and also the deployment and maintenance people, because when you talk about kind of an update of the system, that means, in some cases, the maintenance people, they will be able to do -- they will be able to deploy and maintain the system. So, that means you have to have a capability to who can do the update, the person, the automated system, or over the network if you are doing all this what we call it is end-to-end security. For example, the person who wants to deploy the ability new phone software configuration, from that he will throw it from a remote location he wants to update in the field, that means the channel from remote location to the end point, the complete path should be secure. If any point, if you miss something, that's a vulnerable channel.

The scope is -- we restricted of scope. Can we do all the devices which are sitting in a physically secure location and all this stuff, or it is not connected devices? We decided to have the scope limited to connected, remotely addressable devices and systems. If you are within a lab environment or within a physical secure environment where you can do an update of the device or update of the system physically, then there is a -- we are not considering that. That means we can use a different secure mechanism or safety mechanism. We know who is doing that. Our authorized person will be doing the update. So, we are not covering that part of it. We are considering the remotely connected devices and systems.

Yeah, we reviewed wide range of devices and categories, capabilities, and use cases. We discussed several update mechanisms, both updated and human intervening. Although we talked about remotely connecting and doing it in some cases some of the devices in the remote, the end to end part may not be able -- feasible to have the automated stuff. In some cases, we may have to use some exception where in the end place some manual intervention may be required because he has to personally verify that, validate this is coming from a trusted source, and then he can trigger the update mechanism. That way there may be some kind of manual intervention maybe there.

We mapped out the necessary steps update process, including basic. We decided to make some kind of a category. One is the basic for any device -- the basic necessity kind of stuff. And then other stuff is it depends on some kind of use case [inaudible]. So, we made two different stuff. We will talk about that. There is a table prepared in that. We can go on and discuss that.

In our discussion from last three to four months, we -- like everybody will agree with me that there is no one-size-fits-all model. I cannot take -- like, okay, I have a solution, I will go and implement this from a small ten-dollar device to a multi-thousand-dollar systems. So, we may have to -- as I mentioned earlier, we may have to find a scalable approach to these kind of implementation. But although we say that it doesn't fit, but we cannot say that I will have 15 different types of mechanisms. So, what we need to do is we can sketch out the components of a bid that fits the general use case. You make a basic general case kind of a thing, this needs to be done. Okay. The basic thing is okay, I need to do a kind of an authentication, an authorization; who is doing that?

Then, next level, do I need to communicate -- do I need to encrypt this data kind of a thing? Again, it is use-case-specific. Then, the next trip is do I need to do it in a secure communication channel or normal channel is okay? If I encrypt and do the integrated measurement kind of a thing when the -- in the packet which I am sending, can I send over a plain channel without securing that particular channel, or a special tunnel, kind of a secure tunnel is required or not, these are use-case-specific. So, we can increase the level of security by doing step-by-step.

And also when I'm using, can I -- do I need to do -- for doing the authentication and encryption, do I have to use standard crypto algorithms mechanisms? What is the key size I have to use? What type of algorithm I have to use, RSA, [indiscernible], what key length I have to use? These all depend on the use case and application use cases, and what is the value you're protecting. For example, if you are protecting -- I'll take an example of a smart meter where you are protecting the signal, the prey [ph] signal of a kind of a thing when you are transmitting that kind of information, you need to be very careful because that's money.

So, the value of protecting. So, in that case, you might have to think about encrypting that kind of [indiscernible] with crypto mechanism. This is where we -- this is not a one-solution approach. It's a multi-stage or multi-phase approach we need to take. There are different use cases, and security contexts will have different security needs, specific additional features to update. Based on this, we may have -- that's where I'm reemphasizing that scalable security solutions need to be decided.

So, the basic use case, we attempted to establish what might be seen as the minimum one. All these were driven by people brought some use cases and we discussed all the stuff. Some use cases were made for [indiscernible] like, as I mentioned, some application and some use cases are very basic. We have to implement those things. On top of it, depending upon what value you are protecting, how critical that information is, how the device is used, what kind of application, it's a nuclear facility or an electric directory infrastructure or it is a financial center bank, or it is just a smart home [inaudible]. Based on those kind of application scenario, you decide what level of security needs to be implemented. [Inaudible] components and technical. Yeah.

So, steps understood as a baseline for updates. Sorry. The -- we discussed about some of the baseline what we need to do, kind of updates, mapping between -- how we can map between the components and technical capabilities. When we say "component," it is not only the physical component, we are talking about the logical software modules or the low-level firmware, booting of the system, booting of the device, some other things, operating systems -- the [indiscernible] operating system used in that, and application layer software, which we have to consider all these things when we need to talk about the implementation factor.

So, at this point, I'll stop now and I will hand it over to Allan so that we can continue the -- do you agree with these kind of designations? Do you think anything is missing and what are the appropriate next steps we can -- over the course of the day, we will discuss these things? Thank you. Thanks for the opportunity.

ALLAN FRIEDMAN: Thank you. [Inaudible]. We're swapping out mics for a second, so I'll just use this for the moment. So, we will try to pull up this handout that you should all have, which is a two-sided table that walks through what this working group has said here are the steps of an update. Give us one moment to pull it up on the big screen. This is why we have the handout, because the type is fairly small. And Angela, I think we also, if we can, we're going to go into Q&A on the call line so that folks can chime in.

And if we can open up the mics of, I think, Jason Wall [ph] and Tim Hahn, since they're part of this working group, if they have contributions to add, in addition to what Shrinaf just said about the working group. So, let's start there in terms of anything further to add.

ANGELA: Lines are open.

TIM HAHN: Yes. Thank you. Hey, Allan. This is Tim Hahn.

ALLAN FRIEDMAN: Hey, Tim.

TIM HAHN: Hope you -- obviously you can now hear me. I just wanted to reinforce that it was a good overview and I think that the items that you see on the two tables are the things we've identified. There's obviously still more work to do, but I think they serve as a great understanding of requirements or what we see as required for basic updates and then additional items based on use cases in the second table.

ALLAN FRIEDMAN: Thanks. So, now is the chance that both the room and those of you who are watching at home can chime in and say here is why everything you've been saying is wrong. And so -- yes, please. And just as a favor, for the first few hours of discussion, if you can just introduce yourself, if you like say where you're from, so that folks can get to know each other in the room.

RALPH BROWN: I'm assuming, for those in the room, holding a hand up will be sufficient to indicate being in the queue.

ALLAN FRIEDMAN: Yes.

RALPH BROWN: Okay. Good. This is Ralph Brown. I'm the CTO of CableLabs. I had a question. When you talk about value in terms of what is being protected, are you considering not only direct value but indirect value? And so let me pause there.

SHRINAF: It is both. Direct value was -- it's a cost; right? For example, that's why I give you the example of a smart meter when you are remotely updating the price signal kind of a thing, this is a direct -- this one. Indirect values are, for example, when you are updating the device through this one, you broke the channel, somehow security attack happened. Now, when you happen that some of the loss is -- the corporate which has deployed this kind of a stuff has a reputation that's lost. For example, the update has happened, the target breach has happened, financially they lost, but, at the same time, the target also lost the brand value. So, that's the brand value and this one, it's not only brand, it can be applied to any critical infrastructure. For example, this particular power utility has done that. For example, if you take San Francisco area, PG&E or in the Southern Texas or some kind of other thing, they lose their brand value. That's the thing. They are -- the brand value is not a direct cost. It's an indirect one. So, I will take that.

RALPH BROWN: Okay. One of the things I would like to add is, so, for example, in the consumer marketplace, there may be -- one of the things I always like to say is lightbulb, you know, how secure does the lightbulb need to be? It has a processor. It has internet connectivity. You know, it has memory. It's a computer. It has the capability to do various things. If it can act like a controller on the consumer's network, then there are ancillary value that gets at.

So, for example, I can now detect -- control the lock. I can open the lock, I can access the home. And so the risk associated with theft could be a safety issue in terms of smoke detectors and other things like that. So, I think it's very important to look at the other indirect effects, because that really is the value you end up protecting.

ALLAN FRIEDMAN: And forgive me, I'm going to chime in here as I try to facilitate. One of the things that we've found in these discussions is the broad issue of IoT security is a massive issue, and very important. And one of the things that we've tried to do to sort of target the conversation is to sort of focus on applying things to mapping it back to the software update question. So, you know, for example, we're talking about the value of risk, how does that change understanding of updatability?

SHRINAF: No. Perfect -- you are -- we can have an offline discussion, too, one-on-one on this topic. In an overview, you are exactly right. I'm coming from a company, we provide the security solutions. From a scalable approach -- that's the word I was using -- I need to notice the same thing, the same "cautionality" comes. Lightbulb, they are becoming intelligent. So, from my perspective, everything is intelligent, capable of communicating, needs to be secured. That could become, just as you said, a small device with -- you may ignore the lady, but that has that kind of a capability, that can steal a secret, safety issues, privacy issues, all these things can happen.

So, from that perspective, the answer is yes, but, like as Allan mentioned, our focus was on the update. That's where I always bring in the scalable security. Yes, we need to identify that [indiscernible] lightbulb. I need to identify the data. For example, just I'll take a minute and complete the answer. For example, in a home, you have a smart meter, water meter, and gas meter; right? What can I -- do I need to have the same level of security for all three? No. We need to design in such a way that water and gas meter can identify itself as, like, a brand protection kind of thing. They can provide the data information in a local [indiscernible] kind of communication that the electrical meter, whereas electrical meter can act as a hub in the home this one and that can communicate with -- or a gateway built in your home can communicate to the outside world. In that way, the level of security required for water meter and gas meter is I'll say low to medium, whereas your electric meter is a medium to high, in that where the categorization comes into picture -- device categorization.

ALLAN FRIEDMAN: Great. Did you have anything you wanted to add, to follow up on this? So, we've got a couple of questions on the phone. Angela, can we hear from Seth, who's been very patient?

SETH: Hey, Allan. Actually, I was just chiming in to complain about the mic, but I feel like that's been settled. No comment on the update process right now, but thanks for giving me the floor.

ALLAN FRIEDMAN: Thank you. Question in the room.

JUSTIN CAPPOS: Hi. So, I'm Justin Cappos, NYU. I have kind of, like, a bunch of questions here. I'm coming into this meeting a little late, and I want to apologize for this. But I -- there's a lot of concerns that a lot of traditional update systems have, especially those that are designed for security hab [ph] that I'm wondering if they're not maybe adequately discussed in parts of the document. So, issues like protecting against different types of attacks that seek to keep clients from obtaining updates instead of tampering with updates; there's different classes of those types of attacks.

