>> This is Allan Friedman.
>> We will start in just one moment for those of you watching the web stream. Thank you for your patience.
>> For those of you in the room we have Wi-Fi. The password is on the slide.
>> My name is Allan Friedman and nine the director of cybersecurity initiatives for the National Telecommunications and Information Administration and I would like to welcome you all to the kick-off meeting for a multi-stakeholder process and IoT security upgradability and patching. I want to thank those of you who came to Austin to be with us in person and I want to thank those of you watching at home in your offices on the web stream. We are working very hard to make sure you can participate actively and you could join us from the call bridge later on in the meeting. I will be standing in front of you for a lot of today but I won't be doing much of the talking at all. All the work that is happening today will be done by those of you who showed up and said you are passionate about IoT security and need to make progress. We will here in a little bit from the Deputy Assistant Secretary Angela Simpson and my boss Evelyn Remaley and why were doing this and why we think it's important but the fact you are here you already understand it's a critical issue we hope to make progress on today. Before we get further some quick announcements. There are restrooms at the end of the hall into the right. We will be breaking for lunch at 12 PM Central Time. That is until one:30 so if you are watching the webcast there will be a break and 12 PM until one:30 PM Central Time on this webcast. The lunch comes to us as those this space courtesy of the Consumer Technology Association and would like to thank them for hosting this meeting for us today. We are not affiliated with them but we thank them for their support of our initiative and I like to break -- to invite Brian Markwalter to say a few words.
>> I will be very brief. I'm Brian Markwalter and Senior Vice President of research and standards of the Consumer Technology Association. It's been a pleasure to partner with NTIA to co-locate these events. We had already scheduled our technology and standards for him and had a security emphasis and it just worked out there was an opportunity to bring together a lot of experts in this field. I look forward to the discussion today. We had tremendous amount of information in discussion yesterday on a series of panels and a great wrapup session at the end of the day and I'm sure that will get rolled together in our thinking going forward. It has been a pleasure to work with you guys and let us know if there is anything else we can do. Our staff has badges and you will see a little black stripe on them so if you have questions just let us know. If you don't have a badge yet, when we go to lunch just so we know who is to, if you don't mind please get a badge at the registration desk. That's it. I think that's all we have. I look forward to the talk today. Thank you very much.
>> Thank you, Mark. I appreciate that. I'd like to invite deputy secretary Angela Simpson who was the deputy of the national tell location information administration to offer opening remarks.
>> Good morning everybody. Thank you and I would like to welcome this good-sized group of folks today to the first meeting of NTIA multi-stakeholder process on the Internet of Things security upgradability impenetrability. I'd like to thank those of you who joined us in Austin today as well as those watching on the webcast and those participating on the phone. For those of you who were not familiar with NTIA let me take a minute and let you know we are the executive branch agency that is principally responsible for advising the President on

telecommunications and information policy issues .@NTIA our main areas of focus our domestic and international Internet policy, broadband spectrum, and communications research and testing. We have also promoted the use of multi-stakeholder processes broadly to help address a range of policy issues. Specifically when it comes to cybersecurity, many other federal agencies including NTIA sister agency the National Institute of Standards and Technology have done a lot of work to enhance cyber defenses in the US. But NTIA believes here we have the opportunity to complement this work with the other federal agencies by bringing together stakeholders to boost digital security and promote US innovation. So today marks the six multi-stakeholder process we have convene since 2012. Over the past few years the colors of work to improve privacy protection related to disclosures on mobile devices and develop best practices on the commercial use of facial recognition technologies. We have also created best practices addressing the private and commercial use of unmanned aircraft systems or drones. We have worked with one of our other sister agencies, the United States patent and trademark office, USPTO on a multi-stakeholder process to explore ways to improve the system for removing infringing content from the Internet under the Digital millennium copyright act. Most recently NTIA azole ongoing multi-stakeholder process with the stakeholders work to finish principles and guidance for the disclosure of cybersecurity vulnerabilities. We think the record shows that multi-stakeholder processes can be an effective way to address emerging technological issues while allowing for more speed and flexibility when compared to a typical regulatory or legislative response. This approach has played a major role in the design and operation of the Internet and other new technologies and we think the issue of IoT security upgradability impenetrability is urgent, complex and a really good fit to be addressed by a multi-stakeholder approach. If you have not participated in one of our multi-stakeholder approaches before, be forewarned they can be difficult at times and at times a little chaotic and you may be a bit outside of your comfort zone. Be assured that they can produce good results for all parties if you engage with a collaborative spirit and a goal of reaching consensus. It's important to note that the creation of the project was a direct response to stakeholder feedback. In 2015 we asked the public to identify cybersecurity issues that could be improved through consensus decision-making and coordinated action. The area most cited in these comments we received was the Internet of Things. Earlier this year we asked for comments on the benefits, challenges and the potential roles of the government in advancing IoT. Security with the most recent topics. Your comments give us confidence that this is the right time to take on this issue. As with our other processes that will be up to stakeholders to determine the outcome they want and when they have reached consensus on it. NTIA is going to act as a neutral convener but to be clear we are not regulators and we are not developing rules or bringing enforcement actions and we will not tell you what to do. In our notice announcing this meeting, we suggest the two potential products. One is a broad share definition or a set of definitions around security upgradability for consumer IoT . The other is a strategy or strategies for communicating the security features of IoT devices to consumers. What we're really looking for is transparency in the security practices for consumer devices that are increasingly touching every aspect of our lives, our homes, our families, and for stakeholders to chart the path forward. We assess group work together, make decisions and reach consensus. So today specifically, we like to hear you share your perspectives on the current practices and challenges regarding IoT patching. We like you to begin to address the scoping of the process as well. For example, we have announced

the discussion will address consumer IoT devices but what does that really mean? It's up to you as a group to decide whether you want to take for instance a narrow view and can find the process to devices used in the home or if there is a desire to widen the scope and tackle things like connective cars and other applications, that is an option too but it's up to you how you want to scope it. At the end of the day, what we hope is you will have identified some concrete goals and created some internal structures about how you're going to work together to make the process manageable. This could include things like organizing drafting committees and working groups. You will also need to discuss and decide what you want to do in terms of the location and frequency of meetings that we will have to get to the point of consensus. Our ultimate objective for the process is to drive the creation of an industry led market-based cybersecurity solution for IoT devices and systems. We want to increase consumer awareness and understanding of this issue and help to create conditions for companies will be rewarded in the market for their investment and patching and operating devices. The response by stakeholders over the last couple of years and today's outcome and turnout here is very encouraging. I know there's a lot to talk about so I'll stop here and turned back over to Allan and hope you guys get to work and thanks for being here today.
>> [Applause]
>> Thank you. I now like to invite the deputy assistant director -- Deputy Associate Administrator from the office of policy analysis and NTIA and also my boss Evelyn Remaley who will give introductory remarks and will dive deeper and what we will talk about today.
>> Good morning everyone. Thank you for coming in. I see some familiar faces. Nice to see you all. Thank you. I want to thank CTA for locating and partnering with us and today we're very happy to be here and to share this venue to have this discussion. I'm going to be brief as well and just want to cover three quick issues. One is why are we doing this? Why is this important? The second is what we're going to do today and what we will start here and then wrap up a little bit and talk about how, of how the process works and how we move forward. On the wide, I'm sure all of you like us have heard quite a bit at numerous events about the growth of IoT and how important it is to our economy and where things are going. With NTIA we acknowledge that we see IoT here today and so many connected devices already in play. It's here, in the issue of security is a very big and important question related to these emerging technologies. NTIA is so invested and interested in furthering the innovation in this area and continuing the economic aspects. We see the security piece being something that can't be left behind.@NTIA we know we can't do this alone. It's about partnering with our society and industry partners to dig in and get to the bottom of what we can do here. As Angie mentioned we have heard a lot of feedback on what is important to stakeholders in looking at this issue. The issue of patentability did the bubble to the top and for us it so compelling because were interested in driving the market around security for these devices. This is interesting to consumers. How do they evaluate products? What does security meeting to them in this environment and how can they make choices and evaluate? We really wanted to explore this in this group together as a way to look at design principles, look at what we should be doing in terms of patentability in terms of these devices and thinking about consumers and transparency that make sense for them. In terms of the feedback that we received and what we can focus on here, there were a few high-level points that I wanted to mention. One potential vision that has been raised by stakeholders in our conversations has been that there could be

several classes or levels of upgradability out there which might amount to different technical capabilities. Each could correspond to a consumer friendly term or label that could be used to communicate simply and directly with purchasers and consumers. Behind these terms and labels could be a set of principles or specifications to help developers, manufacturers, integrators and other keep players deliver products that offer specific security upgradability capabilities. But what these features are and what we do here is entirely up to you. We're looking for you to drive what is important and what you think consumers are looking for. That brings me to my last point which is the how of how we get there. I want to say as Angie mentioned as well but sometimes multi-stakeholder processes can be chaotic. We have a lot of different perspectives represented which is what we want. I ask everyone to please don't hesitate in speaking up. We want to hear from everyone and this is what will drive the best product. It doesn't stop today. We hope to make a lot of progress today but this is a process. It's about driving consensus which isn't always easy. We will start here and we will hear from a lot of great people and I'm excited about hearing from them were doing great work. Then we will talk about what that means and where we might be able to go. We will also later in the day map out what the process might look like for us to move this forward and reach some conclusions and build consensus on what will work in the marketplace. Thank you all for coming and we're looking forward to the discussion in the process. Thank you.
>> [Applause]
>> Thank you, Evelyn. We're going to start off the day by hearing a few different perspectives to put ideas on the table. We are at the technology and standards forward for the Consumer Technology Association so we wanted to bring voices in the were necessarily part of the device manufacturers perspective to make sure we have as many perspectives on the table to start the discussion as possible. This is really the only part of the day where people will be talking to you on the webcast. After these introductory remarks from four but incredibly important voices, we will open up the conversation. I would like to as we have this discussion to listen and get ideas and figure out what you would like to see. What are some of the outcomes and goals of this process? After this we will open up the discussion and we will open up the call. If you are watching the webcast, once the presentations are over feel free to join the call bridge and we will have you come in and join us from the voice in the sky so you can participate as well. We understand not everyone could get down to Austin. With that I'd like to start with sharing perspectives and we will start with Olaf Kolkman who's the Chief Internet Technology Officer of the Internet Society and yesterday for those of you who were here yesterday gave a talk about collaboration around security for IoT . We hope are starting off in the right direction by giving an example of collaboration. Thank you.
>> Thank you for inviting me here. Sharing a few thoughts on IoT and security and multi-stakeholders. Yesterday I talked in the plenary session of around lunch and a panel discussion we talked about the security of the Internet of things. I think the feedback that I got was that the security of the Internet of Things is the topic of urgency, a topic that is shared by many to be of importance, but also a topic that is incredibly hard to address because the incentives to deploy security, the benefits and the costs are mostly externalized. It is not quite clear who needs to do what in this context and what are the benefits for people to take action. I have been talking in terms of responsibility towards the overall Internet. That's where we come from at the Internet Society, looking at the impact of these things on the general environment of the

Internet. And unprotected thing can be recognized and used against other actors than the consumer about that thing. So the approach here when we talk about security, we try to channel something that's called the collaborative security approach. And the key of that collaborative security approach is recognizing that on the Internet there is no central authority. There is no securities are -- czar. CTA might be a good level or a good place to solve this set of problems around the security of the Internet of Things. So a certain level of [Indiscernible] is needed to come together to identify the common goal and get consensus around the common goal. That's the multi-stakeholder process as it's often used in the Internet technical community. DIT if is an example of a place where people come together to solve problems. At standards maker that's what you do, you find standards. My colleagues know everything about that particular dossier. I leave that as a mechanism identifying stakeholders that have common ground in solving something is the way to go. The second thing, you are not the only one coping with this. There are many discussions going on around security and patching and upgradability. Allow me to dig out for a moment and there was a workshop in June organized by the Internet architecture board and it's a body that's affiliated with the ITF, the Internet engineering task force . They are interested in things that drive the long-term evolution of the Internet and they try to bring people together. This workshop was about software upgradability of the IoT. The report of that is that IoT software upgradability [Indiscernible] is the name of the workshop and I guess if you Google for that you will find that report. The conclusions of that workshop, I don't think they are very surprising, but there is good agreement among the participants which are from academia, vendors, and the Internet standardization community. Having some standardized way to do authorized and authenticated software updates is an improvement to having the situation that we have now. Now we have no standardized way to do this. What the scope is of that standardization activity is not quite clear. Do you want to have standardization of the full suite of updates that you can do? Is the scope really about semantic information about what types of upgrades are needed? Are there metadata formats, protocols for mainframe of states, that's not at all clear in the work ship the second workshop didn't have a consensus and that's a question that needs an answer. What is the scope of the standardization? That's another aspect of what I have just heard about signaling of capabilities toward the consumer which is an economic incentive to actually do some of this stuff and being able to signal that some economic benefit for doing the good thing. What is a good thing and what kind of standards we need from a technical perspective is not quite clear.
>> One of the questions as you know is what type of mechanisms, and outcome of the workshop, what mechanisms do we need? You can't allow yourself down time during the upgrade. A television set is turned off and having a software upgrade in the downtime is probably a good thing, but the software upgrade of an alarm system, I don't know if you want downtime for that. Questions about authority and responsibility at the end of life. When a device vendor goes bankrupt or something else happens, just the end of life of the device, how do you transfer the responsibility for upgrading that device that might live a long life in your home like 40 years or so? The realization that is essentially the same as [Indiscernible] if you want to do that, that brings security questions. How to do this in a secure way? It's also clear that this is a very young industry, or a very young topic. People don't have good examples of how to do this. Sharing good practices, sharing examples of how to do this in practice, how to do this on devices with a lot of capacity in terms of power and CPU in storage versus devices

that have no power at all in little storage and very little CPU power. Those are all open questions. I think in order to get to a point where we collectively start to address these features, we need to share information. It's not only about working in your respective circles where you find the agreement but also sharing out. It might be what is applicable for your organization or your environment in the industry or your particular vertical is very useful in another. Sharing is an important part of this multi-stakeholder aspect. And what that I'm going to get the microphone back because I think I'm out of time.

>>[Applause]

>> Thank you Olaf. I appreciate the broad perspective and of course we have talked to some of our colleagues at IAB in the report is excellent and I'm sure a lot of the work they have done will be somehow incorporated in the process. Now I'd like to invite Lorie Wigle was a general manager for IoT security at Intel Security to give us a broader perspective and IoT security from and IoT security companies perspective.

>> Thank you. First of all my name is Lorie Wigle . I'm very used to that. No offense taken. I will talk about this from two perspectives inside Intel. One of them is from a security research viewpoint, part of our Intel Security group, former McAfee and soon to be McAfee again and I will also talk about from a mainstream Intel viewpoint. I will cover both of those quickly and mostly with pictures. First of all from a security research perspective but -- I think everyone here understands there's a really big problem but I want to point out some recent insight for us as we have been doing work in this consumer IoT space specifically. Everyone is familiar with the [Indiscernible] attacked and Olaf reference that in his remarks in that it was a case where these variably, stupidly vulnerable IoT devices were used as part of a botnet and took down some important Internet sites. In that case the consumer really didn't feel the main pain of that. As Olaf mentioned the devices were used against someone else. We see on the horizon a big shift in that and in particular our belief in what we have started to prove out in the labs is that ransomware will end up playing a really big role with these vulnerable devices and that will have a very direct impact on the consumer. In fact we have done experiments with a couple of different devices that are pictured here and I want to talk about them a little bit because they bring up some of the things we need to address as we are working in the solution space. One of these is an aftermarket in vehicle infotainment system. And entertainment system in a car that you would have added by a car toys or someone like that. In this particular case this system will allow the consumer to browse to an Internet site, one of the options on the IVI screen is to do that. Unfortunately this IVI system is running a very old version of android that has the web you vulnerability. For people in the IT industry this is a very well understood vulnerability. If they were just using a modern version of android they would not have this specific vulnerability. But if the consumer goes to a malicious website, the system could be compromised and we can have a situation where there is ransomware and it's hard to read but our researchers have actually populated the screen with you need to click here to pay the ransom so you can drive your car. The IVI itself doesn't control a lot of safety critical systems in the car but there's a device you can attach to it that does so you actually could get to really breaking the car. I think this notion of ransomware is an important one to think about. The second example is a product line of consumer devices in the home, everything from Smart Plug's to the picture here of a coffee maker because that would work for me if you need to get ransomware from me. I want to include this for a different reason, because here with this whole product line it's a different

vulnerability because are using a buffer overflow to pull -- to compromise this and well understood and easily remedied with a software update, but the other thing is these devices don't have displays on them a lot of the time. All of a sudden it stops working and maybe the consumer ends up getting an email or the app associated on the smart phone will be where the alert comes. As we think through what we want to do to protect these things we need to think about the whole system associated with them and not just the specific device. I just wanted to bring these up as examples of the sorts of things we think are on the horizon and should be part of the discussion as we get into solution space. The other thing I wanted to touch on briefly is from an Intel perspective, we have been worried about operationalizing security for quite some time. I think the notion -- when I was practicing this morning I had trouble with this word, we need to think about the whole life of the device and how we protect it. It's really important that this not just be designed in security, but that we can operationalize it. For Intel and again I thought this was an interesting viewpoint because we're an ingredient inside something, we're not the end product typically, but yet we have the mechanisms in place so that our processors can be updated and in a very secure way.