There's also attacks relating to the infrastructure itself. Historically, there have been a lot of major companies, Microsoft and Google and Fedora and Red Hat and Debian, and I could go on and on, that have had people break into different parts of their infrastructure and distribute malicious updates that way. And I am willing to bet that most IoT device manufacturers are going to have worse server-side infrastructure security than those major companies that I just discussed will. So, it makes it even more important that they design the system with the understanding that attackers will break in to parts of the system.

So, there are a few different types of update architectures that are meant to protect against those, including some that are even specific to IoT. So, I would be happy to follow up and bring those to peoples' attention so that they can be added into more of the discussion. I want to pause here and I have one other quick thing I want to say, if there's no other --

ALLAN FRIEDMAN: Any reaction from Shrinaf or Jason or Tim?

SHRINAF: Yeah, you are exactly right. So, let me use the microphone. Yeah, you are exactly right. That's where, in our discussion, all these topics came up. One is protecting the stuff -- one is a kind of a license management kind of stuff. Who can get access and who can do this kind of a thing? That's where it comes, the authentication, authorization, access control, and how do you do that, and the channel, which I mentioned in my earlier presentation that it's in the end-to-end point security. The firmware living in a server, that needs to be signed and verified -- signed by a third-party CA so that it is not particular to a staff. And then when it leaves there and then the secured channel will take that to maybe a multiple hub because we may have multiple hubs, multiple -- it may have to pass multiple servers.

So, all these servers, any point in the channel coming to the end point, for example, your thermostat at home, when you are trying to update, so the complete path needs to be protected. And when the blob of data comes into the end point, that's where you verify it, because it is signed by a crypto mechanism, you verify that. Integrity is checked; that means nobody modified anything in this one. And, first of all, you establish a secure channel. Then you transfer everything.

And when it comes to your end point device, where that credentials to verify that authenticity, that is where it will be stored, for example, a tamper-proof storage. When you have that credential sitting there which never leaves that particular tamper-proof storage secure micro [indiscernible] when you do that, the verification happens within that secure micro. And then when it comes back, it decrypts and verifies that. In that way, you can securely do those [inaudible].

ALLAN FRIEDMAN: So, I want to avoid getting too far into the weeds, but flag this. And we love the participation [inaudible] please do --

JUSTIN CAPPOS: Give me just ten seconds. So, Fedora, which was broken into twice, by the way, had exactly this design, and it didn't protect them either time. So, there's -- there are things out there that I would love to discuss offline with you that should be -- I think should be a major concern.

ALLAN FRIEDMAN: Well, and I think that's -- you're raising a very important point, which is scoping the security question, because, as I understand you, you're saying it's not just the device that we need to think about, it's the organization that is providing the patch. And traditionally I think with this discussion, because IoT is such a big issue, we have said the manufacture and development is going to be a separate discussion. But I'm hearing from you that at least the operation and maintenance needs to be part of it.

JUSTIN CAPPOS: Right.

ALLAN FRIEDMAN: Just a quick whip around the room. Do people -- what do people think about that scope of saying we need to actually look at the organization or provider as well as the device manufacturer?

JASON WALL: Hey, Allan. This is Jason Wall.

ALLAN FRIEDMAN: Jason, go ahead.

JASON WALL: So, my question for Justin, are you talking about securing sort of the location of the updates [inaudible] server system, or are you talking about also securing the API that, you know, can cause remote updates?

JUSTIN CAPPOS: It's a little hard to hear you, but what I'm talking about is effectively what a lot of organizations do is they have different people in different roles that go and perform different actions, and these people have to have signed metadata in different steps of the process in order to get things out. And so these kind of policies and procedures are -- you know, over the last few years, have become very commonplace in major technology companies and cloud providers and, you know, areas where security is important, including, like, automotive/space has things in this realm. And I think it's something that is becoming kind of industry best practices.

ALLAN FRIEDMAN: Craig.

CRAIG SPIEZLE: Craig Spiezle, Online Trust Alliance, Internet Society. I think your point is valid. I think as we look at the problems, and I've been part of most of the working group efforts here, is there's a range of companies. And it is -- as we look at patching, we need to look at the integrity of that patch, error check it and such. And we have found those are risk vectors. So, I think we have to look at that.

Allan, to your question of the manufacturer and such, the process, I think the integrity of the patching is clearly something, but we also need to recognize that in the vast array of companies coming to market, there's a whole range. And when you say, well, metadata and different people, it may be the same person within a company. And so their processes of code development are very broad and varied, and I think we have to recognize that. And so, as we look at the framework, we need to identify those issues and hopefully they adopt as many of these as possible. Clearly, we are at risk of the integrity of the patching process as well.

ALLAN FRIEDMAN: John, very quickly, and then back to Ralph. Do you have a response?

RALPH BROWN: Yep.

ALLAN FRIEDMAN: Okay.

RALPH BROWN: I was going to say you raise a very important scope question. In our previous conversations, you've allowed that this is just one aspect of security within IoT. And so if you're trying to define that the scope of this work is really to guarantee the integrity of those updates, then I think that is definitely within scope. If you say it's just a matter of guaranteeing that updates take place, that's a smaller scope.

ALLAN FRIEDMAN: Thanks. John.

JOHN BANGHART: Yeah. Hi. John Banghart with Venable. So, I think that the question that I heard you ask, Allan, is whether or not the sort of things we're talking about here, broadly speaking, are in scope. And I think the answer is definitely yes. And in working group four, which we'll hear about later today, we actually account for that. Again, very high level, but we actually account for the fact that there's software, hardware, service provider, different elements that all come together, that may be different companies, different people, that all assemble to actually create whatever this IoT thing is.

ALLAN FRIEDMAN: Great. Just want to make sure if anyone has one more two-fingered contribution to this conversation, and then we can go to the phones. So, we have James from Juniper. Angela, we have a question in the queue.

ANGELA: Your line is open.

JAMES: Can you hear me?

ALLAN FRIEDMAN: Yes, we can now. Thank you.

JAMES: Oh, okay. The question I have may be a policy issue and may not. What you've done in this first part of this -- or this first working group focuses on the manufacturer and his process, or the developer of that device, how he updates it. What happens to either the government or the developer or whoever, the industry, to update the consumers to tell them that there is such a thing as IoT, IoT updates, IoT security updates, et cetera?

And in that vein, for example, I have probably dozens or more IoT devices sitting on my network in my home. And I block all paths in and out, except those that I want allowed. How does now the IoT device tell me I should allow an access so that the developer, manufacturer, whatever, can download to me an update, or that I can send information back on my network? Because I own the network, not the service provider, not the IoT vendor, not the data processor. I own it and I control that data. How do you get that information out? This is a consumer issue really, but it is a technical issue that most consumers couldn't deal with.

ALLAN FRIEDMAN: So, on the consumer issue, we're going to hear from that from working groups three and four, but on the technical question, Shrinaf?

SHRINAF: Yeah, so this is, again -- that's a good point. So, now you have let's say ten or 20 devices at your home, but whenever you bought those systems you must have also signed up with something with some service providers. For example, you bought a thermostat. Whoever installs that, maintains that, are you -- your home appliances, anything you buy, service agreement. In that service agreement, you can make sure that mutual communication is possible in the sense, as a consumer, you should be able to talk to the service provider, those are all need to be defined in your consumer agreement. If you say that, "I don't care," that should be there in the agreement, "I don't want to do any update to this one," fine. Or when the update happens, when the new firmware comes or the new configuration comes or something like that, then I should be able to do that. They have the -- you have to authorize that. Consumer should authorize the service provider so that they can automatically do that, irrespective of what you are kind of a thing. So, those are the agreement you have to put in place.

JAMES: Well, I can tell you as a response that most consumers do not use their or read their user agreement, and they have no idea what you just talked about.

SHRINAF: That's where the service provider and all those things, they have to talk to them. For example, if you are -- if your device is a risk to my network, I will penalize you kind of a thing. You have to force -- sometimes you may have to use the force them, because you are connecting to your network and that's a vulnerable one, and that's a problem for the whole infrastructure, not only for you, because you are not only compromising your device, the neighbor's device, too.

ALLAN FRIEDMAN: And James, I just want to say that, in terms of communicating with the consumer and having that be a bidirectional conversation, I think the work that we're going to hear from later from working group three might have a lot to say about it. If you don't hear what you're looking for, please chime in on that issue.

JAMES: Okay. Thank you, Allan.

ALLAN FRIEDMAN: Thank you. So, I wanted to sort of focus on the document that we have in front of us. And for those of you who are on the technical bent, are there steps that you think we're missing? And for those of you who are on the policy side, how would you like to see this sort of document used in terms of -- that's something that we've talked about in the group? And Tim and Jason, please chime in. But we have --

JUSTIN CAPPOS: Sure. So, Justin Cappos again. So, I have a bunch of kind of specific technical places in the document. Is this the right forum for me to bring this up or is this detracting?

ALLAN FRIEDMAN: I think, given your level of engagement and your particular expertise in this area, we may try to draft you into the working group. And perhaps over lunch Shrinaf and I can sit down with you. Does that make sense?

JUSTIN CAPPOS: Yeah.

ALLAN FRIEDMAN: And if people are very excited to hear -- because we definitely want -- can you give the high-level summary or a couple of very quick bullet points?

JUSTIN CAPPOS: Possibly. Yeah, I think I said it -- I gave kind of a high-level perspective of it before, so it's probably easier. I did have one thing related to the way that risk is viewed in this that I wanted to bring up very quickly, that was brought up in the initial presentation, if that's okay. While I have the floor, I'll just say something quickly about this, which is I think that a discussion about is adding an updater going to add risk to a system. Well, anytime you add software to a system, you're adding potential attack surface.

And so really, I think the question is how do we make an updater that minimizes the overall risk of the product, because not having security patches for a product is also a risk. And so that, I think, has to be a fundamental way to think about it. And I think one of the really awesome things that was said earlier by Srinivas and the -- in his talk was this discussion about one size not fitting all, people might need to pick and choose things that are appropriate for their environment. So, I just wanted to kind of bring that up, that thinking about it as secure/insecure, vulnerable/invulnerable, whatever, is maybe not the right way to do it, but instead to think about what are the risks and what's the best payoff we're going to get for the work we do.

ALLAN FRIEDMAN: Thank you.

TIM HAHN: Allan, can you hear me?

ALLAN FRIEDMAN: Yes.

TIM HAHN: Yeah, this is Tim Hahn. I just wanted to reinforce that last comment. I very much agree with that. Also, with the comments made earlier about, you know, were certain things thought about, what about these issues, I think a lot of that comes out in, all right, when you pick a particular use case and you identify what you're going to do for that use case, then you need to do a threat assessment, threat analysis, risk assessment, evaluate all those risks and potential attacks in what you chose in that specific use case or deployment. This doesn't get to that level of detail, but you have to get to that level of detail to address what is being mentioned.

SHRINAF: Yeah. Yes, we started discussing on that particular topic, too. So, what we said is these kind of threat analysis and vulnerabilities and attacks and the kind of thing has been already addressed by so many standards and alliances already. That's why there is a list of what we thought was the organization targeted for review the standards catalogue. So, that comes from Industrial Internet Consortium, NIST, or Industry 4.0, all those organizations we listed here, there are already set of this threat model or maturity model, capability maturity model, all those things have been already there.

Moving forward, what we want to do is that's what we were discussing in the last when there may be -- depending upon the member's contribution and presence, we should be able to go through, review these things, and see is there a gap in those things so that we need to add something new. Otherwise, we can go ahead and adapt it. For example, IAC recently developed a security framework document which covers most of the things what we are talking, maturity model, different use cases and all that stuff. We can refer to those things and use that.

ALLAN FRIEDMAN: Thank you. And, in fact, a great segue into the second page of the document, which is additional components that might be relevant to use case. And that's something that the working group talked a lot about is there's the baseline, you really can't call something an update if it doesn't have the first page, and then there are going to be features that just -- if you are going to be demanded by context, to be accepted. And in terms of what the broader community thinks, how useful is this and how would you like to see -- would you like to see this embedded in more discussions of threats or is this fairly substantial, if we just put -- if the group puts this out as -- turns the table into a document, as a freestanding document, is that something that's going to be useful for the community by itself? Let me tell you, the working group has been trying to figure that out themselves.

JOHN BANGHART: So, I think, yes, it's useful. I think, at least for me, some use cases would also be helpful; right? So, you know, pick a couple of devices or whatever sort of ecosystem you want to choose, and then show how running through all of these different pieces, the first table and the second, and start making a little bit more concrete. I think there's plenty of folks in this industry that can look at this and sort of understand it, but I think there's a lot of folks who can't, you know, folks who may even be technical, working in the IoT manufacturing space, who may have never addressed something at this level of detail before. So, I think you need to have a little bit more instruction around here's what this means to this kind of device and the steps that would happen and why it's important; right? And we heard a couple of those pieces, but I think building that out some more would be helpful.

SHRINAF: [Inaudible]. That's what I was mentioning. Some of these use cases and all of those things have been done by other entities already, for example, Security Framework Group. I, myself, is creating all the set of use cases there. So, those things we can refer, bring it back here, and we can review these together, if possible.

ALLAN FRIEDMAN: Great. Any further thoughts on how this can be used? We've got the idea of having use cases around this idea. Yes?

JAMES SIMISTER: So, I'm James Simister from Panasonic. And one of the things that I was thinking about as I reviewed this list is the scalability. So, you know, one of the lines up there is transmit the updated code. That sounds really easy, but when you're talking about millions of devices in the field, there's a fair amount of infrastructure required to handle that. So, one of the things we've found is working towards having a nice scheduling capability to do that. And so I don't know if that needs to be discussed here or maybe that's too far into the details, but maybe as part of those use cases that we were talking about is to talk about what does this look like when we're dealing with millions of devices. How does that play out? What kind of infrastructure is required for that? And what is required from the device side so that they don't inundate the infrastructure all at once?

JUSTIN CAPPOS: So, I'll just say one really quick thing, which is Microsoft actually published some pretty useful information about how they do updates and how their infrastructure works. So, I'd be happy to point you to that offline, if you're curious. As for whether this belongs in the document or not, I could see that perhaps it wouldn't, except for as an example of "Hey, if you want to do this, then here's somewhere to look," but it doesn't -- if done correctly and if it's not a mechanism for people to indefinitely -- to have a man in the middle indefinitely deny you updates, then it seems like it's more of a, you know, performance-tuning bandwidth issue than a security one.

JOHN BANGHART: Sorry, Allan. One last thing, I promise. This is John Banghart. This, to me, seems like something that would be great for NIST to work on at some point. I mean, this is the kind of thing that NIST likes to do. And you could foresee NIST IR or something to that effect that starts to codify some of this. I think the community needs to work on it some more and refine it some more, but, ultimately, I think there's potential value there in that avenue as well.

ALLAN FRIEDMAN: Thank you. And, in fact, stakeholders have been citing things like 800-147, which is BIOS firmware updating. So, I think there's some engagement. And we know -- I see there's some NIST folks that have been tracking this project quite closely. Any further thoughts? Anyone on the phones want to chime in? All right. See, this is the joy is you just have it silent enough so that -- aha, see --

RALPH BROWN: Yeah, I felt pressured to say something. Just, again, this is Ralph Brown with CableLabs. Just an offer as a resource, CableLabs has been doing device security for well over 20 years. Every cable device that connects to cable has elements of security and secure software download. All of our specifications are publically available on our website. You're certainly welcome to reference any of that material in terms of code signing, download process, all those sorts of things. So, it's just a resource that we'd be happy to share.

ALLAN FRIEDMAN: Thank you. I appreciate that.

SHRINAF: Yes, I have seen that we also worked on [indiscernible] stuff kind of stuff. We have reference to the CableLabs spec, and we are part of it. We are aware of that. So, that's where we can add that to our list here.

ALLAN FRIEDMAN: And for those of you who are in the room and those of you who are watching the webcast, there is still plenty of work to be done in this working group, so I think afterwards please reach out. We'll add you to the working group list and we can roll up our sleeves and dive into the nitty-gritty. All right. So, I think, in terms of this working group, I want to personally thank everyone who's involved in that working group. We've got Shrinaf in the room, but a lot of people who are listening and watching who've been working very hard on weekly calls. So, thank you all so much. This has been a tough thing for folks to get their heads around. And this short presentation does not really show all of the work that went in to get us here. So, thank you all for those of you who were behind this.

Now we are going to hear from the Standards Working Group. We've got Matt. And Angela, can we open up Kent Landfield's line?

ANGELA: His line is open.

ALLAN FRIEDMAN: Great. Hi Kent.

KENT LANDFIELD: Hey, Allan. How you doing? Can you hear me?

ALLAN FRIEDMAN: We can indeed. Thank you. And we've got the slide up. And Matt is -- or would you prefer to be at the -- up here? We can get you here, and that way we can just get to have the slides in front of you. So, he'll just stand here. Use this mic; that might be a little easier.

MATT: So, this is a bit of a tag team effort. Kent couldn't make it today, so I raised my hand to be the person to present it, but Kent and I are going to kind of co-present. He's going to jump in and add color as needed. I'm going to try to do my best at doing -- giving a read out on what the group did. The group's done a lot. So, let's go forward. Perfect. Okay.

So, the update on what the group's been doing, the group got organized at the first kickoff meeting back in I think that was October. The scope of the group really is to kind of do a survey of the existing standards and best practices to identify what is being done in industry today to ensure that any work that's being done by this multi-stakeholder group isn't duplicative of what's already out there to avoid reinventing the wheel. And, you know, what we're looking at is we're trying to go through the various standards, best practices, and anything that companies may be doing to kind of identify how you're doing upgrading "patchability" so that we can identify patterns and kind of synthesize and figure out, you know, what's being done, and then also so that we can inform the group so that there's kind of a map or a catalogue of things so that when people in the IoT industry are looking, there's a place that they can start as opposed to having to do all this work themselves. Is there anything you want to add that I missed there, Kent?

KENT LANDFIELD: Yeah, you didn't miss anything there. The reality is that this is a very diverse environment. And we're finding consortium standards groups, we're finding small consensus groups that are working together to try to address this. In many cases, there's not a lot of detail. We'll get into that in a bit, but this is a very time-consuming effort to go through these documents and, first off, identify the organization that we should be targeting, but then go through these documents. So, what you're seeing here with the catalogues that were sent is part of this effort was really trying to sort of codify what we had found and what we were investigating so that other working group chairs and working groups could leverage that information.

MATT: So, on this slide, what we're showing, the group is not trying to boil the ocean, but, as you can see, there are a lot of standards out there. Anybody who's played in the standards space knows that there are a lot of standards. What we're also seeing is new standards groups that are trying to address the IoT space as well, so that's adding to the list.

So, what the group did is we first tried to identify the standards first. So, we've put together the big list. The group's gone through the ones on the left. We still have work to do on the ones on the right. So, we're still looking for some help, because, as Kent was just saying a moment ago, if you've ever looked at these things, you know, engineers can write and produce documents right up there with all the lawyers. So, we've done a good job at writing a lot of stuff. And when you go through these things, they're all different because every standards group kind of has a different style on how they put together their standards. So, as Kent was saying, going through these things takes a bit of work because you got to figure out where to look in it.

And we'll talk a little bit at the end about some of the observations, but what we've also found, and I think a lot of us knew going in, that there's no single section in any of these standards that will say, "Oh, this is how you do a software upgrade on a lot of these." There's some, and we're trying to pull those out to kind of -- as references and use cases and best practices to kind of zero in. There's some stuff in the broadband forum. I was talking to Ralph, I know in the CableLabs standards we also talked about some of that. So, you have to kind of go through all these things.

Typically, there would be a piece of -- will talk about kind of what is the capability. Then you have to go find something in the security section that will link it to how you do it securely is often how it's done. So, it's a big job. And what we're trying to do is go through and zero in and put in a catalogue to specific pieces so that others who come behind us can come in and they know exactly where to go look. If you've gone, say, and looked in the 3GPP specs, you can spend weeks trying to find what you're looking for, and you might be in the wrong version, because they're on what, version 11, 12, somewhere up there, and you'll be, like, in the wrong space totally. So, it's a lot of work. Anything else there Kent?

KENT LANDFIELD: Yeah, the one thing that's sort of different from this effort in the IoT space is that it's very different in the standards perspective. In many cases, in the past, you have standards development organizations or standards-setting organizations that are there for creating "real" standards, either national or international standards. In this space, there is an extremely large amount of consortium and industry alliance work that's going on.

And so, in some of these cases, they're not really standards as you consider standards from an ISO or an ITSO or a SCO [ph] perspective. They're consensus standards that the association is or the industry alliance is using and focusing on for its members. So, it's important that we look past just some of the other areas. As you can see, a lot of these really aren't standards development organizations officially, but they are consortium groups that are working together to address some of the same issues we're trying to address.