>> This is tongue in cheek but we use a technology called enhance privacy ID but it's a form of identity that is embedded into the processor or SOC and it allows for a very secure connection to a microcode update server. It allows signed updates to be delivered to the processor. We get excited about being able to do updates, but those updates need to be secure. If we're opening up the update process but then not securing a mechanism for that, we could be causing more trouble for ourselves. I wanted to mention that as an example and I know not everybody is Intel in our prices are a little more than the $10 Smart Plug so there's more room to get to the point of the market incentive. The other thing I want to mention briefly, from our perspective as a foundational element of a lot of the devices in the marketplace, we have decided that there was a really central core set of hardware security features that should be in every processor for an IoT device. Whether it's super constrained at the microcontroller level or a server class processor that might go in an autonomous car. We have taken the step of agreeing of what we call internally the minimum viable platform of the set of hardware security features that will be in everything from the court level microcontroller through the Xeon processor. We're not holding this close and think everyone should be doing this. You can see the future -- the features listed here including things like being able to do a protected boot and having a protective storage mechanism on the platform so you can store secrets. Being able to clearly identify the device. These things are part of systems of systems, so if the cloud analytics are taking data from some device to give you advice on how much insulin you need, you need that to be secure and two and then you need to know you are hearing from the correct device or taking data from the correct device. We think a very simple trusted execution environment is very useful for these devices so you have a way to execute in a closed environment. Maybe you were only on encrypting the data in a very secure environment. These are not things we want to keep proprietary and we want to make sure they are in place across the board and a lot of people in the analyst community are starting to realize that hardware-based security can play an important role in the Internet of Things, maybe somewhat uniquely in terms of the value. I'm looking forward to the discussion today and will getting more to the solution space. Thank you very much.

>> [Applause]

>> Thank you, Lorie. So you heard from a broad perspective and we have the corporate perspective. Now I want to talk with the Jeff Wilbur from the Online Trust Alliance which is a consortium of a number of different companies thinking about a range of security and privacy issues. For a while they have an IoT trust framework and upgradability is a component of that. Let me load your deck. Thank you.

>> Thanks Allan. How many of you are familiar with the Online Trust Alliance, can I get a showcase? A little over half and that's great. Craig our Executive Director normally participate that rate -- at events and he sends his regards buddy speaking another event. He was here yesterday we covered this material in a session yesterday but I will zoom in on the upgradability patch ability element of it. First I want to give you some context of what we have done. If you know us you know we've done him -- we've done a lot of things ourselves and this is not a list of members by groups we've done collaborative efforts with. Many of you are in the room and we spent the whole range from security to privacy and everything in between and everything we do we try to look at things holistically. Almost 2 years ago now we started looking at IoT and said could be applied some of these principles that we have done at the corporate level advocating best practices and security and privacy so forth and apply them in the IRT area? Why should we care? There are surveys out recently that say that consumers are starting to pay attention to this and pew research did a study that almost half of consumers, the reason they have not adopted IoT devices is concerns about security and privacy and more recently Accenture did a study were 18% had stopped using them due to concerns about ongoing service guarantees. That all please into the long-term view and upgradability. One of the challenges that IoT brings his it has multiple facets. Often when you talk about IoT security, the thought is the device itself. You say how can I put security on a very cheap device? You have to think about it more broadly. There is the device of course and they tend to be very low cost and maybe just a sensor level and you have apps that control them and platforms they tied to. Often there are backend services that be the whole thing. Upgrading and patching on clouded Web services in the app relatively well known and understood, maybe people are doing a good job or maybe not but the devices and platforms often are the ones that have an issue going forward. When we endeavor to look at this, we wanted to look at this holistically. We looked at security, privacy, and what we call sustainability. It's not the eco-friendly kind of sustainability. It's the lifecycle view of the product. Lorie mentioned this and Olaf mentioned you have to take a long-term view especially if you look at the -- the connected home and you might look at a device that has a lifespan of 10 or 20 years if it's a major appliance. What will you do 15 years from now if you need to do a security upgrade on your refrigerator? Will support that a what are the expectations set by the manufacturer and the ecosystem as you embark upon that? About a year and a half ago we stood up a working group to look at this. We had about 100 stakeholders. The range was from technology providers to device and platform manufacturers to consumer advocacy groups to Internet privacy attorneys. We had the whole range represented there. Over a six-month period we distill down these principles we were trying to come up with to about 75 principles. Since then we have distilled it down further if you can say that down to 31 principles. They cover these three areas. I talked about the security element of it. In the privacy cents we're looking at consumer choice and control and the whole process of how their data is being handled and also upfront transparency and notice about what is happening. Some of the privacy concerns tend to be centered from a consumer standpoint

around what if someone gets my data if it's not secured well instead of thinking who was it being shared with intentionally as part of the business model. We want to look at that holistically. And then the sustainability concept. That has to do with the support overtime as well as device management over time. Also be end-of-life issues and I think Olaf mentioned, and Lorie as well, what do you do the end double life of a product or to sell your smart home? Audio we provision that service? These are all longer-term things. We want to help drive innovation and trust in the space. We just issued a white paper that summarizes our thinking here. Our principles are available on our website at OTA alliance.org. I have the teakettle here and I don't know if there are known vulnerabilities here but this is a usability issue, 11 hours to get it cup of tea with your Wi-Fi enabled teakettle. It points to what would you do if you had to upgraded from a functional standpoint to make it work in minutes instead of hours and it still has and upgradability element to it? That long-term thinking is important. As we look at this we develop these principles and I won't read them all but just to prove they exist, there are 31. That document is available online. I want to focus quickly for a couple of minutes on the ones that apply today. The key one is actually principle number six, which is about given the fact you're going to do software and firmware upgrades you want to be able to verify they come from a trusted source. There have already been cases where someone pretended to be the manufacturer, sent an upgrade and a compromise to the device. And a secondary one and goes more to usability but also to security is when the upgrade Tappan, you don't want to suddenly set the security settings to default and open up another different avenue of attack in the process. We have a number of related key principles and number eight is that you should secure your customer communications. This has to do mainly with email authentication. This implies you know who your customers are and of something has to be upgraded or patched, that you can tell them. How do you do that? And you have to reach them in some way, email, text, or in less it's all quite and under the covers, it's a big issue. Number 16 is make sure you are setting expectations properly for support. Warrantee is something people think about and they been talking about it for years. What about other aspects of support now that software as part of the equation? Warrantee does not equal support as we all know in a computer sense but maybe not in an IoT cents. Number 17 has to do with extending that to set the expectation for how long you will support devices or systems. It should align reasonably with the expected lifetime of the device with a turnover. And numbers 22 and 30 have to do with end-of-life or transferring the product, if I want to hand it off to someone how can I read provision that and reset it or upgraded in the process? How do I end-of-life it and wipe out the data? Those might need to be features built into the devices themselves. Another element that is in up here is there may be regulation regarding privacy overtime over what data you can capture and how you capture it. That may impact what you need to do to upgrade the device. The bottom line, an overarching principle is this has to be digestible by an average consumer. That may be the hardest part of all. You don't want to have them bring an IT staff in their house to do the upgrades. It requires a lot of long-term thinking and planning. I think these principles have been well proven and they have been up for about a year now. People have absorbed and digested them. I think they are a good framework. We did it to use as a code of conduct for manufacturers. A voluntary code of conduct. We set up a potential certification program which are measurable in a PCI cents and sulfa testable. They can be used to help frame these issues.
>>[Applause]

>> If anyone has a quick question to clarify since he offered a lot of information. We will have plenty of time for discussion. The last perspective I would like to bring his Beau Woods from the Atlantic Council also an active participant in I am the cavalry to bring a security researcher perspective as well as the security advocate perspective.

>> I've got the great fortune to come at the very end of this which means I get to say all the things that the other smart people said, I believe those too. That takes away half the stuff I would have said anyways. There's a lot of overlap in what our planned remarks would have been. Everybody has mentioned the botnet and something like 650 Gb took down the capability of [Indiscernible] and Google to support his site. The week after a less high profile person got taken off the Internet was something like a 1 Tb per second botnet. Just last week I read their 2 million IoT devices on the Internet impacted by a 12-year-old law in open SS H. The fall -- the flaw can be used for botnet and G DOS. This is not the combination but the very beginning of a trend. We look forward and projections are something like 50 billion devices by 2020 which is coming up quickly as compared to 5 billion devices to 10,000,000,000 devices today. Most of the new devices will be IoT devices with different economics and different capabilities . They will have smaller hardware footprints. Things we have talked about today. If we don't plan ahead for what we can do tomorrow, we will be stuck with these things. I'm now living in Washington, DC and working at a public policy think tank and as such I have the opportunity to engage with a lot of policymakers. Very few things scare them the way that an existential threat to the growth engine of the economy in the 21st century scares them. If we can't among ourselves figure out how to fix some of these upgradability problems, they will find a way to fix it and we probably will hate that way. We have to drive forward and these price points, there's already legislation in the Senate right now on botnets, if you can imagine Senators how to do botnet takedown's. [Laughter] They are not technical experts. They are contacting some people and they won't optimize for everything so the further out the legislation can be and have a satisfactory position in the market where we can say the industry can takedown botnets on our own and we don't need the government to mandate things, that puts you in the driver seat as manufacturers. In the EU there are also considering legislation an action around the Internet of things. It's not a US centric problem even though we are based in the US and Allan as part of the US government. It's a global supply chain issue that we need to consider. It's not just the pipes, that's the engine of commerce and it connects things. The Internet is also a critical dependency now for healthcare, automotive, planes, trains, and automobiles as we like to say. If you look in this picture, you see a small baby in a Neonatal Intensive Care Units surrounded by no fewer than I count seven connected medical devices. All of those in some way, shape or form can be impacted by things on the Internet. Whether it's a botnet or a D DOS attack or a hack of the device that renders it in operable or allows an adversary remotely to control them. We are increasingly seeing the intersection of cybersecurity and human life public safety. We have bits and bytes meeting blood and bone and a higher standard of care is warranted. The FDA in this particular instance that they expect medical device makers to provide security updates with the expected lifetime of their lives. It's on the manufacturer. They don't say how. They leave that to the medical device makers to figure out. So if you are in the room and you are a medical device maker and you were on the videocast, it's up to you to decide that. However if you fail in that duty then someone has to take action. It will be something imposed on you rather than something you developed on your

own that is satisfactory. Being able to commit to your customers that you have some type of and ability to update and giving them confidence that you can support their systems throughout the lifecycle is kind of like a warranty. It's not the same as a warranty as Jeff said earlier but it's kind of like a more tea. Today the default the fact that position is you have to buy a new device for most devices out to there. That won't be acceptable in a lot of places where devices may cost $1 million or $10 million and only are replaced every 20 or 30 years. If that is the case, the only solution to software flaws or defects is to buy a new one, that will stop a lot of people from buying if there is an alternative that allows for a much more rapid response. You are talking about signals to the buying market. As I have spent time in DC and in the halls of Washington there's a lot of talk recently about software liability. You have a liability regime and software that is the end user laser -- and user license agreement and that usually disclaims liability. You of another liability regime of public safety. We have very strong liability laws. Right now those two things are intentioned and they have to be resolved in some way. I don't know how they will be resulted in the next 5 to 10 years were looking at a definition for what software reliability in the Internet of Things will look like. Being able to take proactive preventative action through a software update, communicating that to your customers and setting expectations with not only the customers but the regulators, the insurers and the other people the ecosystem can act as a hedge or safe harbor from software liability if you clearly set those expectations for whose responsibilities, when. At their something like a commitment to offer updates through 2020, then it's clear what your expectations are and it's clear to the buyer that after 2020 all of the care and maintenance and security will clearly be on them. This can be a powerful tool to stave off potential conflicts as we go down the road. It's critical to start scaffolding that now before it comes into effect or before there is some conflict that has to get resolved that, where it's a case of public safety and Internet security liability regimes that come into conflict. I want to spend a little bit of time talking about some adjacencies to patching. This is the I am the cavalry 5-star automotive cyber safety framework. The details Arnaz relative is the concept. And patch ability, that is one mechanism that you have to take care of certain security problems. However it's not the only mechanism. If we try to solve the patching problem in isolation without considering some of the other mechanisms that manufacturers have, we will be optimizing for something that will cause increased cost, increased time lines, increased party, resources etc. Taking into account some of these other principles makes it easier to do upgradability and patch ability. I'm not going to go in great detail on exactly what these are but I will provide a patch ability lens to this 5-star cybersecurity framework. The five are basically safety by design and how do you anticipate and avoid failure? Third party collaboration, how do you take help from willing allies to avoid failure? Evidence capture, how do you instrument and learn from failure? Upgradability, so how do you respond to failure and prevent future failure? And finally segmentation isolation, so how do you prevent failure from affecting your device when there is a problem in the ecosystem or environment? Very briefly, a patchability lens on this is that in the design phase you have many opportunities to avoid having to do future patching. You can use higher-quality components. For instance, the 12-year-old vulnerability in open SSH is being shipped on devices today. That's an absolute failure of design. When it goes out the door it shouldn't have a 12-year-old bug in it that is known to be exploited on the Internet. By reducing the number of flaws you have in your devices when they ship, you can reduce the need to patch. By reducing the number of

components that you have to just those that are necessary you shrink the footprint for what you need to be able to patch. And might conceivably be the case that there are three or four different Java versions on a device that goes to market. If you have to patch all of those Java versions, you will be in a never-ending patch cycle. If you only have to patch one, it's much more simple. You can also add capabilities and the design phase that you can use later. For instance, Johnson & Johnson recently dated coordinator vulnerability disclosure with [Indiscernible] and Radcliffe and were not able to patch the device in the field however they offer their patience and alternative mechanism to keep them safe that was built into the design. If you build those capabilities that the design phase you have them to use instead of patching in order to buy yourself some time or reduce overall costs. The second point, disclosure puts you in the driver seat. If you look at similar cases a medical devices several years ago, the Hunt Spear infusion pump, Hunt Spear anew about a vulnerability 49 to 12 months before they took any action and it was the close -- disclosed to them privately and took a long time to get pics but they chose to do nothing. The same vulnerability was discovered by a different researcher and independently published in they had to act. They had a 12 month window to do something and they chose not to until they had to end her hand was forced. Knowing about those things early gives you the ability to control the time line. Isolation segmentation is critically important because for instance, if your brakes can't talk to your infotainment system, then when there is a flaw in the infotainment system you don't need to worry about whether or not you have to patch your brakes. You can reduce the number of things you have to patch within a device to just those that critically need to be patched because they are correct -- connected directly to the Internet. Finally I want to make an appeal as we go through this process to not just look at a very small segment of devices or consider a small segment of things we want to look at. We need to expand it. In the future we will have does ISIS we can't possibly imagine today. We're in a very early part of this Internet of Things. It will go on for another 50 to 100 years at least until we come up with a better or different way. If we can't build a patching an update ability regime that works for all the devices we know about, we can't hope to anticipate what we need for all the future devices that we are coming out with. And in this multi-stakeholder process if we can get the hard problems solved then it will be easier to get the easier problem solved. If we only optimize for the easy ones than if and when we need to go for the hard ones it will be much harder. That's all I have for today and I look forward to further discussions with you. [Applause]
>> Thank you and I appreciate that and thanks again to all four speakers to get the perspectives and I was struck how much they had to say in common and that's a note of optimism as well. Now we get to turn things over to view. It's your time to get some work done here while I pull up the next slide. In the meantime while we do this, operator, could you open up our call so people can have QN a? We have some microphones in the back next to Stephen. The first thing we want to discuss today is why are we here? What would you like to see out of this process? What are the goals that you would like to accomplish and what are some potential outcomes? We want to start off by making this as concrete as we can so we have something to work on. We will pass around some microphones. As you speak, speak to each other. This is a conversation and we tried to make the room as round as possible given the shape of the room. Don't hesitate to offer an idea or thought. Please introduce yourself and tell us where you are from.

>> My name is [Indiscernible Name] and I'm from Intel technologies. As the guest speakers presented it's all a heterogeneous environment. We talked about home devices and [Indiscernible] also the industry and somebody expanded to the medical industry and automotive kind of thing. It's a very wide spectrum of devices and systems and that requires a scalable approach. There are scalable devices so you want the security mechanism to be scalable in the sense of the mechanism you use, it will start at home like maybe a [Indiscernible] updating the [Indiscernible] environment. When we consider different mechanisms which are technologically available, they need to be scalable and its different. It's not one solution for everything. We should achieve that.