One thing I should note on this slide, when this was sent, I don't think the broadband forum was on there. Since the efforts -- since the documents have gone out, we have had three different other efforts request participation. So, that's a positive from our perspective. And they'll be added to the research pending this. It's always easier when we have folks from within those organizations assisting us. It makes it much quicker when we can get right to what we need, as opposed to the gumshoe kind of approach that we've had to go through in digging this stuff out. Matt.

MATT: Great. Yes, hopefully we'll get some other people to step up and help, too. So a couple things, so we're still kind of zeroing in what we want to deliver. But I think kind of what we think we want to do is the first one, is we're putting together what we're calling a "catalog," where we're kind of, as I said, collecting all the things that we've already pulled together, make it an easy to read, kind of zero in on the different places of what is the section in the specific specification, standard, best practice, or consensus document that you are referencing so that you can go find it easy. We have something in a draft form that we've been using to work off of.

The second thing kind of is an internal document for this stakeholder group. We are looking to put together, potentially, something that will capture the observations that we've seen so far to help inform the other working groups going forward so that they can use that as well, so maybe kind of like a crib-notes version of everything that we're discovered. So, that's kind of what we've laid out. And I'll show you on the next slide kind of what the catalog contains. But let Kent jump in here as well.

KENT LANDFIELD: No, I think you did a good job there. Thanks.

MATT: Okay. So, I've signed up to write this thing; right? So, just real quick, this is kind of what we're capturing in there, so you can kind of see. The kind of key thing in my mind is we were capturing what is the useful section and kind of where to go find these things. Sometimes these things can be a little difficult to find, and so we're trying to make it easy to just zero right in. I think one of the takeaways for me that when you look at this, is that you will see some design patterns that start to emerge across some of these. There's a lot of common things that are done to kind of spell them out a little different. But if you kind of look at them at a little more macro level or you kind of blur your eyes, they start to all kind of look similar. So you see lots of things. And I think what we're -- and I know Kent will say a few things on this one as well.

But one of the things when Kent and I were talking earlier this week about this whole thing is what we're seeing is that there's a lot of things that have been done historically in the software industry that are now -- that are applicable in the IoT space. So, there's a lot of best practices you can just carry forward if we can kind of make sure everybody's aware of what those are. There's a lot of lessons learned. I think those of us who have some scars from over the years of doing this know how to do these things better from just the pain and anguish of doing it wrong. So, if we can not do it wrong again it would be helpful. I think everybody would be better off.

But one of the other observations -- and if you've played in this specs and standards, you'd probably know the standards in this case aren't all that, I would say they don't provide necessarily a cookbook or a recipe for exactly how to do this. It isn't like an "instructable" on the Internet to go look up, oh, this is how I've got to do it. They're often a lot more descriptive and not prescriptive. And so, you know, even though it will talk about the capabilities, it won't tell you exactly how to do some of these things that we've been talking in the room on how you make it necessarily scalable. It may not be spelled out in the standard. It will just say that you should be able to do software update. Just assume that you can make it scalable and you're thinking ahead.

And what else? Yeah, so -- and if you want to add anything there, Kent.

KENT LANDFIELD: Yeah. The real focus is that what we're seeing is a lot of these standards aren't really -- a lot of these documents aren't really focusing on specific show and tell. In other words, how to do it precisely. And those that do, like, for example, the IEC documents, 62443-2, have some very specific things for a specific industry. In this case industrial automation and control systems. So, we're finding that there are some relevant capabilities documented out there. But most of them, from what we've seen, mirror what software vendors have been doing over the years. The software industry has been discovering and stumbling over these processes for years and years, as Justin mentioned. It's very accurate. There's been a great deal learned from what they have done in trying to step past the mistakes of the past and step into the future.

The real question is, in a lot of these that we have gone through, it seems the "IoT" space is focusing very much on best practices that are existing vendor practices from the software industry. So, one of the questions is, is there really a difference between the techniques and processes of today for the software industry, versus what IoT is going to be requiring in the future. And if so, maybe what we should be doing is trying to address really what that gap is, what those differences are, so that then we can really inform vendors and manufacturers alike.

MATT: Okay. And with that, I think we're kind at the -- a couple things, A, I think Kent and I would like a call for help. There's plenty of work to do, and so if you want to help, we have a mailing list on the Google Groups. We also have a Google Docs Drive so that it's all easy to get there when Google Docs is working. So, and with that, questions, comments, discussion.

ALLAN FRIEDMAN: Good. I see a couple questions in here. Let's go with Craig and then John.

CRAIG SPIEZLE: Craig Spiezle, Online Trust Alliance Internet Society. I think this is good. A few comments I want to make, and I think Kent made a point here, is not to call all these standards. Standards have a very specific term meaning here.

The second thing, and I have participated a little bit on the group here, I would segment this out and maybe even think of a grid. Some of the activities listed here are very, very focused. Some of them, for example, interoperability, technical standards, how devices are going to communicate with each other.

Others are very much core security. Others, like our framework, includes also privacy. And I think even though the scope of this effort is patching, I think to really provide as much utility it would be really good to perhaps flag or have a grid of kind of like what are these frameworks, what do these include.

And there's another part of this is there's three dimension to IoT. It's not a one-size-fits all. It's the physical device. How I am going to patch my device? How am I going to patch my mobile app that it works with and/or the cloud service behind it? And the reason I point that out is, dependent upon this list here, some of them are looking at all three. Some of them are only looking at one. So I think, again, visually that would be very helpful. You could go down and you could identify those areas. So, again, I think that would help take it to another layer to make it more useful of what's out there.

KENT LANDFIELD: Yeah, Craig, I totally agree. One of the things that, you know, shortfall in the document as it exists today is that we really haven't classified these into industry alliances or SDOs. We haven't done any real classification as to the applicability to any or all parts of the IoT space that needs to be addressed, and I think we do need to do that.

JUSTIN CAPPOS: Okay. So, Justin Cappos again. So, like, one thing I'll give offline is I'm happy to give you a few other standards documents that are very update-focused and very specific about that, and that's, like, the whole purpose of the standard, is to have this, you know, massive discussion of how to do update security.

And then I'm sorry, I didn't catch the name of the gentleman who is calling in over the phone, but I thought he had a really nice question that he kind of ended with, which was the question of, well, what is different from traditional software update infrastructures. And since, you know, I've worked a lot in that space, and kind of more recently came to the automotive space and tried to understand it from that context, we've been trying to understand not what only what is different, you know, from the server space to IoT, but also what's different from the automotive space to other things in IoT. And we've come up with a couple things that I'll kind of quickly say something about, but then could have a broader discussion. I don't know what the right area is.

But some of the things that we've seen that's quite a bit different is that it seems in the IoT space there seems to be a general consensus that everyone wants to be on the master or latest release of software that comes out. And while that's true with some things like, you know, Chrome and other software that you have that will automatically update itself, it's very frequent that people will intentionally, like, pick and choose what software they update for their Linux distribution, for the different packages and their environment and systems. So that's one difference that I believe is fairly pervasive across the IoT space. And I'd love to have people come in after I'm done saying my list and tell me that I'm wrong. Please tell me I'm wrong if there's things I don't know.

In general, in the IoT space it's not very important to coordinate updates between different devices, because usually devices you have in the home probably come from different vendors, and so you don't think of updating them as a collection, where a lot of times in traditional servers you do this. Certainly within a car you need all the components of your vehicle to be able to talk to each other so that your brakes still work after you do your update. So, that's another area that we saw was a bit different.

There's also this question of who decides when devices update. And this was brought up earlier on. It was, like, a passing point of the consumer making this decision. But one thing that does happen in a lot of other contexts is that manufacturers will go and be the ones who decide they want -- when you buy their device, you're also getting updates. We're going to fix security patches in your device for you. And I think that that model is a model that is something that perhaps should be recommended in the case where you have an inattentive home user. If you have the informed attentive home user, who does want to manage their updates and do things, I can see the wisdom of wanting them to do that. But I think it's, from a risk standpoint, thinking about what would be worse overall for the security of the user, I think forcing every user to have to be an informed and attentive user is a recipe for disaster.

The devices have very different capabilities, the weakest to the strongest device. This was brought up very nicely before by Shrinaf. He mentioned that there's such a wide array of difference that some devices might not be able to do things like even check signatures or do other operations like that. And the final difference I have here on my little cheat sheet is it has to do a little bit with how you do updates and what the delivery mechanism is actually makes a very big difference, because, at least in some Internet-of-Things environments, you're going to have a master-slave sort of relationship, where you have a very, very weak device that is just sort of a dumb device that gets directly programmed. And while there are some parallels with this, where, you know, for instance your Smartphone, you have things like the cellular chip and other things in there that you go and you directly apply firmware to, and there may not be the same level of verification that happens for the OS packages because it's stored separately. There is, I think, quite a broader range of differences for how people do this in IoT devices that doesn't commonly show up in desktop or other types of environments.

ALLAN FRIEDMAN: Wow. [Inaudible]. Dan.

DAN CAPRIO: Thank, Allen. Dan Caprio of the Providence Group. I've been involved a little bit with this group, so I just want to point out there's an effort that's beginning, it's underway, but I think officially beginning tomorrow on the civil society side, led by the Center for Democracy and Technology. And they're beginning to look at some of the same issues and some of the same frameworks. So, we ought to make sure that we're plugged in to what CDT is doing and that we're all aligned and not reinventing the wheel. So, I'm happy to help with that.

ALLAN FRIEDMAN: Thank you.

CRAIG SPIEZLE: Dan, that's exactly what I was referring to without disclosing that. But agree.

DAN CAPRIO: I misunderstood, Craig.

CRAIG SPIEZLE: No, when I made my comment about -- the earlier comment about segmenting and such things, that level of detail is very specific; for example, consumer notice, consumer choice very much in a checkbox what framework has that. So, it goes into a much greater level of, effectively what are the principles within it, the FIPS in a sense, in that area, and so I think it's going to be a very helpful document.

DAN CAPRIO: Good.

ALLAN FRIEDMAN: Thoughts, in particular about this sort of difference between software and connected devices? Kent, do you have thoughts on this?

KENT LANDFIELD: Well, just a quick point. Joseph has reached out to us and, in fact, actually contributed entry to the catalog as well, just as a heads up. So there is communication going on.

ALLAN FRIEDMAN: Thanks. And I have apologize. Justin, I keep saying your name wrong. Make sure we get it right. On the phone we have Jim Mann.

JIM MANN: I had originally chimed in to talk about one of the groups I think was missing on a slide that I saw, which is Trusted Computing Group. They have an IoT workgroup that's active right now and actually looking at some of the updates, you know, best practices and so forth. And so I think it would be good to add that in there as well.