>> Fantastic. Thank you.
>> I have a question mostly to Olaf. We all appreciate the openness and impressive progress on the Internet. You somehow excluded but maybe not intentionally the use of private networks for things that are very high risk like IoT patching. I work for Verizon and my name is [Indiscernible Name] and Verizon for example today offers firmware over the air, they offer IoT patching, remote diagnostics over the wireless Verizon network which is a private network. I guess what I am saying is it's okay to leave the door open for private networks to play a part in security. If you're talking very high risk medical devices for example and they are all accessible over the Internet, even though the Internet is a great thing, something will afford the kind of risk we're talking about.
>> Speaking to the group but the question of what about a private network solution.
>> I think I wholeheartedly agree. It speaks of the architectural separation that was just so just act as shown on the board. You could think about architectural separation from a functional separation of firmware updates in a more secure environment. If that is available to you but it might not always be available. I think the question whether a device should be on the Internet in the first place is always a question. I actually think that all of the devices should never be on the Internet. A home network probably benefits from being completely private and have functional separation. I think being conscious about what you coupled to the Internet and what remains in a private or closed networks as part of the solution.
>> Thank you. We will hold on to some microphones and maybe Stephen who was also helping with the microphones, any thoughts about outcomes or goals?
>> My name is Victor and I think I will respond to what Allan is asking. We have been hearing a lot of problems and the security conference there's always talk about IoT and how to scale this and how many things are connected to the Internet . I think what we are left with is a framework to how to solve the problem. I think we can articulate the problem quite well. We may not know everything about it but we can say something about it. There is also a framework and just that the OTA presentation we see there is a framework but then is the framework being adopted or accepted is the challenge that we are facing. Hopefully from this meeting we can get something out of it. We can have a framework that people are accepting and adopting that will be my goal to be here for that.
>> Fantastic. A need for useful framework.
>> For the last two years there is an industry Internet consortium [Indiscernible] working on this and made a security framework document which covers some of the people sitting here. That has covered a very wide spectrum of the various Internet of Things scalability approach

which I mentioned. It is covering that. So we leverage that effort and move forward. We may not be exactly talking about updatability and patching but we can use it as a basic and do the leverage.
>> Would you like to offer a quick moment about how we might leverage that? So talk about updatability or patching?
>> What you are referring to is the industrial Internet consortium would just publisher security framework. Someone who works for be cochaired the security workgroup, the effort on that. We are finding it is actually extremely well-received because it's complete looking across the whole device lifecycle including the updatability. It's focus on industrial by definition since it's the industrial Internet to control that? This one is $129 and we've already seen the market fracture on that with a home kit which is significantly more expensive than all the chief competitors. They are not selling the volumes and consumers are choosing it. It's too expensive. They don't see the value or understand the value and part of the value is my thing will last and I don't have to replace it so I don't have to get consumer by Ian.
>> Up here and then we will go to the phones.
>> My name is Andy Wilson and I'm from the technology Institute in DC and one of the things and I can't remember if it's Angela R Evelyn who spoke with us earlier and a definition of the scope of the framework is important right now. The concern could be we're talking about too many things which will make a framework not tailored but also I would be concerned about defining the problem away by severely limiting the type of Internet of Things devices we're talking about. That's an important thing that needs to come out of today to make sure the multi-stakeholder discussion continues in the most productive way to figure out for this situation what the Internet of Things means to people in this room.
>> Can I put you on the line and offer a scope?
>> I think what we specifically at OTI would prefer a broader scope and we would limited to devices within the home is concerning because as Beau said we have no idea what devices will be in the future in the framework that is applicable , in 10 years we would not assume many people would have devices in their home. A framework written when we weren't sure that I would have on nest in my home and sensors on my light bulbs and all those things would not be productive now. So a broader framework is really important for this to be a lasting discussion.
>> Operator, we will go to Charlie on the phone in a moment but if there is a two finger response on scope to continue this line of discussion, I know Chris had one.
>> I think the scope overall, when you look at IoT you should break it down to different components. We did a lot of work at the stack and standards body and different components of IoT. There's GSM eight has published IoT standard that talk about standards for the device ecosystem and standards for the network layer and the application layer. If you want to simplify it, those are the three areas I think of. Devices, network connectivity and the application side. The scope should be covering each one of the aspects. There are different roles to play in depending in some cases you have devices that consumers are getting from the Internet and it's a cheap device they put in their house. In other cases it's a full service with the device and connectivity and application. Depending on the market and how the product is provided there are different aspects. I support the view which should be in ecosystem wide scope. I think we need to break it down into each area so there's some specificity around them. Otherwise it can get too diluted if you focused also probably. If you want to cover the whole ecosystem but drill

down in each area. As a network provider I would tell you there are things we are doing it IoT that might be different than device guys .
>> Thank you. I will have your network collect from Verizon animal go to Charlie on the phone
>> Along the same lines but maybe more of a focus scope. Very focused like you were calling for. The real barrier or the fragmented IoT market is basically due to the super diversity of devices. Some don't have enough memory to put enough security on them. Of course you can play tricks with security and put some minimal level but this is customization a very expensive. The scope I am claiming should be what kind of security, what minimal security should be put on IoT devices? The answer is really very simple. The answer is a firewall, intrusion detection software, secure storage like the lady from Intel is talking about, and of course you cannot on low-end devices to TLS or SSL because it's very difficult. There's need for lightweight encryption protocols. If you define it that way, I think it's a big step in the right direction.
>> Thank you. Last comment on the scope.
>> Another way to categorize the IoT devices and those would be durable goods and nondurable. When I think of a wearable device, something that will operate up battery, I will basically assume the battery will have a finite lifetime, 2 to 3 years at most. That's something I expect I would replace as it becomes obsolete work there would be a limited support vector. Of I think of a refrigerator with some connectivity, that will last more than a decade so that's the expectation. In these recommendations that we have heard talked about there could be a guideline between is at a durable good or is it not? There different consumer expectations accordingly.
>> Thank you. I appreciate that. Now were going to go to make sure we get remote participation so Charlie, are you on the phone?
>> Can you hear me?
>> We can. Can you introduce yourself?
>> My name is Charlie and my day job is that the [Indiscernible].
>> Charlie?
>> I'm very interested in personal medical devices that I can build.
>> Charlie?
>> [Indiscernible] vocabulary and communications patterns can be used in the public. It's extremely important that we focus on standardized ways of explaining how this stuff works, what it is and everything else. I'd like to point to a comedy came out recently that's called the in -- the Internet of ransomware things. Can you display that on the monitor?
>> We can't pull that but we have long day.
>> And [Indiscernible] the Internet of ransomware things [Indiscernible] exact [Indiscernible] you see why it's applicable to this group. Wyatt fits into the communication thing I'm talking about.
>> Thank you. I appreciate that. There were some sound issues in the room. Encouraged to think about the to medication to the public and it's not just something on one side, it's a technical issue we have to be specific on technology but on the other side we have to be very clear how we communicate to the public. Did I capture your comments?
>> Yes and by the way spell ransomware correctly [Indiscernible]. Can you display that for the people to see that and think about what it says? [Indiscernible] the thermostat says I'm turning up the heat until you warm up my bank account. The coffee pot says I will be burning [

Indiscernible] I will only make decaf until you add $75 to PayPal. It seems funny but this is the kind of stuff that is possible and the public may see stuff like this and be scared silly about any kind of devices in their house. It's very important that we emphasize that we are really thinking about security and how we avoid things like this. [Indiscernible]?
>> I'm sorry?
>> Are you able to bring up the comment?
>> We're not able to bring it up right now. Thank you and we have logged it in the notes. It underscores something that Lorie product earlier in her remarks about the rise of ransomware so thank you. I want to go to the right side of the room.
>> Jeff Wilbur, just to answer the question about framework and adoption and such. One of the things I neglected to mention was we had a few people involved in our working group that were in the distribution chain for these products. One is a large retailer you would although nationwide and one is a home security provider. Both of them are using the framework as a checklist for their vendors. Just by doing that and inserting that in the supply chain, that has raised the bar on what they are looking for for these products. So products will have security and a long-term view of things and abide by certain privacy rules. That is one way we could insert ourselves into the market to make an impact.
>> Thank you.
>> I think one quick thing I want to mention is we think about patching as something that we have [Indiscernible] but at the same time we should think about before a product is released maybe we should do something about it. A few days ago I was reading about Tesla when they were releasing the first version of software, they have not been spending much time on the security development. Often times during the development lifecycle it would make a lot of easy to discover bugs and after they release, the bugs come out. Of course going back to the comment before, about the investment and often times that would be difficult to convince management because that usually is not making money. I believe security for the lifecycle should be part of the discussion. That's it.
>> Thank you. And for those of you who were not aware, earlier this morning there was a discussion that CTA posted with [Indiscernible Name] on applying that model to device manufacturers. Beau?
>> I wanted to comment a little bit, I've heard several people this morning talk about things that are more the means and ways to accomplish the goals but not really the goals themselves. If we steer the conversation towards what are the ends that we can agree on, some type of a patching regime might have? I mentioned in my segment that right now the de facto default standard of patchability and updatability is buy a new one. We have that as a floor and how do we build on that? How do we imagine what could be levels of patchability? For instance as one of our ends that we want to connect out with, I think one of the pieces to one of the comments earlier about end-of-life is critical, because if you look at a vehicle, is -- it is expected to have a life on the road of about 11 years. If the carmaker only supports up for 4 years with sophomore -- software updates, what does that mean in year five? What does that mean when there is a critical defect found in a car that is five years old and no longer compatible through the manufacturer? Is it considered negligent to be on the road to begin with? We certainly have that as the case in certain safety recalls that are mandated where a vehicle over a certain age and not be on the road if it has this component in it known to explode like the pintos from the

1960s. You are not allowed to drive those things. When you go back to your missions check they say you haven't done your update and you can try that on the road anymore. I think that can be a very big driver for pardon the pun for fleet buyers for instance. We go into this with the Smart home, home Internet of Things things in mind, but the thesis that buyers don't care about security is not true if you go to institutional buyers like medical devices, cars and others. Security can be a very big driver. One of the ends we should work towards is how you unlock that and how you make these markets more transparent so buyers can tell the difference. So it connects the security piece to something the buyers care about. In the medical device space and the fleet buyers space they really care about how long is this device going to have to be down because of patching or some update? How long will this be off the road if there is a safety recall when I can drive it or rent it out? Those are things that connect very much with those buyers and they have a clear security link. I think making those links evident will build some of the market forces in that we need to drive this. Later we can worry about how. How can be a question of degree rather than a question of presence or absence.
>> A new voice in the back and then we will go to the front.
>> This is airing from Microsoft. We have looked a lot a different public policy regimes around the world and as many of you know the US is behind the ball relative to other countries and that's okay because we learn from others and decide what to do. I want to push the discussion towards Allan and others from NTIA as an insert to the discussion we are having because we all can theorize and where they should go and ultimately we have to own the process and I appreciate that. What I'm curious from the governor perspective to hear about is where do you see the gap if you will from a public policy perspective? Ultimately if this is a document with the NTIA stamp on it there is a question that if you got FTC or even FCC activity and DHS activity over there, where is the NTIA role and how do we optimize so we are not only doing what people in this room think is important but work with you as our conveners in the process?
>> That's a great question. I don't want to derail the conversation too long around that. I can say that NTIA as two work streams on IoT. 2 1/2 actually. The half is make sure we collaborate closely with government partners and colleagues. Ruth from the FTC is here and we have talked a lot and working with DHS as they develop their high level guidelines. Many of you in the room wrote comments earlier this summer on what the government role would be in the gentlemen in charge of taking the comments and turning them into a very constructive and powerful document his travels call. You want to say some quick words about the progress of the document and what that might look like in terms of what it will say?
>> I will talk really briefly. We are currently drafting the green paper and it takes a very high level look at the Internet of Things as an overarching term. We are as the Department of Commerce and the unique spot where we can take an ecosystem wide view of the topic. We can look at question such as security but also question such as infrastructure development and what area of international engagement can or should be. It's a green paper which means Department of Commerce as the focus. Previous papers on privacy and intellectual property have turned into administration white papers. We do have an administration change coming up so it's not entirely clear if that is going to happen but we think the topic is certainly important and ripe. What the relationship between that process and this one is is that like Angie said, security was the number one topic that was discussed in the process. Is extraordinarily important. -- It's extraordinarily important. On the green paper process were looking very high

level. Were looking at the overarching government role in policies. At the same time we don't want to rest on our laurels. We don't want to wait for the next administration and we want to get our hands dirty and get to work. When the Department of Commerce gets to work it usually includes listening. We involve stakeholders and getting you guys in the room and a certain extent to a lot of the work for us. That's allowing you to lead. That's where we're at in terms of the differences between the two processes. I don't think that actually specifically answers your question which is what are we looking to get out of this process? Would like to potentially be overruled, but I do think the overarching thing we're talking about is transparency in patchability practices. This was commented on by a number of people so far, but talking about how do we actually communicate to the public or to public facing groups like CTA or others what patchability is and means to help create the market? That is our goal with this. However, that being said, this is your process. We are here to learn and be led by you. If you want to expand the scope, we're willing to work with you on that. I will turned back to Allan to further discuss that.
>> Thank you and a great model. Commerce likes it when markets work. Anything we can do to help foster that, I think we've heard from a number of people that security is a large risk if it's not addressed and it will really do great damage to this trend and innovation. I've got two remarks, one in the back.
>> I think this is an incredibly good discussion I want to the throw out some arty ideas that might have already been mentioned but I don't think have. The first is to what degree as a goal or outcome, one thing that would be interesting is to leverage the governments acquisition process in terms of contracts so it could be recommended contract language. When someone acquires IoT devices, what type of software needs to be baked in? The second thing is on the notion of not only do we want patchability but I like the discussion about the 2 million devices with FSH vulnerabilities. The question is the ability to make people more aware when things are not patched.
>> Could you introduce yourself.
>> [Indiscernible Name], University of Washington.
>> Matt within CTA. I want to circle back to the goals and the outcome and it goes back to what Chris was saying earlier. The key thing to look at a framework for how to put together the framework. It is a boil the ocean kind of problem. It's important to get the scope and talk about the framework so you can look at where you talk about patchability and use a patch the device, patch the network, patch the application. If you think about the Jeep problem that got disclosed a patched the network initially to solve the problem. Then they came back and patched the jeeps themselves. If we put together the right framework to solve this problem, the same framework can be used to educate the consumer's so they can understand where the solution should be coming from. Right now everybody looks and says fix it. But who was to fix the?
>> A two finger response next to you? Or a five finger response.
>> Two thoughts and this goes to what I was saying earlier. I like to think of this as a horizontal and vertical issue. Horizontal you have a concept is there a framework that applies to upgradability across each one of the different parts of IoT? Each one of the verticals you have to do more of a drill down of what specifically can be done in each area. If it's a device side, network side application side, but there could be consistent methodology applied across each

of them. The other thing I will say is the other thing the group should focus on a maybe not the perfect example but when we did the work on the botnet, I think we should identify quick wins or some practical pragmatic things that could be done and could be recommended in a short-term to build momentum and as Matt pointed out the problem is boiling the ocean with so many different aspects to it. If the group can identify some things that could be done in a reasonable timeframe that are practical and pragmatic, just common sense things that could be done in a short timeframe, that's a way to build momentum and builds the value of the process. It would help you with the other issue that a lot of us are concerned about witches -- which is having one process dealing with the issues are having it splintered off into five or 10 agencies looking at it.

>> And some of the industries when they address a long range of [Indiscernible] small devices [Indiscernible] network or a cloud kind of thing, they adopted a certification or qualification methodology with adopted levels. For example you must have heard of [Indiscernible] one, two, three, four, five and you have heard of that. You could do certification like gold, or silver, and copper and we can adopt the kind of method to certify that so that the cost is covered from your perspective and variability and flexibility is available so you can deploy level by level. It addresses his point that you may not have to do everything together. We can do with step-by-step.

>> Very quick response.

>> I like the idea of some type of certification and common criteria which I think is a good one. One of the problems with it is it takes a long time and it's very expensive.

>> [Indiscernible - low volume]

>> We have folks watching at home.

>> Currently you are right. Certification is a long process kind of thing. We need to adopt and leverage what is best used and we need to create a new process. For example [Indiscernible] took the same approach but they did it in an easy methodology. We have to define some certification process here.

>> One of the problems I think you will run into there is how do you convince a kick starter size project that they need to do some type of certification and once you have convinced them, how long is the weight before they get tested? And once they fail, how long is the weight before they can go back and recertified? I like the certification process and I certainly think it makes sense in things like cars and medical devices and other things, but it might not scaled-down to the very small manufacturers. We should also consider other mechanisms within that. It may be like a material model where you certify and that's a certain maturity level or you can self declare.

>>[Indiscernible - low volume]

>> We will come back to the certification question but I want to go over to Darrell.

>> I am Darrell and a research lead at rapid 7. Some of the comments coming up dealing with QuickWins. Probably one of the areas I thought was fascinating, I did some research a while back on consumer automation systems. One of the products I was looking at, I was amazed at the way it handled its patching process. The thing was mentioned up there that end-users need to be notified that there are patches and that is a plus. Consumers won't go out and get patches and put them down if they are not notified of them. On that particular product, there were several cool wins. One was the actual cold, the firmware was encrypted. That's a good process.

The second every time I fired up my mobile app to take a look at my lighting system to turn it on or off, it would do a check to see if there's a firmware upgrade or changes and they would notify me if there was. It would tell me each time and let me pick the time it was upgraded and I was able to do that. When I did it it would automatically update the gateways, push out upgrades to the light bulbs, and notify me when it was all done. It was the a real Goodwin and something I like to see. Unfortunately you don't see that an everything we look at so it caught my attention when I found it.
>> Anyone else have thoughts on either some QuickWins or broader question of what would you like to see coming out of this process?
>> My name is Mario when I'm with electronic solution company and growing university. I will give a slightly different perspective on this. As a consultant I get paid to tell people what they need to hear and not what they want to hear. I hear people talking about patching and upgrading. To me that terminology is like putting lipstick on a pig. The underlying problem is we screwed up, we failed as manufacturers to do a good job to begin with and were trying to fix it later on. We're too quick to get to market and not taking enough time to design a proper product when I look at the whole thing of IoT, IoT is not a product. It's a piece of technology we can use. ICFs discussing this stuff around the table and it's kind of like we have a fire going on it we should put the fire out but what are we doing? We are pouring more gasoline and making the system more complex and the more complex the system, the more difficult it is to wrangle it in. You will never fix the security problem. We can make it better but this is a game of cat and mouse. We may come up with something that is hard today and tomorrow someone will break it. You need to go back and do proper and generate. One thing we tried to impress upon students at the University is stop and take a look at what the real problem is. Do we need to apply this level of complexity to everything? And some cases it's true when the gentleman from Verizon and Olaf said earlier not everything should be on the network. We're taking devices that don't need to be on the Internet. You have a thermostat. What is the task of a thermostat? Maintain comfort in our home. You can do that with a little bimetallic switch and a [Indiscernible] and now we put processors and there and we have exposed our home to take a very simple process and made it extremely complicated. I think it security is a primary concern for yourselves as manufacturers and for your clients, do some systems engineering and say do we nearly -- do we really need to apply IoT to a simple device? If you do weekend cooperatively talk about it but one of the gentleman before said in the next three or four years we will increase the number of devices on the network in order of magnitude. Do we need to? Can we take some of these devices and go from IoT to DOT which is what Olaf was getting too. Have our own enclaves in your home. My home automation clients have their own enclaves and are not on the Internet. I want stick and IoT device in their home because security is number one for my clients. I was working with one of my medical clients the other day and we were talking about pacemakers. I have worked on pacemaker programmers two decades ago and the only way to program the pacemakers literally get right up against it but now they say you can program it from across the room and you can hack them.
>> Thank you. I think we talked about a number of things there and one of which is why are we talking about [Indiscernible]? At NTIA we said building security in and having security engineering is part of this discussion. Were not trying to imply it's a substitute . We also feel it's a compliment as we roll out these issues just as you said, we will never have a perfectly secure

device so what can we do? The question of complexity is something I'm interested in. How do we talk about adding upgradability or patching? Not everything will be a patch. Sometimes it will be other mitigation strategies without adding extra complexity.

>> One other comment. We need to address or think about the notion of orphan devices. We talk about end-of-life but there is also orphan devices and the company's I represent, that's a big problem for them because no one is making a patch for them because the company no longer exists. How do you address that in this whole thing because that's a big problem?

>> I just wanted to add comments on the question of thinking about the disconnected homes and disconnected axis. We did a collaboration with University of San Diego we did work on automotive analysis where we looked at vulnerability in one of the things we found was that the car's CD player was connected to the car's internal computer network. Because of of vulnerability in the CD player we can make a CD that if you put in your laptop would play Beethoven's ninth Symphony but if you put it in the car up with unlocked the doors. An example that even these ecosystems that are supposedly connected to a network can have vulnerabilities and thinking about the patching there. And of course we see situations where someone designed the system to be disconnected and not on the Internet but something happens five or 10 years later the ad connectivity and ecosystem becomes vulnerable.

>> Thank you.

>> I am a consultant to the IOC and I appreciate the comments on the IOC and I want to comment on the disconnected stuff. I want to take the counter this particular point about the disconnected thermostat. This is an evolving world. You mentioned earlier the fact we need to look at needs over a period of 50 or 100 years, the first people who put thermostats and probably thought this is just a more cute and sophisticated way to control the temperature. The way I eat use it in my home I don't even use the programming feature in the current thermostat. When he wanted to be hotter I just turned the dial. You have legitimate reasons why people may want them to be connected and we don't know all these reasons now. This will cause a lot of these devices to be connected. One reason is you decide you were coming home early and you want to connect to your thermostat and get your home air-conditioned better because your returning earlier than usual. The other reason is you want to pay less in utility rates and therefore you want the utility to be able to reach her thermostat in order to shave off some of the peak electricity consumption that costs you and him so much. I don't think we can dictate that consumers will not want to connect the devices. We can scare them into thinking that but if they have an incentive such as lowering their utility bill they will accept that the utility provider connects to the thermostat so we better be ready for this. We will not be able to control the fact that it doesn't happen just because we think it shouldn't.

>> Thank you.

>> We have a comment in the back.

>> I want to make a couple observations and comments to help us potentially was scoping. I notice that both AT&T and the Online Trust Alliance highlight a three-part framework between devices, applications and backend network and that's a hopeful framing for us going forward as a potential focus area. I think in the discussion we lose ourselves a bit because we go back and forth between really pure consumer stuff and I've seen internet-enabled jump ropes all the way up to critical systems. For going forward purposes I think there's more space to covering noncritical sectors as a potential focus. That's where I think the market failures more likely to

happen. The critical sectors are regulated and eventually the regulators catch up and forced some of this. If it's not addressed for example by the FDA or other authorities, that is where potentially commerce and the other agencies have a role and we can support that role. I would advise focusing on noncritical sectors. The final thing is I think it would be interesting for this group to focus not necessarily a things like recommended practices because that can turn into a war of words over who's doing what, but rather what are the desired outcomes in the spaces? What do we want to see happen within a five-year time period? You get into groups that have been mentioned and I won't go through all the acronyms that can develop the practices and standards to get us there. I think desired outcomes and noncritical sectors across the three different areas might be a good place to go.
>> Thank you. Professor, can you introduce yourself?
>> [Indiscernible Name] I'm Chester with [Indiscernible Name] and I will continue from there. A couple of the comments that talked about orphan devices and things and seems like, I don't know how you go about it but it would be nice if the framework and address mitigating those risks. I did research a year ago and I bought six random devices and they were all vulnerable. By the time I reported the vulnerability two of the six manufacturers had close so I couldn't report the vulnerabilities responsibly for a third of the things I purchased and everything had vulnerabilities. One, the state of affairs when -- the state of affairs at that point everything I touch found vulnerabilities. Two, those things are out there now. Is probably a few hundred thousand houses with smart door locks that will never be patch because the doorlock company is bankrupt. They don't have a website so I assume they're not even a legal entity. These things happen. Is there a way to build failsafes because back to the Krebs incident, that was Plano http traffic being [Indiscernible] by a Linux operating system and no way to identify as being that camera. The Verizon's of the world than any other network operator couldn't say I identified the traffic and one allowed out of the network because there's no way to know what it was. Are there ways we can tag these things in some way so at least they can be identified when they are exploited to the scale that it could be a network takedown event? We can't count in organizations that continue to exist to be available to be bullied into patching them. The only other comment that is leading to a lot of this to building things by design was the buzzword right now of everyone I talked to building of the stuff is minimal viable product which doesn't include security at all. Minimal viable product if I put on the shelf will make a penny. If I can make 1 million pennies I am off to the races and I worry about it later. Without regulating I don't know how you fix that. As long as it's voluntary I will ignore everything you tell me.
>> I'm still back to the goal. The goal being signaling I believe. Breaking this up in network [Indiscernible] and application makes sense to me. What is ultimately the goal of the signaling to inform the consumer about bad things and have the consumer make informed choices because we know consumers are bad at making informed choices? Or is it to create a market differentiator for the people who make the product?
>> Any thoughts?
>> I have a thought on that and I won't say it's incredibly mature but it's an observation that a critical part of markets is differentiation. You have to be able to tell one product from another. It is the ability to know what costs and other considerations you are taking on, what responsibilities you are taking on. It's to have some type of recourse when even in your own best actions something fails when there is a defect. Right now I could make a case and I won't

say it's the truth, but I can make a case that right now we don't have in the security market differentiation. Everything looks like the same crappy to Peter is everything else to quote someone from an FDA panel earlier this year. The second piece of that is that consumers cannot, even if they really want to, find out what risk levels the manufacturer has taken on their behalf. That part of the market isn't working. The third thing is we don't have liability regime that is consistent and well documented. Sold three critical parts of a market. Your question is a good one. What are we trying to solve for a year or? What is the signaling solve for? The signaling can be prototypes to help build those pieces of a market so it's efficient and can be efficient. I don't know if that is the answer you were looking for. But it's a thought.
>> The question was does that help the discussion. You mean this discussion we are having today?
>> I think so. The Department of Commerce their job is to make sure that markets work. I think the market in this case doesn't work in this current state, what can we do to help shape that market and allow it to work in the way it needs to so we don't have to take other measures. Legislation and registration, the point is to step in and [Indiscernible] the market when it doesn't function on its own. The market is and even set up to function and I'm not sure that legislation or regulation would fix that. Would you spend it in a different way.
>> Megan, I'm a lawyer and I help a lot of tech companies and IoT folks figure out what's coming down the pike. I encourage NTIA to be mindful of assuring there is adequate rigor to determining or speculating about what a market failure is. It's easy to say there's market failure because consumers are behaving the way we think they should in a future we don't yet understand. I would encourage folks to have some humility about what we are saying about the functioning of this market given that the inputs are so pretty unknown and I agree that legislation or regulation is likely to distort that. I don't want to rush into everything is broken and we must come in and provide a fix.
>> Transaction Mac
>>
>>I think part of what we need to do is to get people thinking more about these issues and dealing with awareness. I know I have had conversations with underwriters laboratory for example. They told me they have their own members. Electrical issues. They have had the members today saying they would like UL to provide a cyber security program so they can say they are defined -- devices have cyber security building. You actually have manufacturers going in and same we want this to differentiate ourselves from the consumer devices do not have that. If we can try things there is a market value. The challenges to get consumers to care enough about a device that has a UL that has a label. If you get consumers to care enough about security so they look for this type of label you can create a market-driven mechanism to get folks to go out there and do these type of things to sell their products. That is a long road. It takes a long time to get people to actually care. Not very sex-role today on that issue. We made security way too complicated. That is a way to drive demand to get people to create a value for the device manufacturers themselves. The only other comment is that I totally agree with the comments for Microsoft that we really should on the industrial IOT space and enterprise space a lot of companies are going to require security built into the products they are purchasing so that is more of a procurement supply chain thing and that is more easily manage than the consumer side.

>> We have a few minutes before we break for lunch. Is there any left comments on this question of goals are what you would like to get out of this?
>> I am from rapid seven. One thing that came up early in the slides, I believe it was the set of Intel slides, I saw the hardware controls on their. While I am a giant fan of encryption and verify where your patches come from and all that jazz, what I saw was also a [Indiscernible] enforcing mechanism. I am super concerned. I want there to be a good solid safe way to patch devices in the field. I also want to not accidentally be enforcing a very heavy-handed digital rights management solution. So I want this unicorn of super secure patches and also the users ability to tinker retained.
>> Thank you.
>> This resonates a little bit with a concern that I have if it comes to certification in general. One of the things that we identified as one of the properties of the Internet, so this is really a little bit of an intranet focused remark, permissions innovation. The ability to innovate without having to ask anybody for permission. Certification might be contrary to that. Might be, I am saying. If it is used as a cynical -- signaling mechanism, I don't think it is. But as soon as you need the certificate to connect, we might cut into our own flesh. I think that's resonates with what you said. And I also think that what you just said applies a little bit further down the road with obsolete devices. If they are heavily protected, nobody can take over the responsibility. So I think those things all come together and have complexities that need to be thought about.
>> Thank you all. This morning's conversation I think was broad, free ranging and that is good. Sometimes these processes feel a bit messy. Because everyone comes in and have seen the type focus of discussions from their perspective. I think the power of this process is that we all come from different perspectives and backgrounds and approaches and goals. So this afternoon I will continue to look at what a shared goal that can make progress will be. That brings in the themes we heard this morning, the consumer side, communicating approach, and also that builds on the market incentives on the producer size. -- Side. So keep this in mind. Have conversations with each other. Make new friends over lunch. The consumer technology association has very kindly agreed to buy us lunch with their broader convention that is going on around us. For those watching at home, we will be resuming at 1:30 PM Central time. thank you all for participating. This was a productive morning. [applause] [Lunch break until 1:30 CST]Welcome back everyone. Thanks to those of you who are stuck with us or who have stuck with us rather on the webcast. Last -- [laughter] the discussion this morning I thought was very productive. What I took from it was that was heartening was that everyone seems to have reached a very similar conclusion that IOT is a very large and messy issue. Security is important. And one thing we can make some tangible progress on is this question of upgradability and patching. A couple of themes that came out is we want to revisit the question of scope. We had a good discussion around that and what we want to consider in or out of scope. Scoping is I think very important to gaining traction. If we do not have something somewhat clear about where we're going to focus, it's going to be hard to target discussion. The other is a joint discussion in parallel on one hand the consumer side, what does the consumer see, and understand, and that drives the market. It is not just the end consumer. It is also enterprise purchasers and things like that. On the other side, we have the technical side. You cannot have those discussions completely independent. They mean -- me to be the same part of it. Does that sound like a good some of the main -- sum up of the main themes this morning? We want

to start off continuing this discussion of outcomes and goals. Those of you in the room have done a decent amount of travel to get here. Hopefully slightly better than how the government census places. Those of you watching online are giving up a decent part of a very busy time of the year. So we want to find out, what are we hoping to get out of this? What is something that you would like to see? What is a vision that you have that can be tangible and constructive and genuinely help the security of the ecosystem? I am going to turn the floor over to you to do the hard work. I just get to ask the questions. With a reminder that our phone lines are open. Call now. And have added. -- At it.

>> Just a couple thoughts and they fall in the category of a quick win thing you were talking about before lunch. One is, and I will tell you we attempted this after we posted our framework over a year ago, is getting whatever the side of principles, whether they come from a conglomeration of things that have already happened or whatever, whatever the final list is, getting companies to publicly say that they will follow that as a code of conduct. That can happen very quickly. It becomes public and shows movement. But it is not easy to do. Because as we went through the process, I said to over 100 stakeholders and we came to the end and there was agreement, but not a lot of public endorsement by the companies themselves. Most of them, the rationale was our current products do not do these things. We will be there in a year. So maybe we will revisit this in a year. That kind of thing. So that is one idea. Just getting public commitment from stakeholders, especially device manufacturers and ecosystem suppliers. The second is, and I don't know how this would be funded or done exactly, some kind of benchmark of where the state of the market today in security and upgradability and where do we stand. That you can measure progress as you go forward.

>> Sounds like a very interesting research product, looking at the professor in the background. What can we do on the commitment side, whether it is getting companies to commit as an organization or at the product level in terms of -- a number of people talked about labeling earlier today. Anything else about what you would like to see? Dream bed. -- Big.

>> I have been thinking about this for quite a while. I think there is a number of things that an outcome from this multi-stakeholder process should hopefully yield. These might not be fully inclusive, but I think that the clear public commitments is a very good one. That is one that definitely is on my list. Another one that's on top of that is that it should be easily measurable whether or not those commitments are hit. We don't want to get into the business of saying in my opinion you did or did not. That makes it last -- less trustworthy of a mechanism. I think that we should look -- more broadly. Across not just consumer, but also some of the industrial or regulated industries. The thinking being that even if this never gets applied, if we ask ourselves the question, would it be a success to have something that works only for a type of consumer IOT that fails to work in medical devices in cars, in windmills. I think if we -- if our target hits that consumer grade, but it misses the other ones, then I just have a feeling and an instinct that we are at the wrong level, to specific or that we are too much into the how this should be done and not enough into the objectives and goals. I think that what we should come out of here with, maybe not today, but definitely by the end of this process, is general buckets. Once you have these kind of buckets or categories of what we want to see in patching and updatability, then we can talk about measures of degree, whether it's 10%, 20% better. But if we do not consider all the buckets, then we have to be incomplete. I think that those buckets can fall along the lines of a who, how, what, when the white type of list. Who is responsible for what. Is

it the manufacturer will push all updates? Is it the consumer will go to a website and download and apply them? Is it somebody will take it into an expert to do this? Who has these responsibilities? What will be updated? So maybe my brakes have a different update mechanisms that might infotainment system. Regardless of whether those two things are completely segregated and isolated from each other, you might still have a desirable outcome to have one part or component of a system that has a different update mechanism from a different part or component of a system. I might be wrong on that, but that bucket I think is a good one to have to consider. The when component to be how quickly you take some action, which might be a patch or something different. Once the critical vulnerability is known, are you going to be able to commit to a certain timeframe or not. I don't necessarily know that there is an answer that is the right one, but that is something to look at. Also, for how long? This goes into the lifecycle. How things age out. Is there an end of life? That one in particular I know that, I think it was mentioned this morning that the Google pixel will have a 24 month support cycle. So from the time when you buy one until 24 months after that they will support it. I am not sure -- you can talk about whether or not you want it to be number of months or a finite and date, 2020 regardless of whether you buy this device in 2014 or 2019, by 2020 it will stop are you that supporting it and stop pushing updates. How gets into the who. Over the air mechanism or something like that to define that against expectations and then why I think could be something like we will patch critical vulnerabilities in third-party code. We will patch some of the other things. We're doing this because of a commitment to the consumers. We're doing this because of a need for a standard of care in the industry. I think we can maybe flesh out the why a little bit more. I do not have a great answer for that right now. In general, I think those things for us to have as objectives, at least that is a stake in the grant. We can add and subtract and modified, but clear public commitments, easily measurable commitments so it is readily apparent as possible, to be inclusive of things that we today know exists because tomorrow we will have things that don't fit into these existing categories and we want to try and capture as much of that as possible, and then to define the general buckets in categories and make sure that they are fairly is not exhaustive -- fairly exhaustive.
>> Thank you. That was really helpful. They will probably be responses. I am going to push you on one thing because that is a great framing for do you see that as the five dimensional matrix, or do you see a couple of different clusters based on different answers? How do you see as dealing with that? Back I see that as a starting point. It is a way for us mentally to think about it. As we get more fine-tuned on what those buckets are, we can give them different names. But for our own thought exercise to figure it out. I'm sure that those will change by the time we get to some future state.
>> Want to follow-up on one of your earlier remarks about thinking that. One of the things I want to throw there is thinking about the fact that IOT has adopted all over the world so we're thinking a lot about the United States. But there are other devices being produced in other countries that might not enter our markets. I would love if we can take a global view where we increase the sea level all around. The other thing I am want to toss out there, the diversity of stakeholders impacted, in particular some of the things we looked at where children's toys. Children who are administrators of devices. Thinking about the diversity of stakeholders in the process of upgrades.
>> Thank you.

>> One of the questions I have is we're sitting here trying to decide what the objectives are. We have already had two frameworks and multiple efforts discussed from an industry perspective that already exist, and we're going to start reinventing the wheel. Probably not a good idea. The question I have is, where is this kind of work those -- focus today much more than any other place so we can actually start to see where the gaps are that we would like to address or we would like to augment that would be beneficial? I am not a proponent of duplicating effort or fragmenting guidance, so I would really like to try to figure out where the bright place to do some of this work is.

>> I think over the air secure social patching. We do it to suit -- today and it is very secure over a private network. Obviously, all companies want to make money, and if they do not commit because there is lots of dependency, not just on the device makers, but the security in these devices. So dependency is a problem. In the absence of a user driven market, which hurts all the -- so you really need to have some kind of leadership on the user side. Obviously, the government with their procurement, assuming be right very since -- specific specs, that would really help quite a bit. On the other side, I think if you just look at the very impressive history of the [Indiscernible] how they put out in the public domain workable code that is neither ambiguous English or paper standards or certification to code is downloadable and free. Companies take it and use it quickly so the cost of building products becomes very easy as an entry to the market. So I think the challenge on the side is finding some very core tensions that -- functions that span a lot of industries. This homework can be done. Having someone like the [Indiscernible] encryption standard, just put it in the public domain and companies downloaded. You really need a closer driven -- user driven approach as well and the government can be part of the leadership and driving the purchase.