And I also wanted to respond to Justin's comments about the updates and customers. I think he was talk about customer control of updates. And certainly in the traditional IT space, you know, PCs and servers and so forth, we have commercial customers who definitely want to control if and when they take something like a BIOS update; right? In a consumer space less so. But I think certainly when you start talk about industrial or commercial IoT space I think we're going to want to see that kind of control over when they take a particular update so they don't impact their operations.

JUSTIN CAPPOS: Great. I agree.

ALLAN FRIEDMAN: He's nodding. And I think one of the things we talked about at the initial meeting that kicked off this even was how to scope this around IoT, and I don't think there was a very clear consensus around, say, limiting it to very particular sets of devices or applying it to everything. I think there's strong cases in both directions. One dividing line that might be useful is is it centrally administered or not, because there are things that are slightly industrial but still will be fairly autonomous in their administration. And there are going to be things that look consumer but they're going to be in a context where there's going to be a third-party organized administration power.

Anyone have some great organizations that we should be adding to this list, or folks that we should be reaching out to who can point us to people who are engaged in this list?

MATT: Ralph's got his hand up.

ALLAN FRIEDMAN: Ralph.

RALPH BROWN: Yeah, this is Ralph Brown with CableLabs. Just saying, again, CableLabs probably should be on this list. With respect to the observation that most of these organizations don't provide a cookbook or detailed specification for how software updates should take place, case of CableLabs, our specifications are very detailed, precisely what needs to be done, what needs to be implemented. And, in fact, we test and certify devices in compliance with their specifications. So, in fact, we are assured that the devices, when they go in the field, actually implement the secure software download process as we've identified. So, it's specified.

KENT LANDFIELD: We definitely want to add those to the catalog, no question.

ALLAN FRIEDMAN: All right. Craig.

CRAIG SPIEZLE: Yeah. There's been a few comments about some of them haven't been extremely prescriptive, and I can say that for our framework that was by design. It was principal oriented so that they're evergreen. The challenges, if we're very specific, on how to do something today, the document will be out-of-date next week. And so, I mean, that's a fundamental discussion of is that good or bad. But, again, principal-oriented, for example -- I'm going to just make this up randomly -- the patch should be encrypted or secured by current standards and protocols, but not specific. And that's by design. And then it can point to others. So, I wouldn't necessarily throw out any of them that don't have that level of specificity on that.

RALPH BROWN: Yeah, I would agree with that. I think our -- in our history, we've evolved what we've done in terms of our specifications. We've been through six generations of cable modem specifications. And every time we have increased and kept pace with what were the best practices of the security, you know, practices. Over time, we've also looked at -- you know, we operate a PKI to support that, and we've had to learn how to evolve the PKI and how we manage and operate it to, again, follow best practices for that. So, you're right, it's something that has to evolve and will continue to evolve, but so being overly prescriptive is probably problematic.

ALLAN FRIEDMAN: We got Dan in the room and then Jason on the phone, and then Jamie.

DAN CAPRIO: Thanks. It also occurred to me -- I was in Brussels last week, working with the European Commission on the Internet of Things. And the Europeans, about a year-and-a-half, two years ago, have launched what they call the Alliance for the Internet of Things. And they've done an awful lot of similar work. So, again, I'm kind of raising my hand to volunteer for this, but we need to be continuing the transatlantic and the global engagement, but making sure that we're capturing similar efforts that are taking place in Europe.

ALLAN FRIEDMAN: Thank you. That's really helpful. And I should also add that when our colleagues -- our government colleagues from around the world come to the United States, IoT security is something that they're interested in talking about, and they're very interested in the work that all of you are doing. So, I think if we can demonstrate this is a successful project, it is a chance to sort of help influence a lot of these discussions. Jason on the phone.

JASON WALLS: Yes, this is Jason Walls from QA Café. I work with Broadband Forum. And the discussion has kind of moved from what I was originally going to say, so I have a slight list. First was definitely with the list that Justin is making, I just want to reiterate that it would be great to get him involved, to kind of get that information.

One of the other things, there is a difference that I think, you know, that can benefit from standardization or at least input from standardization bi-directionally is that a lot of the devices are going to be proxies; right? So, there's going to be the thing that is, you know, controlling their updates might -- they might not be directly communicating with it. You know, it might be being done by some other intermediary hub or other, you know, kind of smart hub situation. And yeah, I just wanted to reiterate about the "prescriptivity."

Obviously, if you haven't had a look at Broadband Forum's stuff yet, that's sort of the line that we've been going down very specifically. And just like, you know, like Ralph said, the service provider and MSO and cable communities have been dealing with this exact situation when it comes to sort of bigger things like home gateways and, you know, in their case, e-routers and cable modems and such. And so the similarity -- we're asking about, you know, are we just trying to get the best practices from software, you know, it's the best practices from the people who have been doing, you know -- and device updates and device security that I think would be helpful.

ALLAN FRIDMAN: Thanks. Jamie.

JAMIE BROWN: Hi. So, I'm Jamie Brown with CA Technologies, bringing it back to the software side. We're members of an organization called SAFECode, which is an organization made up of several software, and beyond that now, other types of organizations that promote secure development. SAFECode has a number of technical guidance documents on patching, on secure development that we think would be appropriate here, and they recognize, I know that the board members and the leadership there, sort of the overarching importance of IoT, and I think are starting to guide a lot of the documents in that direction. So, I would be happy to put the working group leaders in touch with SAFECode leadership to see if we could get those added as appropriate.

ALLAN FRIEDMAN: Craig.

CRAIG SPIEZLE: I want to just reiterate Dan's comment about the global aspect. It's not only what they're doing in Europe I think that's very important, but when we think about the rest of the world's view on data security and privacy, that the regulatory landscape and the norms in Europe are much different. And so we need to be thinking globally in what's appropriate in all of these areas here. And we've talked about that before in many of the working groups on IoT privacy, transferability of the data, and ownership of the data and such. So, I think that's just an important part that we not lose sight of. There was an interesting article yesterday in the Wall Street Journal that talked about how companies in the U.S. are now focusing on GDPR because they expect that to be the norm for the U.S. So, just thoughts on that aspect there.

ALLEN FRIEDMAN: I don't want to sort of fork this conversation to a GDPR discussion, if at all possible, but is there any response on that? So, in terms of next steps, Matt?

MATT: Next steps, I think we're looking for more help and I think we're going to -- I know we're going to continue to build out that catalog, and I think we got a few more volunteers to go with some of the specs to help us flesh it out. And I don't know what else we have planned, Kent.

KENT LANDFIELD: Yeah, no, I think this has been very helpful both from the standpoint of access as well as potential volunteers. But over the last few days, since this has gone out, we have received, like I said, additional input to the catalog, which is very much appreciated and we'll look forward to being able to add those that were referenced here. Thanks.

ALLAN FRIEDMAN: Question for Kent and Matt, in terms of sort of the documents that you're going to be producing, could you tell us a little bit about what that might look like and what the target audiences of that would be? How do you see -- where are you aiming this?

KENT LANDFIELD: Well, that's a good question, and that's one that I think we need to have a discussion around. Internally, we've had a discussion that the document was really sort of an outgrowth of our research. We didn't want a whole bunch of people going after the same groups, so we initially used it as a means to sort of self-de-conflict, so to speak, some of the research. There's a lot of research to be done here. We don't need people wasting time doing something that someone else has already done.

In the process of doing that, we have, in essence, been able to create this beginning catalog, so to speak, as to the efforts that are out there, some of the documents that are out there, as well as we're, you know, using this as a means to sort of get to the point where we can communicate to the other working group leads as to what documents they may find most useful for their efforts. The question is, this is taking a good deal of time from our standpoint to do all of this research, and as we, you know, today learned, there's probably another five or six different resources that we need to add to the emerging research side.

So, it depends on what we're trying to accomplish, and that's part of the discussion I think we have to have. This was initially done to make sure we weren't reinventing the wheel in what we produced. At this point, I think this is something that could be very useful internally, but I think also, because of the amount of work that it's taken us to get here, and it has been substantial, that this could be beneficial as a point and time reference for others who were either involved with this effort or were not involved with this effort to be able to use, but I'm not sure what forum it would be published in directly. That's something we can discuss.

ALLAN FRIEDMAN: Excellent. Shrinaf.

SHRINAF: Yeah, the similar effort has been made by the Smart Grid Interoperability Panel, SGIP. They created kind of a set of -- a catalog of standards. They have gone through most of -- some of the list whatever we are seeing here, they have gone through all the list standards and they have created a kind of a catalog. So, if we can refer to that -- of course, some of the new things are there -- we can follow the format of that particular catalog where they say, okay, these are the highlight point of this one, these are applicable to us, and there is a gap. So, if we can identify those things and put it in our whatever the document we are talking, that would be helpful to all this, I think.

ALLAN FRIEDMAN: Is that catalog public?

SHRINAF: I think it's on the SGIP website. I am -- I can check and refer that back to you.

ALLAN FRIEDMAN: We'll connect with you because that could be a very rich data source for the working group. More standards to read through.

MATT: I think there's a couple things. There's a gap analysis that comes out of that, that has been mentioned. I think mapping it potentially into a framework, as mentioned, for the IoT might beneficial, and then potentially even looking at what are the common design patterns across all of these so that you can kind of summarize it so that somebody can do a quick read and figure it out, and then drill down as they need to go.

SHRINAF: Yep.

ALLAN FRIEDMAN: I agree. I think this is -- the work you're doing is going to be of tremendous value, not just to this initiative but it's going to be, I think, foundational for private efforts. And, of course, I've been talking with some of our government colleagues about the importance of -- this is knowledge that would be really useful. Say we can say, hey, NTIA's stakeholders, they're doing the work and we'll have to -- that means we get to loop you guys in all those discussions.

MATT: Right. So, it sounds like we gave ourselves a bunch of homework assignments.

ALLAN FRIEDMAN: And we will make sure that when the notes go out, that we have a very explicit call for making sure we have the full range of standards, but also calls for volunteers for people to analyze and do some of the work on that.

MATT: I did see a lot of hands going up that want to volunteer, so that's good. Great

ALLAN FRIEDMAN: Thank you, Matt. Kent, any last words?

KENT LANDFIELD: No, other than I'm sorry I wasn't able to be there today. I would much rather be there in person than on the phone.

ALLAN FRIEDMAN: Thank you. So, any last comments on the standards question? All right. We are slightly ahead of schedule, which is always good news. So, now we have the third working group. We're going to pivot from the primarily tech focus to both the technical aspect but also the policy and usability side on the consumer focus. And we've got Harley. Do we have this loaded? No. So, if you haven't -- give it -- if you haven't loaded it, then you just want to use your machine. Yeah, let's just -- probably just -- we will see if it is actually easier to do a hotspot. I once saw four tenured professors, two of which had [indiscernible], try to connect a laptop to a projector.

So, while Harley is setting this up, after this discussion, we'll have lunch break, and then we'll return to the final working group, and then we'll talk about some of the big picture of where we're all going.

HARLEY GEIGER: Good morning everybody. So, I represent the Communicating Upgradability and Improving Transparency Working Group. And what I'm about to present to you is a consensus document from that working group. And I want to emphasize that this is a product of the working group. We have roughly 25 members, including technologists, engineers, lawyers, and public policy specialists from private companies as well as civil society. And I want to especially call out and thank my co-chairs, Aaron Kleiner from Microsoft, Beau Woods from the Atlantic Council, who were not able to make it today; and also Megan Brown from Wiley Rein and Craig Spiezle from OTA for exceptional participation, but this was a group effort and a lot of folks participated.

So, the first thing that we did was come up with a problem statement. What is it that we are trying to solve as a working group? And our problem statement was essentially that consumers have difficulty assessing the security of a particular IoT device without manufacturer communication. And this is, of course, as it relates just to updates. And then we came up with a mandate for the group, a mission, how will we address this problem. And we focused on what information manufacturers should communicate to consumers about IoT security updates. And we did this really before we got started on the elements that I'll be presenting. And we reached consensus on this as our mission. And honestly we kept a militant focus just on this mandate. There was, at various times, a desire to perhaps talk about other IoT security issues, segmentation or privacy. And these are absolutely important issues, but they were not within the specific mandate that we were trying to fulfill. And so we did not address them.

Now, in previous multi-stakeholder processes, issues of voluntariness or whether the documents relate to legal standards, these were discussed at agonizing length. And we wanted, and the lawyers in our group especially wanted, this to be crystal clear about what the document was and what the document was not. So, it is just the output of the multi-stakeholder process. And the output of our working group specifically does not describe or supersede any regulation, domestic or international, and it is not intended to create a legal standard of care or future legislation or statutory obligation. And we put that right up on top in footnote one to dispel the preliminary terrors.

Now, in addition, for the prevention of bewilderment and heartache, we also included important context in the intro and scope. By the way, if you haven't noticed, on the bottom right-hand corner there are the page numbers. These follow along with the document that we have a hard copy out there, if you don't have a copy. It will be helpful because we're going to go through the elements. But, so in the intro and scope, we put important context, such as that IoT methods, capabilities, deployments vary widely. They're incredibly diverse. And this is not intended to recommend exact language that manufacturers must use or specific vehicles. It's not -- we mentioned a box label or a website, but manufacturers will have to choose the communications vehicle that is right for their own deployment and their customer needs.

And we also wanted to make sure that folks that are reading the document don't get the impression that security updates are the silver bullet for IoT security; they are not. And that we acknowledge that it is just one security measure, it does not offer complete protection. And then we also included some of the stuff that our working group, as a whole, reviews. So, we looked at existing standards, some of the things that FTC, DHS have already said. We drew on our own experience as members of companies or civil society, as well as our personal opinions in coming up with the list. I would also point out, just if you're reading the document, to note throughout the document the use -- the careful use of words like "could" or "may" or "consider," because there was a big effort to be gentle, to make recommendations without being too prescriptive.

And so this is the real meat of the document, starting on page two. These are the elements that we suggest manufacturers communicate to consumers. And this section notes, it reiterates that the communications are voluntary, that the elements can be communicated in a variety of ways, box label, website, et cetera; and that the communications can change, will likely change over time to match the evolving technology, evolving threats, and consumer expectations.

And in drafting these elements, as you can see here, we wanted to -- there was an effort to prioritize some elements over others. Some of them were more fundamental, we thought, to the issue of IoT security updatability than others. And so we broke them out into two categories, with a temporal factor, which is important. You know, the key fundamental elements are ones that should be communicated to consumers prior to purchase. I shouldn't say "should." Could be communicated to consumers prior to purchase. Manufacturers should consider communicating to consumers prior to purchase.

And then additional elements that could be communicated before or after purchase, and an example of a post-purchase communication would be an instruction manual. And part of this is not just one being more fundamental than the other. Some of this is also trying to account for different levels of expertise and savvy among consumers because some of the additional elements may be things that somebody who's very technically savvy would really care about but is not necessarily very fundamental to a broad range of consumers.

Now, there are six elements in total, three of each -- three key elements, three additional elements. I'm going to go through them one by one and then, at the end, I'll have a slide that has all of them together so we can review them. So, this is the first of the key elements. It's the most fundamental, of course. Can the device, as a technical matter, receive security updates? And this can appear as a simple statement. It can appear as a check box, yes or no.

And the second key element, a summary description of how the device receives updates. And part of the point of this is to give the consumer some sort of an indication about what level of effort, what kind of commitment does the consumer need to anticipate in buying the device. Are the updates automatic? Is there a manual option? Will you have to pay a mechanics fee or some extra fee in order to get security updates? These are the things that you don't want to find out after you've already bought the device and you find out I have to go to a specialized mechanic who will charge me a fee every time that I want an update.

And this is the last of the three key elements, when does security support end? And so a specific date is preferable because a range, like one year, will not necessarily account for the amount of time that a device sits on a shelf. And it can be unknown. It can be indefinite, in which case we recommend that manufacturers consider communicating that to consumers. We don't know when it's going to end or it's indefinite, or a manufacturer perhaps will provide critical updates but not necessarily routine updates. So, that's the last key element which manufacturers should consider communicating prior to purchase.

And now we're on the second category of additional elements that can be communicated before or after purchase. And these are deemphasized deliberately because we don't consider them to be quite as fundamental as the key elements. So, the first additional element, how is the user supposed to know when there is an update? Is there a proactive indication or does it take some sort of user action to find out that an update is available? And this can be combined with A2 which was the "How does the device receive updates." However, we thought that this particular component of how the device receives updates was important enough to be called out sort of on its own here in the additional elements.

The second additional element, what happens when the device no longer receives an update? So, when the lightbulb reaches its end of security support, does it continue to emit light; right? Can you still control it with your phone? Does it lose functionality? Is there an official means for users to continue to receive updates, perhaps an extended subscription fee, or does the user simply continue to operate an un-updated device or unsupported device at their own risk?

And then the last of the three additional elements, how does the manufacturer secure the updates? Is there a way of verifying the source of the updates? Is the update tested to make sure that it preserves functionality with other devices or that it doesn't create new security problems? And here we call out specifically that the manufacturer maybe doesn't describe at great length how the device is -- the devices updates are secured. The manufacturer can also reference the standards. So, the devices are secured or the updates are secured, compliant with X standard.

So, those are the six principles, the six elements. And we'll look at them all in a moment, but first I wanted to call out a potential additional work, and these are examples of communications on IoT security updatability. And we tried this. We tried to find examples that are currently being used in the wild by other companies. And we really didn't find anything that was on point enough, which we take to be a good sign actually, that despite the sort of numbing plethora of standards that are out there, this still fills a gap.

So, we couldn't find anything there. And then we tried some theoretical examples, just ones that we made up, like how would the key elements look perhaps on a box label. But we also thought that this might distract from the content. So, really, we only had one and then one that was pretty abstract. And so it's a potential area of work. This could go in a number of different directions. Perhaps we will just come up and spend a lot of time coming up with different theoretical examples, or what would be really awesome is if we could get a company to work with us on perhaps applying these principles to a product or several products, and then we can use those real-life examples. That would be great.

So, here is the review of the elements that our group reached consensus on. And now I'd like to open it up for QA, for feedback. So, we'd ultimately love to have this as a -- to reach consensus on these and on the document itself from the larger multi-stakeholder body, not just from the working group. So, let us know what you think, either now or later, please.

CRAIG SPIEZLE: I think it was great work of the group. And I just kind of want to kind of give a few caveats. These may seem very broad, but, by design, they would -- you know, because they need to be, how you do it, provide appropriate notice to these can be very limited. For example, on a fitness tracker, you know, you have -- well, your constrain on the box size versus a 65-inch TV. We went through a lot of those scenarios.

I think one point that I feel is very important, though, and I know there's some debate with the FTC, is notice should be on first use. And I have been very opinionated that if you buy a TV, you haul it up to your home, you mount it on the wall, and when you turn it on that should not be the time you find out that, by the way, patching costs extra or we don't support it in there. And so I think it's very important that this notification be transparent and easily accessible for a user prior to product acquisition. And that was one of the points that we, I think, pointed out to.

I think the second thing is, ideally, these are minimum. We want to see companies compete on these areas. And really -- and, you know, a company might say, you know, we're committed to five years of support, or ten years of support, and that's great, but, again, we're not -- we'll be very careful not to say what that period is. So, I think it's an opportunity for companies to really differentiate their product and compete on privacy and security. So, thank you for your work and leadership on the committee.

RALPH BROWN: Yeah, this is Ralph again. I think -- yeah, I agree, this is really important work. And I appreciate the difficulties in terms of crafting these kinds of, you know, outlines or suggestions. One thing that I think comes back to the question of scope for this particular effort is we acknowledge that, you know, security patches and updates is one piece of the bigger pictures. And so while this talks to that piece, there's a question about does that convey to the consumer more than it actually means; right? Does it give them a false sense of security, because you may get security patches, but your, you know, privacy is totally wide open, or something like that; right? So, is there something that should be added to this or is some way to think about how this is -- how this is caveated, for lack of a better term, to indicate what is actually conveyed by this?

HARLEY GEIGER: So, the document itself does note, of course, that this is just one narrow slice of sort of the range of security issues and privacy issues that are attended to IoT. And, I mean, we also thought that something like privacy or segmentation, encryption, et cetera, that these are not necessarily within scope of a multi-stakeholder process on updatability. Now, if what you're saying is that manufacturer -- that we should build into the elements an instruction to manufacturers that they should communicate to consumers on privacy, we thought that that was out of scope.

RALPH BROWN: Maybe less that than, you know, companies should give consideration to either explaining other security aspects that they provide or stating that this addresses this specific narrow topic. Because you are define -- by fact of saying "This is our scope, we're leaving all of that out," you leave all of that subject to interpretation by the consumer. And it would seem that you would want manufacturers to have some statement about that is out of scope and we're not -- we don't address it, or we do address it in this way. So, I don't know -- again, I don't -- not being a lawyer -- know exactly what language you would want to use, but it seems to me that there should be guidance to manufacturers to be explicit around that.