>> There are multiple things people are already working on. And automate if we do communication already. [Indiscernible -- heavy accent] we need to look into those kind of things and to bring that. Leverage. [Indiscernible] has done something, everyone is talking about the device. Smart meter or vehicle. The philosophy is the same. The principle behind those, patching and these things are very important. When you are doing it from an update patch kind of a thing, the device, I call it [Indiscernible -- heavy accent] the device also should be secure. It is not only the one mechanism which does this activity, that is very important.

>> I can offer quick comments on process. First, my understanding of the federal advisory committee act says that this kind of process cannot dictate government policy. Which is not to say that we cannot produce something that other parts of the government could look at and say that is useful and we should use that, but as I understand, we cannot use this process to directly advise the federal government on what to do. But feel free to create things that are very useful for, among other things, a very large purchaser based on the District of Columbia. The other thing that is important to acknowledge, and yesterday we had a panel where appeared next to each other talking about how we work together, this was not set out to be a standards development process in a classic technical process. There are different approaches. And there are many different bodies, and I love the suggestion that said we should make sure that we are aware of all of the other ongoing efforts because the sectors right now are quite split and diverse. And what we can learn and maybe even help harmonize across different verticals could be very useful.

>> I would like -- in the effort to get a little bit meat on the bones on the why. I think it was clear from my introduction and what we talked about yesterday that, for me one of the reasons why we want to have this is to protect global public good. The Internet. That is one aspect of why. We want to protect our environment. And environmental reason. Second, consumer protection. After 24 months the consumer is not left with a brick device for instance. Clarity in that. I think if we make an inventory of reasons we do have -- we could have something we can walk away with today. These are the things we all agree on. There are several reasons why we want to do that. I think that perhaps the approaches given the why in the context of why might be different. So get to an outcome, this might be the low hanging fruit.

>> One quick response to that. I agree. I also think one why is when an update is sent, why is the update being sent? Doesn't fix something critical or is it something that might be postponed. That is a big part of Microsoft's patching. Your notification to customers. The other idea that I wanted to throw out there is, a lot of people have mentioned existing standards and frameworks and things. I wonder if one of the working groups would look at existing standards and maybe part of the benefit of this group is that we could emerge a superset of objectives and goals and outcomes that all of those standards have in common. So we are not reinventing the wheel. So we are creating something new that is an extensible framework, and then we could hang some of the other work that exist like the OTA and technical standards. We could hang those within the domain of what is going to be produced as the output of this process.

>> [Indiscernible -- low volume] I am reminded of the fact that years ago and perhaps even still ever tends -- advertisers reverse engineer updates to figure out what the exploits are. So tossing that out there as a consideration with software updates variety especially if devices are much smaller and the code might also be smaller.

>> Something is running through my head as we do this discussion. Watching out for some unintended consequences such as what he just mentioned. I have had conversations with other people about installs, upgrades to firmware that broke something that works. Undefended consequence of patching security issues are fixed in some other bug happen to break some desired behavior. There may be other unintended consequences. We want to keep our eyes out for those as well. This may tie back to the ability initiative we are talking about. From my perspective I think one of the factors to be successful is the responsible disclosure practice set up by different stakeholders.

>> It is all interconnected. Who knew?

>> The whole idea of vulnerability disclosure in this environment is going to be very important. As we're looking at companies who have never understood what a security researcher is an all of the sudden have to deal with them. As we're talking about security and upgradability we also have to educate on reasonable and responsible security practices. One of the NTIA efforts is a multi-stakeholder process going on right now in conjunction with NTIA. It is interconnected. This will have to be a part of that.

>> For those of you who would like to learn more about other products from NTIA including the vulnerabilities disclosure process feel free to chat with me after today's event.

>> Just to follow up on that. One thing NTIA could do to add to the discussion would be to highlight some of the barriers are obstacles creating some of the problems that people are perceiving. One of which is that fear of adverse publicity, also litigation, the stock shorting manipulation recently. All of this goes into an ecosystem problem about how you deal with

vulnerabilities and this overhang of the potential for litigation. When it comes to questions of when to patch, how, what are the triggers for needing to. There's a lot of complexity that I think NTIA could help clarify without offering solutions and also identify some of the obstacles that currently exist in the legal regime and the public discussions of these issues that made the contribute to some of these problems.
>> What would that look like?
>> There are obstacles to communication about vulnerabilities because companies fear what will happen to them and if we could take some of the basis for those fears away you might have more robust communication. I don't know if this has come up in your vulnerability disclosure setting, but those anecdotes out there are -- are chilling if you're going to get sued by a class-action group that is going to say your product was defective because of a latent discovered vulnerability, what does that look like and how does that affect the incentives to address the vulnerability and talk about it publicly. I think that is a challenge that policymakers have to keep in mind that the private sector whether talking to the government or public, there is something that folks are going to have to keep in mind as a figure out what to do about software vulnerabilities.
>> I want to hear if there are any reactions to that, but first I want to clarify that the outcome of this project will not be NTIA says. It is going to be stakeholders to participate in a process convened by NTIA that was open, transparent and consensus driven site. -- Say. So whatever you would like to say, this is your chance. So try to say convinced the room full of people that this is something that could really help the security of the ecosystem. If folks have both on that we can make some real progress.
>> One of the things that come up a number of times is this question of scope. We have some folks saying let's focus on a small subset. Some said we can incorporate some types of devices or applications that may be regulated, and then others have said let's actually go all the way into any setting or connected device setting. Do people have thoughts about how we should scope or when we should make that decision?
>> I have said a lot. So I will ask a question instead. I asked it before but in a rhetorical sense. Would we see it as a success if the outcome here that we define only applies to one segment of the IOT market and breaks when we apply it to another segment of the market, or multiple other segments of the market.
>> I love the question. Because it is not exactly a loaded question, but I think you expressed an opinion before that a broad scope was probably better than a narrow scope. So I am going to offer an alternative point of you. That is that getting something that works in a narrow scope and could be copied or modified to work in a broader scope is a way of doing it with training wheels. When we think about the size and scope of the problem that we are facing, it is pretty big. If you look, there was a bot net level XXXII weeks ago that came up again, and this particular one is based on a device out of Taiwan and is deployed, it was sold and deployed in Brazil and Colombia and Taiwan and India and Russia. The United States deployment of this is relatively small. The overall scope that the US government, that the US manufacturers, brands, retailers, consumers have over this particular part of the problem is relatively minor, and yet it has a big impact on the Internet. So going back to the original question, we cannot solve this whole problem with a broad solution. We can deal with an aspect of it. So I would suggest going smaller and dealing with something where we can get a success and possibly take some

pressure off and look to grow that into a larger solution rather than try to start with a very broad solution and get overwhelmed with the many problems coming in from automotive, consumer electronics and someone.

>> We can do that way, but the problem is, let's say if you take a thermostat. At home it may be okay, and now when you put it in the building or a factory automation, it is slightly different. For example, you only want to consider this for home automation and not address for the industry automation. Or for the factory automation. How do you distinguish? [Indiscernible -- heavy accent]

>> I am going to dodge the question entirely. I do not think that is the right way to view this. Forgive me. The challenge right now is to say, let's take any size segment. You are arguing for a larger segment and I am arguing for a smaller, but the premise is how do we enable upgradability for [Indiscernible] industry. We don't have all of that put together yet. Single companies have solved this, but we don't have it for comprehensive groups. So finding solutions for comprehensive groups and then broadening the groups I think is what I am suggesting. I could be wrong, but I think looking at it and saying how do you take a bunch of competitors and get them all on the same page in terms of doing patchability and find a solution all the way through to the end zone. Had you get to their? Doing that without trying to deal with a global problem come across industries, the difference of regulatory regimes between automotive and communications devices and home electronics.

>> I think my concern, and I am not from industry so in no way, forgive me for making a broad common, I am concerned that if we pick a narrow case, companies are going to try and categorize themselves out of that standard. So if we decide we want to do something specific, start with thermostats and say all thermostat for the company save -- will say we work in corporate settings so we don't apply to these standards. It is concerning that something there were no will ensure that -- narrow will ensure that it is a goal of people who make these products to not participate because it is not valuable for them. So that type of scope might mean that these are only voluntary to a very small number of organization to cannot find a way to make themselves not part of that category. People who work for companies, I am sure that all of you want to be engaged in this process and that is why you are sitting in this room, but a lot of people who would have trouble meeting the standards are some of the most prolific IOT devices are things I buy on kickstarting. The ones that are exploding into more devices are the things I buy to try to find my keys not something created by a big consumer tech company. My concern is by creating something very narrow it will not be relevant and we're going to put ourselves in the position where we end up having this discussion again. I am not opposed to the idea of a test case of here is a broader set of standards that we get for a specific set of companies were going to try implementing the standards, but I just worry if we say this does not include cars or medical devices or all these other huge industries, you're going to be leaving the implementation of the standards to people who do not have the technical capacity to whereas the big companies here are the ones who have security researchers and test their software and might be the best want to try and help implement these type of standards as a test case.

>> We have a bunch of comments.

>> I will make a couple of general observations and then ask a question. I think a of couple of different, I know people talked about standards but this is not a standards making process.

There is also not an enforcement mechanism. So it is not about forcing someone to do something. It is completely voluntary. I think that a lot of that is looking at, here is how updates would happen. Here is the mechanics of this. We expect this to be what you do and here are the thresholds that you must meet. So that is one mechanism and one way that this process can go. Look at the mechanics, look at thresholds, and the other one is to look at the categories of things that we want. What are the outcomes that we seek? Or the types of outcomes that we seek, such as, we want to have a public [Indiscernible] of how long something will be supported with updates. I don't care what the length of time is, but I care that manufacturers talk about that publicly about that they have some type of public commitment. And that is much more flexible. I think that is probably the breakdown between taking a narrow case and taking a broad case. When I argue for the broad case and the inclusive approach, I am saying or asking us to consider what are the types of things that we should consider, and then within those, each individual industry can absolutely define their own because it's not going to be the same for nuclear power plants and for kids toys. So there's no way that you can have one thing that would encompass all of those if it's a, here is the threshold. But if it is here are the things that should be considered, that should be discussed, that should have some type of a commitment or have some type of a public statement, I think that does work. If one of those does not apply to a certain industry, then it is all set within that industry. But we can come up with a superset that are all the things that anybody who makes IOT might have to consider. So my question I guess than is, is the intent of this process, to come up with something like minimum thresholds or is the intent to come up with something like the categories of things that should be part of the consideration within private enterprise as they go to look at updatability? [Captioners transitioning] I will be quick and then over to the side of the room. It could be my misunderstanding but the way I look at scope is not so much how many industries were talking about but I am thinking of the aspect of the topic we are looking at and the scope could be additionally we start off by looking at a product on the product still being maintain and there is issue and what do we do. That is how I will look at it and there -- we will scale up from there because from their IRT is a new and so expert and may not knew everything about it but for us to picture -- focus on the picture of what might be too naïve because they would be summary problems that so many [Indiscernible - low volume]
>> Thank you.
>> Erin for Microsoft since I'm in the corner I will stand. I like were both going at the conclusion of the last comment about essentially channeling your words a little bit but sort of describing desired in states, if you well and the kind of things that we want to see almost regardless of industry or sector with regard to upgradability and patching, practices and commitments and so forth. I think that is a reasonable place to go. To the women's comment about industry scoping themselves in or out or whatever, yes, surprise that is what interest he tends to do speaking from industry perspective but I think this is a nonregulatory paper, not even necessarily policy recommendations, a starting point so from that standpoint I would not worry too much about persons carving themselves in and out [Indiscernible - static] I think if we kind of end up going with Bo has described, not the kind of thing you get scoped in or out of, side of stands out as its own independent bar if you well.
>> I like were both was going with that and something we would be supportive of and could contribute to from our perspective which is largely on the network back in the side supporting

large-scale enterprise deployment as opposed to the consumer and where we do not have as much engagement.
>> In queue. Want to come our -- come over here speaking of regulators and speaking [Indiscernible - static] police often like to work and frameworks that are not [Indiscernible - static]
>> One question I have, maybe this ties into what always say a few minutes ago, when we did the NIST framework the focus that NIST with that higher-level around what I will call more process oriented types of steps that could be taken and so is there a way to develop a framework that and set of drilling down on one particular solution set, as was said earlier, folks could opt out of, could you develop [Indiscernible - low volume] process in think that would apply across the board and it could be things like have a security plan or other know what they would be but macrolevel they could be really simple things like have a security program, have a person in charge of the program, have an idea of what -- how you're going to do security, do not have to tell people exactly what to do but if you got security to be a priority at a process level inside some of these firms, that would then presumably, go higher to people who are security experts to build into their products [Indiscernible - static] that could apply the matter what the solution is.
>> Great, thank you. We can just make sure -- we will divide Tom and Darrell into lots of different pieces and spread them around.
>> Great conversations, I hope I can [Indiscernible] on the topic, companies defining themselves [Indiscernible] I think that speaks to one of the goals or object as I would like as an outcome from this. Whereby an outcome is not just methods for companies to use for example make sure they have secure updates but in a way that makes it so there companies are incentivized to actually fit into this set of -- incentivized to adopt the procedures and on the topic of this and I think it may have come up already but what's helping incentivized companies to jump on board and use the secure updates, having whatever we recommend not to [Indiscernible - background noise] Achievable and so on. And then on the topic of scope, not sure exactly where I spent [Indiscernible] have a broad focus but I would just say based off of test expenses it is often a lot easier to make traction when the focus is small because it is very kind of clear and of what is within scope and what is outside of scope in terms of technical choices, but once we start to be too broad we could spend whole time tying -- try to generalize [Indiscernible] not much impact that we want.
>> Andy?
>> Thanks. I think that there is an agreement that these winds are something that we are looking for and probably voluntarily easy wins are something that also show that there is a benefit to this process. And there is a buy in from many different interest his. It seems like one of the easiest level decisions look at what people have said is sort of a transparency reporting as an idea like we went like companies to make it public available how long will their devices be available and how often the issue patches and that type of information that could be provided basically saying this is what we are doing to a set of questions it would be great for consumers to know and understand, could be a big first step that at least helps build public trust or understanding without companies having to take steps are industries at all having to take steps to move further. So that all manufacturers of certain product will be able to say this is our timeline. And that is a huge win that we could have across as a voluntarily think that would

make your company look better and maybe more attractive to customers, that type of transparent information.
>> I see some folks none, any particular response to that?
>> Please.
>> [Indiscernible - low volume]
>> In some of the things already reporting those things happening for example [Indiscernible - heavy accent] What is the call, ICS sort, there is a program where all of the vulnerabilities, especially in critical infrastructure, that are reporting and it is happening so if you go to the site and you see what are the PLCs on interest in system [Indiscernible - heavy accent] Everything is dead. So same way there may be some mechanism, may be required, to other sectors also, we need to find out how a recommendation from our [Indiscernible - heavy accent] I'm not calling it [Indiscernible - heavy accent] Some monitoring agency can take this as a point.
>> Please.
>> Introduce yourself.
>> Yes, hello everyone on Dr. allowed the party I work for Hewlett-Packard enterprise. I was listening to many of the comments about what interest you would do and I guess I am representing interest here. As you would expect we have a history from the data center side of the world and we have slowly try to come onto the edge much [Indiscernible - heavy accent] Who are trying to introduce a new class or devices. I just want to bring up if we -- it would probably make sense to discuss about IoT -- IRT from a focal state [Indiscernible - heavy accent] Everybody can agree to that. States one would be the actual sensor that I talk about, and I am not talking about a smart sensor. A smart sensor it just might broad definition and opinion here would be something that has a Mac address and essentially needs its own network but many different sensors which is just brought devices, think of like a [Indiscernible - heavy accent] Sensor which all it does is it gives you voltage value, does not have identity of its own but just a Mac address. That is what I'm saying as a sensor. Next thing I'm talking about, next level would be what we could call as a data aggregator. Or essentially something which is taking the raw sensor value and getting it an identity. Think of it as a microcontroller or in many ways but we are also doing now as an educator, potentially could have [Indiscernible - heavy accent] On it and actually converting and analog value into a digital value.
>> And potentially doing it across a large number of sensors. When you think about smart sensors, actually convergence between stages 1 and 2, where the [Indiscernible - heavy accent] Also on the device, it is fits together with a sensor, and I think we were talking about smart thermostats and so on. If you're talking about both of them being aggregated together. For the four stages let me go to the next stage which is stage III would be where you could potentially think up doing some form of [Indiscernible - heavy accent] We talk about conversion IRT [Indiscernible - heavy accent] Actually happened right at the edge before it goes off into the data center.
>> Stage IV would be data center [Indiscernible - heavy accent] Whatever you call it. So if we think along these 4 lines, you would say especially along the context of security and update ability, I think it will be easier to go map out whatever existing technologies are there which would apply into these existing spaces so what I can think as one of the designers of say edge computing systems, because we have heard from years of experience in the data centers all of the goodness of many, many years of expense, there in the data center, is now available on an

edge computer device, when you think about [Indiscernible - heavy accent] Or from many of the competitors easily have all the form of update ability and security update abilities [Indiscernible - heavy accent] Not claiming it is not necessarily perfect but what was out there, is now available on stage III.
>> To some extent beginning to happen onstage to [Indiscernible - heavy accent] Other people probably are so maybe take her go from the right to the left and start trying to adapt goodness which is available in the four states ecosystem.
>> May I sort of take this as a really helpful model, can you map it back to some of the consumer space devices that we haven't talked about? Data say a home alarm system and a car.
>> Yes, when you are talking about consumer space, is it a home alarm system. I am thinking it is basically a short-circuit between one directly to 4, do not necessarily have data aggregate -- you may. When you say home alarm system, basically connecting onto something so in a way it is the data aggregator but in certain other cases you could probably just have it connect directly onto the cloud, many of the NIST devices for example. All I'm saying is you can convert pretty much everything into the 4 stage ecosystem and then just basically talk about what can be applied where, depending on what the industry would do because I think this is to general to escape any particular reality circumstances.
>> Mark, and then sushi.
>> This is really a great discussion and I have been trying to wrap my head around how to take all of these different kinds of points and get back to something that is actionable at the end. I made a short list of things that would be kind of cool to have walking out of here, one of them is a list of barriers to the process of consistently and reliably upgrading devices. And what could be done about those, recommendations to remove various. So that his first category.
>> Second category is identify ways to enable industry to solve this problem more quickly, more efficiently, faster, whatever superlatives want to put on there. And those would be things like consumer education, installer education, able to install Internet and these devices in a professional capacity are also a candidate for that. Identify consortiums that might be needed. Identify subject matter experts they should be brought into the process. Another element is I mentioned before the global nature of this problem, who is the responsible or the like to party in the United States that would coordinate with other governments or [Indiscernible - static]
>> Which of the problems that you would want to dive into.
>> [Indiscernible - multiple speakers] I love the list as well, just plus one for everything said there, to add to -- few items of my own list of things to think about. One of which is there is a lot to be said about updating a device before it is compromised. But to the extent we can, thinking about what mechanisms can we also ensure ability to update the device post compromise and of course he might not always be able to do that but that is something I would like to be thinking about.
>> The other thing that I would go out there is as perhaps a requirement for any software update solution is explicit naming of what all the dependencies are. For example of a software update solution is a signatures ability might be on under [Indiscernible - static] losses to know if there's probably with this thing upon which we are dependent, it provides us with more information so explicitly calling out dependencies. And then in case it was not mentioned already, I would like to know there are -- sometimes it could be vulnerabilities in the hardware

level that we just cannot fixed with software. Classic example of being I channel [Indiscernible - multiple speakers] into the hardware, that is picked in. Such as noted there are things like that. Out there.
>> Any thoughts about where you would like to head based on where you think this is going?
>> Please.
>> I would just ask a question back, as an engineer, my brain is always getting frozen, when we talk about obtaining device. I think in general I decide what we are talking about but I think it would be helpful to be a little more specific on what the device is, if I was to go back to what I was talking about the 4 stage ecosystem and I think of the device, I am thinking the device that is the sensor plus the microcontroller and essentially when you say updating a device that is what I think about, basically updating the microcontroller as a flash code, basically updating [Indiscernible - heavy accent] Is that what you necessarily are talking about? It could also mean your updating the firmware of the computer device so that is what I'm trying to go back to be more specific on what the device is. All of them are potential applications and updates would need to be done or security vulnerabilities would actually need to be addressed but maybe it a point where -- each of the devices.
>> I think I could not agree with you more in the sense of calling out there all those different places where one might need updates and insane some of the things I've set already, I suspect others too. Not picking any type of technology but us point out anywhere there is edge of vulnerability, there's opportunity or perhaps need to do the update. And then on the topic of and I forget where was, updating device, before [Indiscernible] question we might have is what is the trusted computing base necessary for the update? Can we minimize that trusted computer base for the update so something is compromise outside of the PCB, we can still do the update, that type of question.
>> And distinction that might be helpful in the report this morning that Olaf mentioned, building on work that ought to be done, is the IRD report distinguishes between class a devices and class letter map -- M device, having a [Indiscernible - static] fully implemented stuck so you have ample memory to do stuff, think raspberry pie, right? General-purpose computing mechanism and class C is much more constraint, without having to be very's best -- specific about how constrained it is not going all the way down to single transistor sensor but someplace that is [Indiscernible] might be useful distinction if they want to still talk about devices in some fashion.
>> When you say take a class M device, not too familiar with the classes, you -- renew you are saying update from class of device, engineer speak, will with it turn out to be? Essentially boils down to some bits on programmable part somewhere.
>> [Indiscernible - multiple speakers] [Laughter]
>> At the end of the day we are changing bits, yes.
>> This is a very good point. There is fortunately a four layer classification, like a pyramid scream -- scheme at the bottom or very deprived devices many memories, where you both 16 kB or less would you could put the but not that much, you could put a certificate on it but not much. Then there is the small -- so I am talking about the lowest layer of the pyramid is 16 kB devices. Because you really need memory to put not just the security stack, something like operating system which is very important, right?

>> And then the next layer is called small and then medium. And small is really between somewhere about 250 kB and then there is medium where you are talking about something like you want to put a Linux operating system or our toes operating system, you're talking 15 make about and above -- 15 make about and above, and the large is like laptops desktops the we will worry but it, right?
>> So the challenges down the lower Lail -- later. What can you do with sitting kilobytes? Not much but you could do a lot with the 250 kB. So just come back to what I call court -- you need some kind of core standards or core maybe Internet like downloadable code for all -- most of the application [Indiscernible] and if you focus on 250 kB and you start to do something like lightweight encryption, right? Something like lightweight authentication, something like the equivalent of lightweight TLS which you [Indiscernible] something like secure [Indiscernible] which Intel was talking about and exist today but it is expensive. Compared to the cost of a low-end device. If you focus on these, I claim this is a very generally [Indiscernible] expand all those domains and if you do it in the public domain and companies can use it, just like the Internet was born, that will take off.
>> May I speak a second?
>> Sure.
>> For example, service, -- I guess I'm trying to distinguish between -- bring them into context. You said 16 kB memory as an example, [Indiscernible - heavy accent] Spy devices where the bios gets loaded, right? So it is not that far away. Yes, you need megabytes we larger. But that is it the forward level due but servers for example you also need to have servers -- anything else which is running in our toes will also have the OS update going on. There are really two things which are happening on a server or on an edge computer system. As you started bringing them onto the left-hand side of the domain. I agree it is actually a small devices probably more challenges are but all of them can be mapped into the four stage ecosystem, right?
>> I want to see if there is any interest insane okay, here is a class of devices that might be interesting, just a quick clarification, is the 250 6K memory size, is that a formal distinction that we can cite someplace?
>> I think the Internet engineering test has a old Argosy [Indiscernible - low volume]
>> Is there some interest in least carbon that out as a particular area of interest in order to carve up this problem?
>> I think to your point, open-source, make it accessible -- work on the problem, come up with a solution and make that available to these vendors because I still keep coming back when I am looking at the consumer side of this and my head going I see no market reason for me to ever secure my product. It only cost me money, consumers generally will not pay for it or do not know the difference and they go for the cheapest thing and that makes me not market competitively. If I can get it for free, I know there is this data can implement and instead of just grabbing to their clinics today with [Indiscernible] slapping it into my device, if I can choose the equivalent of that, that has been vetted by some experts and energy and effort has been put in and maybe that is interested consortium that gets money from some mentors [Indiscernible - static] make it available then I think we're starting to make some progress because now I'm going to take the cheapest free thing which is generally clinics at the thing is big enough and just put it on there with all of its words and not have any understanding that Jesus there was a

root is HKEY from that type get hub and it is in all my device is now, right? We need to get beyond that. But the free, has to be free.
>> [Indiscernible - low volume] expect Olaf first.
>> I want to drive the point first, free and open. If you do this an open letter, this will be -- have a transnational effect were operating in a global market, if you drive the price solutions down, be it in global standards, but with open source solutions, are those type of things, I believe these things will be adapted. So that is making sure that these standards are freely available, making sure that it is international context, [Indiscernible - low volume] one venue but not the only venue to do that.

>> Just to clarify, it has been great to hear the emphasis on having this be a global issue, razor hand if you work with an organization that has a global presence.
>> So I think we already are at least in some ways capturing a global perspective. [Indiscernible - multiple speakers]
>> It is wonderful, I think is spectacular to emphasize and for those of you that did not get shot in the whites and Nvidia almost everybody just raise your hand to sort of underscore the idea if we can come up with somebody useful -- something that is useful it will put the nature of its participants have a global reach. And you and your partners and industry are also going to continue to have that emphasize that as a global issue. Going to Erin and then [Indiscernible - low volume] and then you she.
>> Erin does not have a mic.
>> I will say, very briefly with regard to the global nature and sort of how this will be received and I think perceived also, in discussions with foreign governments about IoT security, because the US doesn't have a national strategy for IoT like Soviet countries -- not directed -- it is a factual observation not a common. It is objective critique, because we do not have a national strategy for IoT, and there is not really a policy document on this at the federal level, this will be essentially in addition to what the FTC and others have done, kind of a more forward living thing for the [Indiscernible - low volume] and I think other governments will immediately be interested in what is produced here and I think that we should be cognizant that other governments are not necessarily as inclined toward multi-stakeholder is of an nonregulatory approaches. And that should inform in part what we write and what we say as part of this document because it could easily be transposed and picked up as more of a compulsory or even a formal regulatory regime. So we just need to be thoughtful about what we are saying, commitments were willing to stand by if you well in other markets.
>> Thank you, great comment.
>> I have two things, one about the global stuff, I want to give you an example, [Indiscernible - low volume] [Indiscernible - heavy accent] Working last two years, [Indiscernible - heavy accent] European Union was doing the same thing, came together and there is a giant task group now to leverage the works of those things will happen automatically, one thing. Second thing about this comment on the pricewise, [Indiscernible - heavy accent] $30, [Indiscernible - heavy accent] But still people go for NIST $200, that means there is a market for that. There is a market.
>> Yes, so, [Indiscernible - heavy accent] $30, 40 telephones are gone and now people go for $600, 700 telephones. But people are willing to pay for the value that offers.

>> Quick response.
>> My response to that would be it is probably similar to the whole macro ecosystem, people are choosing NIST because it is a system and polish and easy to use and it is beautiful and widely available not because it is secure. My friends buy it because it is secure but I don't think they are typical. [Laughter]
>> [Indiscernible - low volume] expect --
>> Thinking as a global perspective reminded me of another topic I want to throw out there is potential requirement but then again as you probably inferred right now to out a bunch [Indiscernible] but that requirement I want to suggest was resiliency. In the sense that again related to the notion of dependency, what does the system depend on in order for the software update to occur? If that dependency or fragile or resiliency is fragile than that also becomes pitch point with the adversary will focus on that. So one example would be software updates. The sales are and DNS goes down and cannot reach a server that none of the devices will be updated to not only provide a mechanism to update but ensuring update mechanisms have some level of resiliency.
>> Want to make sure we are hearing from all the voices, anyone who has not contributed recently who has some thoughts about how we can manage this complex conversation? We have talked about looking at very small devices, that do not have a lot of technology available but on the other hand may not be greatest risk point. On the other hand we have the complicated devices that may have more ability to engage in upgradability, we compose more technical requirements. Anyone have a sense about whether we should try to focus on one or capture both?
>> Yes?
>> I just want to say anything that comes out of [Indiscernible - heavy accent] And up necessary being technology neutral be on factors like to be voluntary. Just saying it is very easy for all of us who are in interesting to sort of get biased as to what we may have done from our own perspectives but whatever -- to move the ecosystem forward which would really be necessary is to be technology neutral and prescriptive at the high level.
>> I don't think you would get on argument from an ITA about the [Indiscernible - low volume]
>> I want to reiterate again, I think we need to look at what existing efforts are out there, it might be good to have a working group, a few people in this room who are participating in multiple ones of those efforts already, and it might be beneficial if we could come back and see what the state of the art is before we go of creating something from scratch.
>> Say a little more about what the -- you imagine the outcome of that issue would be.
>> The outcome would be sort of looking at from the standpoint of what are the general requirements that we would expect out of any vendor and any level for security and upgradability, patches and the like in the IoT environment. And then coming back and take a look at my ACO, CF, other efforts existing in the community, trying to determine what they have already done, and if they have done things in this area, that is a real positive we can leverage it, we can utilize it, we can highlight it. But if there is the work that is being done specifically in this area, that tells us we have a bigger job in front of us but we do not know that today.

>> Excuse me for trying to nail this down, you're looking for the superset, all the things it could be done even though it is entirely possible that no single class or no single device could -- all could apply, right? Split that's correct.
>> Any thoughts on that particular idea?
>> [Indiscernible - low volume]
>> Let me bring you the microphone.
>> Thank you. For patching, obviously there is something called Oma DM open mobile alliance. They do a lot of this, [Indiscernible - multiple speakers] they own this thing if you well. But the carriers including when I worked for, I mean, that is where the action is.
>> For the mobile platform?
>> Yes, yes. But you are right, there is tons of consortia standards, some overlap of course that might as you know. NIST [Laughter] as you know. I like your point. There is no point trying to replicate those but I am not familiar with -- the I ate TF is very active [Indiscernible - low volume] to go there but it is too big.
>> There are some very large consortium [Indiscernible - low volume] expect we would be happy to share the preliminary work that an ITA has done gathering [Indiscernible - low volume] Vick and then in the back?
>> Thing to follow up with Ken comment another working group idea may be to look at the incentive or look at why it is so many frameworks but are we moving ahead? I don't know you can tell me but [Indiscernible - heavy accent] Not moving head well enough so we need to look -- why are people not adopting these, what is preventing them from being the first stakeholder to take it up?
>> Great.
>> Yes I only -- also like the idea of what others have done on the Society of automotive [Indiscernible] one of the things I think we suggest we do if we do that is look at went different groups have made different decisions and to understand why because it is that those points were different groups make different decisions that we might find knobs to turn and so on. One other idea want to go out there and this was something said earlier about which companies are participating in this and so on the smaller companies as well, if there is a role for shared infrastructure for doing software updates, infrastructure that startups can quickly jump on that would enable them to participate more rapidly, without such a big barrier. So in this kind [Indiscernible] Constable of resiliency in the [Indiscernible] that shared infrastructure could be made highly resilient.
>> [Indiscernible] to propose working groups.
>> You totally hacked my brain because [Laughter] I was about to say that. I have another point I want to bring out is that as far as incentivizing companies and individual developers and nonprofits and all those people to adopt some kind of labeling thing or whatever, like some kind of like motion that yes, we have these updates on this is how we get them and all that, we still live in an era where we don't have any software liability but we don't have any real practical software liability, some industries are regulated that it than others but because you don't have the software liability issue like I can go and sue people because they should [Indiscernible] having this kind of labeling may help stave off software liability so for the purely self-interested companies that do not want any regulation on software, having this kind of

promise that there is some update ability may help bolster their cases like yes, we are self-regulating industry and we do not need your dirty government hands all over my software.
>> Just a thought but what about a working group to explore exactly that type of thing? A lot of discussion today about labels and certifications but what about a working group to explore pros and cons run issues of coming up with labeling or certification type of thing and ties into my earlier comment about developing macrolevel principles that could apply across the board and could you come up with and I think this is a good idea have not put to it all but could you come up with a set of basic principles could apply across in the IoT device if you agree to the principles you would get some sort of labeling or some sort of indication that you were at least in its ultimate security and could be process oriented as opposed to be being really prescriptive so maybe just there's a particular group to kind of explore issues around that type of model.
>> I like that and I want to ask a question of you and fixed, is that the same thing as incentives or do you think that labeling is a distinct and efficient you want those to be separate discussions?
>> I think the incentives would be around how do you get people to actually implement the labeling and other part of it, right? Maybe they are intertwined it may make -- [Indiscernible - low volume] expect separate issue.
>> Can't and then -- Ken and then Vick.
>> I agree with Chris, I think having a labeling group where we are looking at what are the specific that you would want to try to make sure we are indicated and what are the concerns of the product vendors need to be aware of, it goes a long way towards getting them to think about those things beforehand as opposed to after. So if we had a working group like that it could be beneficial to us to actually come out with something that would be potentially usable.
>> Ken if I could push you long that, how do you see the work of the labeling group playing with the work of the -- what is the space of available tools?
>> To be determined, I don't have a good answer for you. I think that is something we would have to figure out where applicability was and to what level you want to take that. Taking again Chris's idea of doing it from a component application perspective, hardware, network, component, application perspective, you may have different applicability spare. I do not like one size fit all kind of solutions, but I do think there is value there.
>> [Indiscernible - low volume]
>> I think those issues are intertwined because when I think about it if we can develop a sort of first principles that you [Indiscernible] source that off of existing work, right? So I think you would want to go like the SMA, work broken down into two categories imagine and would want to go to any other -- I could name any other [Indiscernible] as Brian mentioned is [Indiscernible] you can pull a lot of different standards to get and save these are the types of things but I don't know that we want to get down -- my vision would be it would be a little higher level than really this of technical standards because I think that gets you into the role of if it is this device, it should have these requirements and I think you keep it high enough level that it is process oriented but within the framework we did there is came up with high level categories and subcategories, right? And then the actual standards were informative references so we did not say go to ISO 27 about [Indiscernible] we said you do you need to do -- you need to have a process for -- you know access protections or whatever. And it let people decide which one