HARLEY GEIGER: First of all, I would strongly urge against using legal language in a label like that. And perhaps the CDT -- the gentleman has left -- but the CDT process will cover this, but we wanted to be very careful not to tell manufacturers what they should or should not say. You know, we're not going to say tell them "You should communicate to consumers an additional statement about privacy," because then, if you're telling them you should communicate something about privacy, then you start to get into what should they say about privacy and which issues should they cover, and we did not want to deviate from our scope.

RALPH BROWN: So, what do you tell the consumer that you say, "Hey, this was giving me security updates and my privacy is exposed"?

HARLEY GEIGER: Craig.

CRAIG SPIEZLE: Well, again, it was a scope of by definition set forth by NTIA. This is about patching and supportability. The Online Trust Alliance, we create a very specific framework that has 37 principles that outlines a very specific set of what's required. So, again, that's outside of scope of what NTIA is doing, but there's other efforts that we think that are minimum requirements of disclosures of transparency to address privacy, ownership, transferability, as well as security and patching. So, again, outside the scope of what's in this room, as I understood it, and Allan will correct me if I'm wrong.

HARLEY GEIGER: We also did -- we did, though, reference a few standards, OTAs and I think at least one or two more in the document saying -- in our intro and scope, we mentioned, you know, call it explicitly, that other issues are not necessarily discussed, except for security updatability. We did say that information on these sources can be drawn from, for example, the OTA framework and I think at least a couple of others. You know, so manufacture -- I mean, that's going to be up to the manufacturers. And I almost think that that's a separate process.

ALLAN FRIEDMAN: Go ahead.

JUSTIN CAPPOS: Yeah, so I have a couple points. So, I really like this. I think this is really good work. I really like this document. I should say that up front. I wonder if this is very, very briefly almost touched on in A.2, but I feel it isn't called out strongly enough is I think having some communication about the expected delivery mechanism, and in particular things like the size of updates and what this means is very important. Microsoft has gotten a lot of flak from consumers, especially those who pay for their bandwidth, due to the large update sizes for Windows 10, and they're not unique in that regard. So, I think this is something consumers care about in a lot of context, and I think it would be a nice addition. And then --

HARLEY GEIGER: Let me ask your opinion. So, do you think that that belongs in A2, do you think that it's fundamental enough that it's something that consumers should know, like, is it as fundamental as manual or automatic or whether there's a fee? Is it something they should know before purchase, or do you think this is an additional element?

JUSTIN CAPPOS: Yeah, effectively, I think it's a fee, but it's a fee of a different type. And I think it's something that belongs in an A number, and I don't know if it -- I don't think it belongs in -- it could belong in A2, in fact, when I originally read A2, just the title, that's what I thought you were going to be talking about. But, here, what you're really talking about is almost entirely what does the user have to do to receive security updates, not how does the device itself receive, like, what's the mechanical process between its receipt of the updates. So, if -- you know, if I were tempted to do it, I would probably just break them out into separate points. But I think they're both A points.

HARLEY GEIGER: And is there a way of distinguishing, do you think -- and I'm sorry for focusing on this, but you're right there. Is there a way of distinguishing updates that are large enough that the problem, like, do you call them significantly large updates or is there a generally accepted size limit where it's like, wow, now this starts to eat up a lot of memory?

JUSTIN CAPPOS: So, it -- yeah, it really depends, because it can vary a lot, even for a device, depending on some devices, when they do differential updates, are very small; some switch from full updates to differential updates over a period of time. So, I think that what a consumer considers to be costly isn't actually necessarily -- but trying to focus on that, isn't necessarily exactly dependent on -- it's dependent on things that are outside of your knowledge and control in part because the same -- like, I don't pay per byte for my Internet access, but if I had an ISP in certain parts of Europe, I would be paying for that. So, for me, the fact that Windows, you know, drains all my bandwidth and stuff like that whenever it's going to do an update for quite an extended period of time is not as big of a concern for me, whereas, for other people, it would be.

And perhaps also there's things with, you know, if it's done -- you often don't want to do software installation or updates or watch things over your cellular connection. You'd rather wait, if you're on your phone, until you're on Wi-Fi to do things because otherwise, you know, you have a data cap. So, it really depends a lot on the exact set up that a user is going to have. And you might not be able to tell those things up front. The user may be the only one who knows.

HARLEY GEIGER: I also note that this would probably get us outside the realm of security updates, right, because they're bundled into a lot of other things?

JUSTIN CAPPOS: Yeah, I think it's along the lines of what -- you could sort of argue that it's a cost, like it's a denial of service style, like a cost-based attack that's being, you know, in some ways, launched by this device that the users let on their network. So, it is something the user is not expecting. It is something that a manufacturer is causing to have happen, but it wasn't an outside party. It was perhaps poor design.

ALLEN FRIEDMAN: Matt.

MATTHEW: Thanks. Harley, good points. Matthew with the Chamber, by the way. Thanks to you and your group for I think the simplicity of the elements here. A couple things just to piggyback, if you will, off of Ralph's points, just so I think I understand him clearly, to be fair to him in the points I think you're trying to be -- you're trying to make. So, I think one of the thoughts was, in terms of what else might be left on the table in terms of what needs to be communicated, meaning, hey, this is one sliver of security. It's not the whole ocean. And then I think the thinking was, of those other things out there to be managing risks, what else should be communicated. I think that's what I heard.

And then part two is does updatability automatically lead to privacy issues? And my impression is a lot of our members would probably say no; right? I wouldn't necessarily want to leave that impression. I think I've got that right. Any thoughts there, either one?

RALPH BROWN: Yeah, so I just used privacy as an example. There could be others; right? I wouldn't state it that way. It's -- and it's not necessarily trying to paint a landscape that would say to manufacturers, hey, you need to cover all these other topics about security as well in whatever you communicate to consumers. So, that wasn't really what I was trying to convey. It was really trying to be more specific to suggest to manufacturers that they be clear about what they get with their security updates, right, that it's not -- it does not answer all questions.

And manufacturers, again, should be able to compete on saying "I go far above and beyond this because I take care of all these other security issues," and they should be transparent about that. Or they say, "This is all we do." But because -- my concern is, by saying -- you know, if manufacturers start putting this language, then they're conveying to the consumer, "We're dealing with security; you don't need to worry about anything else," and that is not true. So, it's really important to be transparent to the consumer what you're actually getting with this, and that's the point I'm trying to make. It isn't necessarily it's an issue of privacy or other sorts of things. It's really trying to be clear about what this addresses. And that may be difficult, I agree, but it seems to me that there's an element of being clear with the consumer.

HARLEY GEIGER: So, in our -- in the introduction and scope language, and this is in the third paragraph, we do say that manufacturers may also consider advising consumers on these additional issues. You know, so we are altering manufacturers that are reading the documents or looking to this as a means of communicating with the consumers that they should also consider other things besides just security updatability.

RALPH BROWN: Right, but it doesn't raise to the level of being an element.

HARLEY GEIGER: Yes, that's right. That's right, because otherwise it would be out of scope.

EVELYN REMALEY: So, this is Evelyn from NTIA. I just wanted to address the scoping issue that Craig had brought up. I mean, you know, we have I would say learned from our multi-stakeholder processes that the more specific we can be, the more focused, the more successful they tend to be. And so we did intentionally want to keep this focused on the upgradability and "patchability" issues. And I think what Harley and his group has done is appropriate to stay within that window.

We're not suggesting at all that there aren't other very important topics here that could also use some additional attention, but we -- as I said, we have learned that taking bite-size steps sometimes is the best way to go. We are certainly open to talking about once this process has been underway and it looks like it's going in a good direction, what's next, where do we need to go next. That's something that we look forward to the dialogue on, but I -- and hearing from you all about what those other elements could be as well. But I do think, for this particular process, that the way that Harley and the group have scoped this is, in our experience, a good way to go.

HARLEY GEIGER: Thank you. I mean, I said we were trying to be militant about scope. This is how we got to consensus. I think that if we had opened it up to a lot of other issues, important though they may be, it would have been a lot harder to get a group of 25 people from a variety of backgrounds to agree on the document. You know, and so it does -- it does feel narrow, but I would submit that it actually significantly advances the conversation for consumers just to have -- to popularize a "standard" that perhaps manufacturers should consider communicating, A, whether the device receives updates, and, B, for how long prior to the consumer purchasing the update. It doesn't exist now. And just those two elements alone, I think, significantly advance the ball.

MEGAN BROWN: Thanks. I wanted to go back to the point that you had raised about the incurring additional fees for data. Sorry.

ALLAN FRIEDMAN: Sure. What's your name, by the way?

MEGAN BROWN: Megan Brown. I was -- I have helped on working group three. I was looking at A2, and it seems to me that -- I think the concept you're worried about is sort of worked into that second bullet. I don't know that we have thought of it. When we talk about paying additional costs as a normal part, I think -- you know, I don't think we had addressed that particular use case or situation, but that perhaps even tweaking "pay to incur" would cover that concept because I think there's lots of situations where that could happen. I don't know that it's broadly of concern to a lot of consumers at the point of purchase, but I think the concept in the second bullet there is broad enough to cover that legitimate concern that you raise if manufacturers wanted to go that route.

HARLEY GEIGER: Perhaps -- and I think, you know, we're going to have a debriefing session as a working group, and I think that we will talk about potential ways to incorporate that suggestion. And perhaps one way to do it is in parentheses after the word "cost" there, say things like "monetary bandwidth data," something like that in order to address the point.

CRAIG SPIEZLE: This is Craig Spiezle. And I agree with Megan there. We've -- and, actually, we've done some intercept retail studies with a large retailer, and I would say the consumers aren't asking those questions. So, we had to be cautions of how much we think about. Obviously, when those update a major PC versus your smart watch and things there. That's not what consumers are asking about.

There is one point that I know we spoke about in the working group, we may have lost it, but we've said that updates should not override user preferences or settings, and to the point that someone asked about privacy. So, if I have my device configured a certain way, the update should not override those. And I think that's important, whether it's a privacy setting or others. So, that should be a "should not" or a "must not." And if there's an exception, then it should be certainly the consumer should be flagged to reset their settings.

So, I point that out because I will tell you that I have found multiple devices, including my cable provider, have pushed out updates and I have found, whether intentional or not, my settings have been set to default settings. So, I think that's an important part that we need to kind of perhaps highlight back in. And I apologize for not catching that earlier this week on our call. It will be interesting if anyone else has any points of view on that topic.

HARLEY GEIGER: I think we spoke about it. I think -- I seem to recall the suggestion. I think we did speak about it earlier on in the process. I mean, obviously this has taken several months. And I would only -- I don't remember the specific conversation around it. I would only take the fact that it's not in the document as an indication that we were not able to achieve consensus on it within the working group.