they want to you so I think you could do something like that and source it off existing documentation.
>> Thoughts, we have a couple of voices here.
>> Introduce yourself.
>> Craig drummer, to source labs here in Austin Texas. I also want to throw out there, possible working group we may need to apply to this. Stewardship of the data, collected during this process. Just to throw that out there.
>> [Indiscernible - multiple speakers]
>> For IoT so whatever company you are you are collecting data from these devices and it is in your cloud, how is that taken care of?
>> All right.
>> For the people talking about labeling specifically, do you feel that is a solution to the consumer education problem we have been talking about, lack of understanding of these issues IoT devices? Do feel like there is a separate conversation about consumer education?
>> [Indiscernible - multiple speakers] couple of responses. One and two and three.
>> This is Brian with CTIA, I think it can help but maybe this is part of what Chris intended, you asked about incentives, I think that is part of what you discuss. Labels are not a perfect solution either so that tells you you go through pros and cons, there's a lot of experience with labeling things and certification programs, so that is what we would want to flesh out I hope in the kind of discussion, how can this be coupled or show to be coupled to consumer education campaigns and who with but partners that could get messages out to consumers?
>> Just Adam, exactly what I was thinking, we would have to do exploratory group to look through what would it look like, 80 it is something similar to what trustee does for privacy, not sure if that is a great example but it should be something that should be explored and other no -- I don't professor one day to have an answer to a complex issue but we get a group together that can talk to the pros and cons and issues around the and how it would work a lot with the in incentive structure been try to keep the first principle level and get something like that done in 6-12 months Windows.
>> The challenge -- with the generation of the principles be in that working group as well or with we need a separate working group for that?
>> There has been a lot of conversation today about -- buyers are never going to be -- to care about security. I think that that is right in the sense that they are not going to care about security and be knowledgeable enough about security to discriminate against -- between different security levels the way that we do, as security professionals. But I also do not think we need to make it, in fact I want to be less security conscious and want to have to be less security conscious so if I go high a device I want it to just do certain things, right? I think when we talk about the labeling discussion and awareness, a lot of that is wrapped up in not making consumers were knowledgeable about what we care about but using the language in a label and then awareness to tie directly to them so for instance, use this example come up [Indiscernible] I think buyers care about downtime of their fleets. So if some part of a label or an awareness campaign for public attestation is you should expect this vehicle to be out of service today set of every month, that is something that care about. They don't care about the security of of it but in order to maintain a secure and safe vehicle, it has got to be out of service for this much a month and that might be time that they are accounting for downtime too. So

does not necessarily mean that is extra cost to them making them aware of the things that they already care about and tying that to security is a way to reduce the impossibility of the task of getting the public to care and to choose based on labeling.
>> And that makes it a lot easier, 24 months, support for a Google phone, is a good thing. Users a good thing to know that. -- It is a good thing to the. I remember Motorola without a phone and said they would supported for six years and three months later they said just getting no more support for that phone. And think about the signal that sense to the market. You put this fall because he thought it might last three years and maybe but for your mom so you don't have to constantly fix it and take malware off of it and that kind of thing and now you have to go back and do the same thing because they broke their commitment.
>> I think those types of things can -- will be meaningful to consumers even if it is not every single consumer. Even if it is just the subset of consumers that want to inform themselves. Giving them a mechanism to be able to do that and to make it a more informed choice allows the market to service itself to some degree.
>> Quickly here and then Chester on the back to you and that we will say goodbye to her friends heading onto the flight to DC.
>> Can jump in?
>> Please.
>> I just want to say back to the class discussion that we had before of the type of devices, I am seeing there needs to be a set of working groups for each class device, I was talking about stage of the ecosystem. Sensor, aggregator and so on. There needs to be working groups to basically bring out the maximum capability with no technology, at each stage. For example smart sensor can potentially do this and everybody will have different opinions, but something has to be done to say what is the maximum known capability for a smart sensor? And then [Indiscernible] what is the barely minimum acceptable capability as far as security an update ability is concerned? Does need to be done as separate working groups for each stage. Something [Indiscernible - multiple speakers] smart aggregator or something for a smart edge computer device and something for what is necessary to make data center. -- [Indiscernible - heavy accent] Minimum requirements of that would basically be a [Indiscernible - heavy accent] Today's no technology here is what we think we can do okay fine. Minimum requirement, every device [Indiscernible - heavy accent] Given label which can be done separately should potentially have at least [Indiscernible - heavy accent] That onset is going to defer it because like he was saying something which has so many kilobytes of updatable space will have only a max capability of so much, no more and there is no point in play that standard to somewhere else and that is probably where there should be different working groups for each one of them and depending on what people want, be able to do that, and how to match to others working groups which different people have proposed is that minimum requirement will give certain -- having a meeting that the number requirement will give certain security an update ability capabilities to each class of device, right? Which other working groups can then come back and comment on and say that is not acceptable, so then you go back and you don't have to go reinvent the wheel but basically go back and say my max capability was that and then I can probably raise my minimum requirements to the other working groups say it is not acceptable. I think that is probably a nice way to go forward.

>> I want to go to you but then quickly any responses or second that approach of a group that really focuses on understanding the maximum capability and minimum tech requirements? Anyone that wants to at least say about that?
>> Second, fantastic.
>> Do I get to tell it?
>> [Laughter]
>> Yes I like one of the bullets up there, not sure what it was like the to know how long the devices supported and in thinking about that, I guess I want to throw out there the fact that we explicitly again considered different stakeholder groups for example on digital divide, I will give an antidote that some of you may or may not know, is that many kind of the most frequent site that has malware on it is game sheet sites at least the case a few years ago, the reason being is that people searching for games, game sheets our kids and kids typically have parents second and computers when they come kids get new computer -- parents get new computers. Question is what demographics is going to be using these older devices, under no, not sociologists are soaking up [Indiscernible]
>> End of topic one, topic to. There are a number of things in the environment that we are used to bind and then throwing away at certain periods of time or hopefully consuming, food in one example. As IoT devices become cheaper and cheaper maybe even sensors and so on, not sure if we are just one [Indiscernible] kind of take it for granted that some devices we take and then throw them away every two years and have to get new ones. That we can also start the but digital representation so fruit that about if it is bad I know it because it looks multi-, is there way to convey information to users to know when that devices useless.
>> Like Washington, [Indiscernible - static] we will try to go to the phones and talk to Harley Geiger, patiently waiting.
>> Can you hear us?
>> I can. Can I ask you to speak with your mouth a little bit further away from the receiver because the sound system in here is a little messy.
>> Is this better?
>> Perfect, thank you.
>> Okay unfortunately I am not able to see the -- what you have projected onto the screen so forgive me if I repeat things ready on the screen. And looking at the purpose of this multi-stakeholder process, that was originally on the webpage, it noted that the goal was to be developing a shared set of definitions around security upgradability and ways to mitigate those features to consumers. And it seems to me that we have talked about a very, very broad range of issues and with regard to many different possible work products coming out of the so I would just like to give my very simple two cents about what an initial work product might look like.
>> Excellent.
>> I know this this has been talked about to some extent already, to the extent that folks of array talked about it I am simply agreeing with them, but I think that an initial work product that could work pretty well and may not be a huge lift, to security labels, right? Security label for end-users and this would be consumer facing and then checklist for supply chain security and I think that separate working groups would make sense for each since the supply chain

security checklist would probably be considerably more in-depth than the former, supply-chain security check list would probably be vendor facing.
>> For the consumer working group, working group working on a label for consumers, I think that some of the factors that up been talked about this for make sense like whether it is a device that is upgradable, shelflife of the device part of whether the vendor authorizes third-party to come up with security patches for example after the shelflife. Of the product.
>> In my opinion I think that some discussion of certification scheme -- seems somewhat premature as well as awareness campaigns because we do not have products to drive awareness on and there are already [Indiscernible - low volume] certification screens that are out there and emerging. As far as coming up with new principles for -- you articulation of principles for IoT security, it seems to me that there are a large number of standards and efforts already existing that do the same thing and I am not sure it would take [Indiscernible] or add to the complexity, I think they are the two separate sets of labels, might incentivize companies to meet the checklist, and to not have a label that says no, the device is not upgradable and achieve the original goal of communicating some security features on IT devices to consumers. Takes a lot.
>> Thank you, very helpful. I want to make sure we captured that appropriately in the room. Suggesting a set of potential requirements for consumer facing devices and one at the supply-chain side of things? Can spell that out a little further the supply-chain site?
>> So the reason that I think it would make sense to distinguish between the two is because I think the consumer facing label is likely going to be more of a summary, simpler, although I think it would make sense for a company selling IT product to also have a webpage that consumers can go to for more in-depth information. But if you think about the nutritional label model, it is something that consumers can look at very easily, like standing in the grocery store, because for some of these products it will be snap decisions, for some obviously it will not. And so I think that differs from the -- from the supply-chain checklist where a company is looking at some components of a product that they want to market and want to see whether those subcomponents include field upgradability and certain other security features. And I were just expect that a company in that position is probably going to skip over some of the summary information in favor of the more in-depth information [Indiscernible] but I think the language of the to labels would differ.
>> Fastening, thank you for putting the supply chain issue on the table. I think that is an important issue that has not been talked about enough today.
>> Any reactions to his comments?
>> We have a thumbs up. We have about an hour left and what I thought we would do is first review the different work streams that have been proposed over the last hour and a half. And to see if we can put some clarity into them, maybe develop a little bit of a mission to help guide each of those work streams, see if we can blend them together. And that the other thing I want to make sure we have time for is the talk about when and how we will continue this discussion.
>> Those of you have been involved in standards development or multi-stakeholder processes like this know that there are two parts, there is a lot of work that happens between meetings by dedicated people, and then there are these meetings which can be a little messy at times but also really important to make progress, to get feedback from our colleagues, and also to serve as goals to keep the progress driving forward.

>> You should also note there are going to be plenty of people who once they hear but the work we are engaging and are going to want to join and we will have to want to do designer process in such a way that it is not -- the people who are here, launching it, but we don't build it in such a way that it is exclusive. Doesn't sound like a good use of the rest of our time? Feel free to throw an interrupt and we can address other issues but looking at my list, I have a couple of different working groups, I have what we might call standards and initiative review, Kent, D have a better way to refer to this?
>> Existing efforts?
>> [Indiscernible - low volume] but summary of [Indiscernible - low volume] but --
>> Sorry we need to give you a microphone. Thank you for catching that.
>> Sorry. Yes, a summary working group that the summary of existing standards related efforts applying to security patching and upgradability and produce reports for interstate documenting the existing current practices across [Indiscernible - multiple speakers]
>> Great. We will come back to that I want to make sure I have enumerated them in such a way that everyone is on the same page.
>> There is a question on incentives. If we have some volunteer efforts, how do we foster greater adoption? Is that Dick, sounds good?
>> Eric is gone so we can say whatever we want to about his labeling idea. But I think it would be the notion of if we were to have a label what would be on that label and what would be the strategy of promoting use of that. Anyone have anything they want to say to help flesh that idea out a little bit?
>> Hang on.
>> My question about that is having [Indiscernible] what degree which you actually include user studies as part of the working group effort because I think to determine good labels requires a lot of user interaction.
>> I will speak for an TIA very briefly which is without a doubt we are now designed to propose a local by committee and certainly you know my background, firm believer of the importance of user testing. That said, one of the things that might come out of this kind of discussion is here is the base of -- base ingredients if we can find resources, could go off and do some proper testing, does that sound make sense to you?
>> Scores, please.
>> [Indiscernible - low volume]
>> Some of the people already working on such things like [Indiscernible - heavy accent] Why don't we involve those people and find out how this can be done very easily?
>> Thank you, great idea and was certainly talked quite a bit with underwriters laboratory, the broader mission for IoT security. And in fact one of the reasons we focused on upgradability is to complement that kind of work.
>> I think -- Holcombe encourage it? I would prefer to encourage adoption label and when I heard Chris I think I heard him talk about putting down the pros and cons of the label and how to understand those dynamics and that seems to me that is a solution, mace bearer will be and also think about that as an incentive space so if we are going to have incentives as a separate working group, then we can kind of part that adoption issues over there may be.
>> We think and unfortunately we are about to lose one of our advocates here -- we will address that question in a moment.

>> As an alternate maybe to calling it labeling, I think one of the commenting that of come out is there needs to be -- one of the common themes coming out today is there needs to be elements that are communicated out to whatever market you're talking about, whether consumer or supply-chain, so I think defining which elements those are is important, whether or not there is a consumer label. I think that is kind of what Allen was same as well, independent of what the label looks like and how it is packaged and awareness campaigns that go on, we need to think about what the elements are that would go into such a attestation, declaration label, checklist, whatever it would be for those.
>> I think that is a very good working group. I think that working group dovetails well with the standards and initiatives reviewed, although they are not necessarily overlapping, they have some interplay but not enter laughing.
>> I think that also captures what party was seen earlier, so let us go, one and two and three and four.
>> I wanted to point out the minute we talk about a label we are sort of implicitly saying that a certain device or class of device is meeting a set of minimum requirements. I think the problem is a minimum requirement needs to be defined first in that was my comment earlier about masking capability requirement from technology perspective is something that I think is open-ended because I think somebody could come out and claimed that it has to be done this way for smart sense [Indiscernible] not do it that way.
>> Gray, I want to get Beau, you have a strong deal of that [Indiscernible - multiple speakers] yes, I don't want to go to for it labeling but if you look at lichen ingredients list on packages of Twinkies, no minimum standards of standards for Twinkies, but the kind of minimum standard is that there is a label that calls out with the ingredients all right, so I do not think we have to define minimum standards to go onto a label, doesn't have to be a binary, either you have a label or do not. It could be something like we will support this device until 2025, right? Or 2024 or 2022 so you can -- tomorrow, right? You can come over the categories that come into a label and let every organization define how they want to work at that [Indiscernible - low volume] so I think the working group be proposed on minimum standards and call it leading practices, is also a good one because that defines the art of the possible sources.
>> Andy, quick response to that?
>> Okay.
>> What you said makes complete sense. What I am trying to just highlight is that when you said for the Twinkies, is set what is a shelf life or what is the support time, right? Implicitly what you meant. I am saying the labeling definitely could be done but it should be based on a set of capabilities or requirements that [Indiscernible - heavy accent] We can go on labeling things with capabilities and you said things you want to have a label [Indiscernible - heavy accent] Or vendor support, right? So [Indiscernible - heavy accent] Does not mean anything, right? So you give me a label and I say I plaster it on every device I haven't been it ultimately -- somebody else [Indiscernible - heavy accent] Everybody has a label but it does not work.
>> I think that would be something the labeling group with engage in so Andy, something you want to say?
>> I was just going to say I think consumer or concept of labeling or communication to consumers is one of the most important things in something we can do without defining internal standards. And that means that labels on certain types of devices would be more --

have more information or less information but I do think we can have that communication development issue without that working group deciding what is enough months or what is that correct amount of information and that could be a leader discussion but figuring out what questions need to be conveyed is probably the most useful thing that that working group can do.
>> Thank you.
>> Very quick to finger from Aaron and the back to Chester.
>>? Possible, yes, agree with the notion of focusing on elements and consumer awareness because labels from the perspective of the company that pursues every label we can obtain, the moment that you say labels we jump to the questions the gentleman is raising here which is okay with us in it and how do I get there and we want to get over every bar. So I think starting from the label is just a tactical tool to enforce but we are really after which is raising [Indiscernible - low volume] awareness and making sure companies adopt practices to raise awareness and meet consumer expectation so let us not call labeling up top because labeling is a tool that can be used to address the higher order bit.
>> Okay. I have a bunch of people waiting so Chester, and then Todd and then back over to the site in the back over to the side.
>> All around.
>> I will be quick, continuing on that and building off with Beau the same, I think where we say things like underwriters laboratories that is a big giant different -- different than laboring the barrier to entry for labeling is I just need to declare some truths about my thing like today you get something that says it supports 2.4 GHz wireless or it says it has a Bluetooth logo because it works with Bluetooth are the supports and right but not iPhone, right? There are things that consumers look for when they buy these things that does not cost money to do those things. As a certification program a UL kind of thing could take months to certify and tens of thousands of dollars and for $12 widget, you're just not going to do it, right? So to try to get everybody to come along you can at least you say can you state warranty, just do these few things to give the comparative label and not go all the way down the certification route for at least the bare minimum consumer kind of stuff.
>> Thank you. Todd?
>> Thank you. I am Todd [Indiscernible - low volume] I am super interested in the whole shared open update framework that you were start yes, you are talking about, I am super hot on that idea. I think that is deserving of a working group. Maybe a working tool, I don't know [Laughter] but yes, I do not want to lose that. I think that is kind of critical especially when it comes to things that are already end-of-life, is there a mechanism where you can kick these orphan devices over to this thing and you can at least send the? To it and of course I will hold all the power over the? And I am very trustworthy and that would be fine [Laughter]
>> Evil talked the.
>> [Indiscernible - low volume] I would love to chat after [Indiscernible - low volume] one of the things and topic of communication from the call labeling and so on and so forth, I heard the word consumer mentioned a lot and I just want to make sure as we go forward with the definition of what we mean by consumer and one of the things particularly interesting to me about the IoT environment is fact that there is both direct and indirect stakeholders so there is the individual who purchases technology he or she babysit person up at seven home for

example the home center but that device in the home will interact with many many other stakeholders, the children and parents and siblings, the people that come to send home [Indiscernible] for the question I have what do we mean by consumer and how do we think about communication in the context of both direct and indirect stakeholders in this type of ecosystem?
>> Thank you.
>> Before we move over there, there was one comment here.
>> From the CTA.
>> [Indiscernible - low volume]
>> Still trying on the microphone. Like Bergman from CTA and I will speak louder. Two points, one is on the incentives, I would suggest include barriers that part of the incentives, incentives as barriers. You want to create pool and eliminate barriers somehow. So as part of the scope of that. The second is are we now dealing with the security of the devices and not the patch ability? Because the discussion seems to have gone that way, is that where we are at now let's
>> That is up to you, we initially try to scope it so it was not degradable devices and focused on the question of patching and other kinds of security upgrades. If folks want to go broader, can.
>> [Indiscernible - multiple speakers] the thing I would suggest is there is an awful lot of work being done in cyber security of devices in terms of low-level sort of bottom up approach is, encryption, hardening the devices, top-down stuff, business processes, the sum survey presented this morning, you can email security dash assessment at CTA.tech if you want more information about how to get involved in the be some online assessment of your software security initiative but you have all of these things going on that are on the right picture but this was a unique drive toward upgradability so I would hate to use let focus, just my two cents, and a small plug.
>> One [Indiscernible - multiple speakers]
>> [Indiscernible - low volume] there are credential mechanisms by using the credential mechanism an individual provisioning activism and that kind of a firewall can be [Indiscernible - heavy accent] Simple example is [Indiscernible - heavy accent] For example USC passport has been given to everybody, right? So that is using like a chip in the passport [Indiscernible - heavy accent] Today those things are possible [Indiscernible - heavy accent] Same mechanism can be updated yet.
>> Over on the left here.
>> You think it really MR said, first time speaking to basal first off I appreciate conversation really think we have had a great discussion, in the conversation about labeling or communication of elements, I just want to make sure we do not lose a concept discussed earlier therapy Chris Power your articulated well. About keeping things process oriented, keeping them high level, based on the sort of similar personally took and the missed framework and so when we start to talk about in a moment, maximum standards are being very specific in elements, the more specific you get, the more limited something can be and the more shorter life it can be, as we have the discussions, I just want to keep that mentality in there and perhaps it is good to have the discussion and review of the existing standards and initiatives, but an outcome from this process be better suited to be a higher level process oriented or something that could be a little more flexible.