SHRINAF: Can I add a point?

HARLEY GEIGER: Yes, sir.

SHRINAF: Yeah, just to address your -- this stuff. When we say "updating your device" means there must be access condition needs to be considered in the sense it's a step-wise update. It is not like going to updating the whole thing in the device. That means some of the layers you will be keeping. That called configuration, calibration of information of the device. That stays. You are never going to touch that. That requires a certain kind of an administrative rights to modify such things. Those things you lock back during the manufacturing of the device are deployment of the device. The updates you'll be doing only on the -- like a firmware kind of stuff, that's the next layer. So, this update, your software or firmware sitting in the device will have multiple layers kind of a thing. So, you will be allowed only to do certain layers on it. So, in that way, you protect your configuration, calibration and everything.

ALLAN FRIEDMAN: So, one thing I'll add is that when you start getting to certain sectors that may be regulated -- and I know there are a couple auto or former auto people in this room -- there's a lot of background about what users can do and what the manufacturer can do in response. So, if you're going to include that in the document, I'd recommend either explicitly engaging with that community or being very aware of that as you describe what you're talking about. Further thoughts on these six points? We like them? Justin?

JUSTIN CAPPOS: Sure. I just have one more point to make about B3. So, I like the concept of B3. And I have seen in -- so, this is the idea of the manufacturer describing, in detail, about the security updates. I like the at the minimum of having the idea, I think the example you brought up was, "Oh, we use this protocol," or, effectively, what it boils down to is we use the standards, which really, in most cases, means we kind of use this protocol. But it often doesn't give someone who's a very informed consumer, like someone who wants to do a security audit or someone who really wants to really understand the process, the level of information they need to have in many cases because they'll be -- you know, if you just tell me, "Oh, we just downloaded it over SSL, HTTPS," right, and that doesn't -- that tells almost no information because, you know, have you pinned the certificate; you know? Do you have your own way of doing key revocation? How do you handle the sorts of issues? Do you also additionally sign things with an offline key or is it all just trust to the server?

So, what some update systems have done is when they -- they go to release information about when they're secure and in what environments they're secure, they often have these nice, like, tables that they put where they have lists of different types of attack vectors and, you know, people compromising different parts of the infrastructure. And then what they'll do is they'll go and they'll label and they'll show what the impact of those kinds of compromises are. And that will -- you know, someone who goes to deploy a system like that can also use that table and use that information to sort of describe to their consumers exactly what the outcome of this would be. And I'd be happy to point you at some examples of this. And if you wanted to put something like this as an example in there, I don't know if it's too specific. I know you've got a lot of people to agree with, but I'm just throwing it out there as a suggestion. To committees interested, I'd be happy to engage more.

HARLEY GEIGER: So, please do. Please send it to one of us. There is my contact info. You can send it to me. I will say that we did try to -- so, you're talking about sort of an extreme end of the informed consumer use case. And we -- you know, recognizing that everybody from my mother to you are going to be buying connected lightbulbs and connected toasters --

JUSTIN CAPPOS: I won't, but yeah.

HARLEY GEIGER: But recognizing that, we did try to account for that in the page two. We said that for all of these issues, all of these elements, the ideal level of detail and method of communication may differ among manufacturers, buyer types, and so forth. And, you know, with the idea that we would -- we didn't want to go into for each element talking about, well, here's what the basic level of detail might look like and here is the extreme level. Now, we might do that if we take on the additional work that I described of having examples, but, for now, that's sort of on a shelf. And we are trusting manufacturers to know their buyers and know that if, you know, my mom is buying the lightbulb, you know, that they're not going to include the table with attack vectors because it will scare her.

JUSTIN CAPPOS: Yeah.

HARLEY GEIGER: Okay.

JUSTIN CAPPOS: Sounds good.

HARLEY GEIGER: Now, a quick question. Like I said, one of the things that we're hoping to do as a working group, we're going to debrief and we're going to internalize all of this feedback and see what changes, if any, we will make to the document. I'm hoping that the document itself, that there is not a sentiment among the larger multi-stakeholder group that, despite tweaks that we may want to see here and there, that none of them are so critical that we can't say this document stands alone as something that we can agree on; right? If there is, you know, please let us know either, again, right now or anytime, contact us. Cool.

ALLAN FRIEDMAN: I wanted to -- before you go away, I wanted to sort of talk about in terms of we can get some feedback from people that had some today, maybe some comments from folks that had a chance to read the documents, finish up with the meeting. We like this idea as a freestanding document. How would we like to see it play the rest -- with the rest of the work that's going on? And, of course, we'll talk about this as a community this afternoon. Do you guys -- does the group have a sense? You've got a very complete draft here. Time to send it out into the world?

HARLEY GEIGER: So, I think that the larger multi-stakeholder body has yet to sort of talk about what the final product is going to look like for each of the working group's products. And so it's difficult to say, you know, how our product fits into that larger product without having a clearer vision of what the final overarching product is going to look like. If I had to venture a guess as to what might make a good product for the multi-stakeholder body, it would probably be something that is -- you take the four working groups, for example, and segment their work at the beginning of a document, and then try to synthesize it together in a second part of the document.

I will suggest that each of the four working groups, not just ours but each of them, the work product that has been developed so far is good as a standalone document; right? Like the compendium of IoT standards I think is hugely valuable on its own without starting to complicate the document by referencing other parts of -- other work that the other working groups are doing. So, and I would suggest the same for our document, that our document, yes, in its narrow place in the world, that's saying these are things that manufacturers should consider communicating to consumers, is valuable as a standalone. Now, that doesn’t mean that we can't integrate it into a larger multi-stakeholder work product that comes later, but, like I said, I think we have to talk about what that final work product will look like. So, yeah, I'm hoping to send it out into the world.

ALLAN FRIEDMAN: Any -- oh, sorry. Thank you.

MALE SPEAKER: One more question. It sounds like you spent a lot of time with lawyers, working on this.

HARLEY GEIGER: I, too, suffer from that curse.

MALE SPEAKER: Is it worth at least adding some sort of disclaimer or a mention of risk to the manufacturer and communicating with consumers in, you know, various markets, to say something about risk and discuss your use of this product and risk of information or loss of information, or a breach?

HARLEY GEIGER: Yes, but perhaps not in this document. I mean, I'd be curious to know, with greater clarity, what you think that element would be or how to work it in, and how it relates to security updatability.

MALE SPEAKER: Let me look at your document I have published.

HARLEY GEIGER: Great. Yeah, please. Thank you.

ALLAN FRIEDMAN: Craig.

CRAIG SPIEZLE: We talked a little bit about that, I think it was yesterday or -- it's a blur to me.

FEMALE SPEAKER: Monday.

CRAIG SPIEZLE: Monday. But I think, you know, in general, there's much broader -- it's not just patching. I mean, if you're concerned about risk, risk assessment, there's a whole range of issues. And we're not talking about online risk anymore. We're talking about physical safety risk. So, that's outside the scope of this. But if you're thinking about risk assessment, it's all of those things. It's not just, you know, are your disclosure appropriate, but the physical, you know, the class action product issues, product liability.

So, IoT brings a whole new dimension as we think about these issues, and as these devices attack other devices. So, the risk landscape has certainly changed, and we've seen that already, whether it's bots attacking other devices and such there. So, I think that's a much broader issue than any of these working groups, but I'll defer to Megan, who has had some call for discussion.

MEGAN BROWN: Thank you, Craig. I mean, I think we did have a discussion about what the other kinds of things a manufacturer might want to talk about, and the list is potentially endless, depending on what they want to say and what consumers want to hear. I am concerned that broad statements about risk, when it comes to use of IoT devices would end up being, you know, something like if you don't update a device and if you don't do all these other things, which are prudent cyber hygiene for consumers to do, you use this device at your own risk, and they would end up being very broad. So, I think there's a scoping issue. We talked about a lot of interesting things that manufacturers might want to say, but I think when it comes to this very narrow little slice of IoT, I think trying to recommend any discussion of risk between a manufacturer and the consumer is fraught and would weigh this process down too much.

HARLEY GEIGER: And I question to what extent that doesn't occur already and whether it would really resonate with most consumers. Very informed consumers are probably going to know this already. And consumers who are not very informed, at least a lot of them, see disclaimers and, you know, vague legal language all the time and sort of ignore it. And this is intended to be something a little different than that.

RALPH BROWN: Yeah, as much as I pushed on scope, I do want to say that I really think this is important work and this is great.

HARLEY GEIGER: Thank you.

RALPH BROWN: So, don't take my comments as being, you know, negative in any way, shape, or form. I think it's great work. I think it's really important. And I think these are the kinds of things that manufacturers need to be stepping up to do.

HARLEY GEIGER: Thank you very much. I appreciate you saying that. And I will reiterate, because we are hoping to be able to say that we have consensus on the document from the larger multi-stakeholder body, please do tell us if you think that there is something critical about the document that, you know, makes you think, no, I cannot agree to this. You know, go ahead and email us about it, you know, even if it is only to flesh out your thoughts about it more specifically later. We will try to tweak it. We will internalize the feedback. We want to perfect the document, but we also do want to move forward with it. Great. Thank you.

ALLAN FRIEDMAN: Thank you, Harley. Thanks to everyone else who contributed in this workgroup effort. We have about 15 minutes left before a scheduled lunch break. There are two things. We can start in on the next working group presentation or we can have a slightly longer lunch. Sense from the community about what you'd like to do?

KENT LANDFIELD: Slightly longer lunch.

ALLAN FRIEDMAN: All right. So, I'm going to ask a favor for those of you who are here in person, which is since we are all together and this is such a fantastic bunch that represents so many different parts of the ecosystem, I'm going to ask that during your lunch, in addition to finding a sandwich and checking your email, that you introduce yourself to someone that you do not know and just share a little bit about the work that you're doing, because a lot of the value that comes out of this is not just going to be the documents themselves but how they're going to be used. And that's really going to come from the personal relationships that we forge as part of this process.

So, that's your feel good notion to go off into lunch. We will be reconvening at 1:45 Eastern Time. For those of you on the call, we'll keep the call -- we'll start the call up again. For those of you watching at home, we'll be starting again. In the meantime, have a great lunch.

MALE SPEAKER: Allan, before everyone leaves the room, could I introduce myself and make a brief ad?

ALLAN FRIEDMAN: Let's hold off until the open discussion after lunch, [indiscernible]. Is that okay?

MALE SPEAKER: Okay.

ALLAN FRIEDMAN: Thanks. Thanks, man.