>> Thank you, really helpful. In a little while, we are going to go through this list and for folks watching on the webcast, who have not spoken up on the phone but you would like to get involved, we are going to be looking for some volunteers to walk into cannon fire -- I mean to accept the mental of helping to coordinate this. There are a couple of caveats when we talk about working groups that are want to help shape expectations at one of the working group is to -- should not be a surprise for those is the oldest -- to focus in and produce -- get real work done and then bring it back to the broader community and have again, a discussion from everyone in this open process are not just going to be building a final deliverable, I also imagine it is entirely possible that working groups may merge, they may fork, they may decide actually the work we are doing is much better off being done over year, they may say the work happening in this working group is very similar to the work happening in this very narrow industry group, let us have a collaboration there. Were open to all kinds of work as long as it is open, and as long as it has this general approach of the consensus across the broader community. Keep in mind you did not really need spare time anyway, and I'm hoping that some of you will help volunteer to at least take an initial leadership role in building out some of these working groups. I'm sorry, Omar?
>> Sorry.
>> [Indiscernible - multiple speakers]
>> I just wanted to clarify for the document, I was talking about minimum maximum standards, for each class of device what [Indiscernible - heavy accent] That is exactly what my concern isn't trying to say every kind of device meaning when I say class, is back to the four stage description or as he was describing, mobile device will have something different other than as computer device and so on. That is really what needs to be taking care of and accounted for in some fashion. So the minimum maximum is not to be prescriptive but really to be industrial aware, like what is the minimum that a smart sensor should be able to do that would be sort of agree on every other devices doing. Versus being aware of what is the maximum that some particular company may have done in the offer start the other capabilities, right? I think that is minimum and that has to be done on a per test device basis, it cannot be like a uniform think that some people sit together and say we will do it or smart sensors and also for its computer devices. As far as open format thing is concerned at the gentleman that there made the point that come some of that capability has existed in the other for example IPM based former/data utilities and so on till a lot of these good practices exist elsewhere which probably can start capability to the rest of the test or devices but again that has be done in open transparent environment.
>> Fantastic appreciate that. To clarify, we help us together in a working better communication, should happen as a separately dedicated conversation, fantastic.
>> Yes, is working that out there was one of the things I was going to ask you and then suggest. Also on the minimum maximum standards, I want to ask a clarifying question, do you think it is really a minimum maximum standard or really a minimum expectation and then a best of practice? [Indiscernible - low volume] [Indiscernible - multiple speakers] good.
>> [Indiscernible - low volume] expect yes,
>> Yes, I almost proposed earlier and I did not that anyone that sets standards has to go to sit outside for five minutes [Laughter]
>> Standard
>> [Laughter]

>> But yes, I agree it should not be standards. It should be some kind of expectation of best in class.
>> [Indiscernible - low volume] expect --
>> [Indiscernible - multiple speakers]
>> [Indiscernible - low volume]
>> What would you see -- all right [Indiscernible] I would see that as being something like a report out to industry kind of like the analysis of the existing work that is going on. Is that the type of thing you would envision their too.
>> Okay.
>> [Indiscernible - low volume]
>> That kind of work with basically be able to help the other working group for example who is talking about how things should be labeled, right? But this capability exist for example smart sensor has an update capability of this much and can support former updates at so many cycles. These things have seemed to have five times of so many years and that is like Max capability, right? I think everybody -- whatever is being advertised by different people so again all these criteria would be -- need to be defined and especially the context of -- [Indiscernible - low volume] [Indiscernible - heavy accent] How long the take to update, these criteria that need to be there and just a question of going and seeing what the state of the art is at the very least state of the art might be like average thing, which would be -- eventually become minimum, right? Sorry not state-of-the-art, the average would work [Indiscernible - heavy accent] If at all what you do some particular companies might have done spatial capabilities and that is work [Indiscernible - heavy accent] This is what technology today allows you to do.
>> Thank you. Further comments on this list of working groups here?
>> Brian Allen, can I jump in?
>> Please.
>> Minus just a question in part I will put myself outside in timeout in just a second but we create standards and I just want to make sure we all mean what we say what we are saying standards here so when I say that I mean documents like we write or are in season other things and there are some environments where standard means the performance level you must meet. For example Australia has minimum energy performance standards and they mean a regulatory limit like your computer cannot use more than X Watts. I just want to make sure what we're saying here here, limits of values or documents that are standards whether open source or otherwise?
>> [Indiscernible - low volume]
>> What I see, standards on there, and Ellen said NTIA certainly not a standards making body, I would see if the use of that term, so I don't think the output or outcome of this process should be a document that outlines things that would be implemented like standards, just to me those feel very technical. It is kind of telling people what to do rather than giving them the guidance on the goals they want to achieve and the kind of weather usage which is the maximum output of computer and that type of thing I also do not think that what we are generating necessarily lights to that either. I -- if you are looking at a specific place up there were talks about standards that you are using that word one clarification
>> [Indiscernible - low volume]

>> Yes, yes, if we want to rephrase that as minimum expectation, and I don't know, class leading or [Indiscernible - multiple speakers] right, to get it out of the standards and to get it out of -- good way to capture it, yes.
>> I don't need this microphone. Yes?
>> In the back here.
>> I'm not sure which group working group this blunts but I think it comes down to earlier comment that was made about unexpected side effects of software update mechanisms. And I think it is worth considering when we talk about directions forward, explicitly calling out the side effects and I don't think this is working group on its own but blunts elsewhere when we talked about for example elsewhere was software updates that they can be reverse engineered very targeted that could be worked on [Indiscernible] another one that comes to mind is on think about ways to make the software update mechanism resilient and you can escrow the [Indiscernible] but then of course comes out other question of whether someone wants to do the whole iPhone thing and suffer base of the can change how encryptions done and so forth. Somewhere calling out also considering unexpected site consequences.
>> Michael, -- token lawyer friend.
>> [Indiscernible - low volume] expect [Laughter]
>> Couple of things, certificate lawyer friend.
>> I think the side effect question is really important because when you talk about updating as I understand there are lots of testing the has to go on for various kinds of updates that I think the group could and if it from just acknowledging and saying it is not so simple as vulnerability identify, patch available, ready to roll and I think it would be helpful for the broad ecosystem for this to make sure that is clear. One other question that popped into my head from some of your past multi-stakeholder groups where I've seen things get a little contentious or logistically epochal is how are you guys planning on doing with definitional questions, goes into sort of a triggering issue for something like this, I have seen various definitions of vulnerabilities, threats, exploits, to the extent we're talking about patching and upgrading it would be useful to have a conversation about what are the conditions to trigger a consideration of steps folks might have in mind for getting in motion an upgrade or a patch because there are certain things that might -- might not rise to the level of critical vulnerability but some ambiguity. Those are my two thoughts.
>> Really key point which is which is definitions are tricky and definitions are things -- I think many of us have been in definitional fights that are formal and they are paying but I think for a lot of this work, they exist unfortunately maybe too many definitions that we can cite from a formal perspective. You have to run away before we can draft -- for your name and had for anything before you leave?
>> [Indiscernible - low volume]
>> Of course an impact I want to propose a way of moving forward. And you can tell me why you do not like it and how we can do it better. Which is that for each of these working groups, we have five, we will have a chair, ideally two chairs. This list we broadcast to the broad community, we have about three or 400 names from just across the digital ecosystem to allow people to join. In our remaining time we will try to specify these working groups a little more as a community but the first thing each working group will do will be to try to sort of think this is exactly what we are going to try to focus on in the short term in the longer term. And then

those work statements will also post publicly and share with the broader community. So that people can decide how they want to allocate their time and everyone in the community can understand what is going on. What do we think of that general workflow? Someone throw something at me if they don't like it. [Laughter]
>> [Captioners transitioning]Is one of these not scoped enough?
>> I would say you just left the door open for these individual working groups to define their own scope. If there is no guidance and this is about patch ability then we will drift into broad security -- cyber security and you will find us boiling the ocean and competing with every other broad range initiative out there.
>> I've got two fingers from Aaron and one finger from [Indiscernible].
>> I agree. In the case with the one that was mentioned earlier, I called out security patching upgradability.
>> So this's letter a, I think. Squirreled up your -- scroll.
>> One way to address the challenge that has been raised is to get -- when I think about the working groups one of the steps to define a public statement or a problem statement is a person that comes to mind. In that problem statement focus on the challenge of [Indiscernible] and patching and that helps us stay in scope before we get in a room with 70 new people and 70 new directions.
>> Thank you.
>> One of the groups that was created should have security and update ability. It should be divulged into two separate working groups. Security issues may be issued from date ability. In many cases there may be related. Everyone of the working groups should have that statement.
>> Will be like the new fortune cookie. At the end of it you have for secure ability. Other comments on how we can maintain a tight scope? Thank you for keeping us focused on task. That is helpful.
>> I have been warning you we will call for volunteers -- but before we do that, let's talk about timing at the next meeting. Probably a minimum of six weeks in between meetings for our part because it takes is a little while to get federal contracts going for space. There are holidays coming up. I don't know if people want to pull up their calendars. I'm sure there are 18 different industry events. This is the downside of having cross industry collaboration. Everyone is scheduled differently. One open question, we want to schedule something before the holidays? We are at that portion of the calendar.
>> Or in between holidays? Do we want to schedule something for early December, the December? -- Made decent -- Midshipman December.
>> What possibility -- one possibility is that the [Indiscernible] and management group are meeting in Coronado, San Diego the first week of San Diego -- December. If you want to talk to them about co-locating and be attract more attendance from their crowd and also attending the event I'm the point of contact you can do to talk to.
>> I think we got most of those our commute -- our commute -- remains -- Acre Jim's -- acronyms.
>> We do not ask other people to host things. If someone feels there is a great fit like this that is something we will keep in mind. The downside is because of the federal contracting the final decision will be made by NTIA but we try to figure out what works best for everyone. There is no optimal solution. By the end of this process, you will all hate me. Those of you that don't of

course now. Are there other thoughts or do people have other professional field events in the first two weeks of December that may be a good fit to try to locate --: okay --
>> [Indiscernible].
>> That may be a good idea. We appreciate that. Is it IEEE? Is anyone working with that organization? I'm sure there is someone in our water network but if anyone in the room has been working on that --
>> It's a conference. I know the organizers. You can find it online. It's almost DC.
>> Those are some ideas -- do we feel by looking at these working groups we can make some progress that is worthwhile to having a the first two weeks of December? Everyone is optimistic. It's the end of the day and we are all still alert. So we have a general consensus by silence which is the worst kind of consensus. Before we start to write down and ask for volunteers, looking at this list we scroll up and we can get a through E on the same screen. We may have to zoom out a little bit. Trent I know you have been taking careful notes. Can I ask you to read out we have from your notes? Let me get you a microphone. I know you have been --
>> I don't know if they match up.
>> If they don't we should clarify that.
>> First group effort to do a summary of the existing standards related efforts supply the security patching in effort to produce a report for industry documenting existing current practices. The second one --
>> Anyone have a question or comment that they want to say about that? About that task?
>> In the second working with how to foster the adoption incentives and beers to be included.
>> Any thoughts on that?
>> Here's where I deviated. I wrote down working group to explore labeling for security products upgradability patching etc. using the NIST model . For specifics potential URL participation.
>> And that we're talking about labels. Some of the discussion that came after it we muddied that idea whether or not we want to jump straight to labels and what we would include in that.
>> Fourth one was -- I have seven. Fourth one was working group for each class of device maximum and minimum capability and requirements.
>> Good. Thank you.
>> This was from our web contribution develop a broad shared definitions around security upgradability for consumer IT as well as supply chain security checklist.
>> I think that -- I folded that in with the communication side. What would be.
>> That makes sense.
>> Is everyone okay?
>> The next one which is probably been folded in because I was taking notes as to what was there. Develop strategies for communicating the security features of IOT devices to consumers.
>> Then the one that was brought in the back, I was interested in. Shared the open update for project for IOT life cycle.
>> I like that idea. Can I ask you guys -- since I think it was taught and [Indiscernible]. Can I ask you to talk a little bit about what that working group might do before they built an entire global open forum/business model. If you are looking for seed capital talk to me.
>> [Indiscernible - to far from mic]

>> I have not thought about it too much. I would begin by identifying the requirements and the deficiencies with a small companies that today could benefit from the shared infrastructure. Just to see where the pressure points are and what their barriers are for entry into doing more secure libel updates. One of the requirements for the small entities also -- I would begin by identifying points of single point of failure and points of weakness. The points were greater resilience would be needed for potential laces for the shared system to step in. I was thinking off the top of my head.
>> I have to comments on that. Before you jump and I want to apologize for hardly -- Harley.
>> To point out these kinds of things sort of exists in the commercial space. I was looking as the vulnerable device was playing it was quite clear there was licensing of stock in a cloud infrastructure from a central provider and there were hundreds of Chinese companies licensing the update infrastructure from a third party. Even though some of the companies producing the products have finished they still get updates and report into shared cloud infrastructure that is provided by an entity like a shared platform. Although a small start up I will pay five grant and will provide to all my customers on my behalf. I don't know if there's overlapping there.
>> There are a few organizations --
>> Selling [Indiscernible].
>> I was going to suggest the same thing as far as that more which is they are all good practices as far as open up [Indiscernible]. It's just a question of applying that in case of IT devices. Could he be a simple late in the working group that you are talking about? As you were saying, these things exist it's just applying in a different way.
>> That would be to look at what exists from different vendors and it's a question of reporting them as part of a working group.
>> Great. Harley, operator can we talk to Harley who's stuck in the ceiling?
>> Can you guys hear me?
>> Yes.
>> Some of what I want to say it was lost as I was waiting. I apologize to whoever is operating the cameras but for those of us watching the webcast it would be helpful if we could spend more time looking at that screen. That's where the working groups are being defined and that is important. At least I want to know what I am volunteering for.
>> We will assign you Harley.
>> I have ideas of where I want to be assigned. It's unclear to me as to whether or not the working groups will continue to be scoped through readability and not in the back security. The group will make that decision that I will put my vote in for keeping the scope to credibility as opposed to holistic center security. I want to raise the possibility of the work stream -- looking at the minimum and maximum capabilities of IOT with the working group that is examining existing standards and best practices. I would expect that the existing standards and best practices should have some indication what minimum and maximum security baselines ought to be and perhaps other than coming up with a new work product that shows him him and maximum capabilities are, you can summarize or consolidate from the existing standards and best practices. I wonder if those two groups can coordinate?
>> That is great. Thank you. Since you have been so patient from the ceiling, I'm going to give you first pick of what working group -- you can see them but they are numbered A through E. I'm sorry. Is one of the working groups that we talked about that you are interested in?

>> Operator, --
>> I'm still here. Believe it or not new talk to the [Indiscernible] moved away from the screen. You have a through E? I'm looking at at C.
>> The communication of elements which is little bit about labels but that captures your idea earlier of saying what are the components that we should be talking about as we communicate to consumers.
>> I think some of the bullets that are in their -- I'm not sure how relevant they are. Some of these things I'm not sure capture what I would consider to be communication of security to consumers. That's the only group that seems to encompass that part of the original mission.
>> Thank you. I got. -- I appreciate that. The working group itself will define what it is they want to do. These are notes from a real-time discussion. Even with the [Indiscernible] Manning -- Stephen is from our public affairs office. It is difficult to capture all of them in real time. Now is the time you have been waiting for. Everyone tries to avoid contact -- eye contact with me. Who would like to play a leadership role in some of these. I think I have thought about a few of them. I'm going to start by passing the microphone to Kent.
>> I will volunteer to co-lead A. The one I recommend it.
>> Great. That's everyone who is listening on the phone and on the webcast. This is Kent [Indiscernible - name]. Does anyone want to help Kent in this process of reviewing, existing initiatives to figure out -- in the standards -- patching -- working through what to take advantage of it so we're not reinventing the wheel.
>> I will work with Kent.
>> I'm going to raise the point again that Harley brought up and feel free to disagree. Harley suggested that perhaps this question of maximum capability minimum expectation made sense to think about in the context of what is already out there in the industry but it is also possible you want to focus on existing organizations and not delve into the hard technical questions.
>> If there was a standard for each -- let's talk about the classes. Classes we were talking about was one sensor [Indiscernible] lets call it class I. Class II was a data application and class III was an [Indiscernible] computer device in class for with data center. If standards existed for each class, I have yet to see it, which I presume will happen on A to determine what exist for each of those classes of devices -- that's from looking at if all standards exist for each class of device. These devices are out there. We're talking about millions of devices. Thequestion of the maximum capability expectation is a question of finding out -- these devices exist. They have an average lifetime of this many years. This is a question of looking around and seeing this is what capabilities are. A and D will complement each other. A look at what standards exist and D would look at what if any capability that are being advertised from different devices which are out there and has to be different subgroups and [Indiscernible] class.
>> It makes sense to keep them separate for now.
>> These would be co-collaboration. The standard might exist then we don't have to do anything. But if we do have to do something that we have to -- if nothing exist the least that will come out is there are devices and that's what they are.
>> I will jump around. I will ask you if you will like to volunteer to cochair the minimum/maximum [Indiscernible]. Is anyone interested in thinking about technology from different classes and what's possible?
>> [Indiscernible - to far from mic]

>> Fantastic. Give me a moment. That leaves -- we have the labeling -- we skipped incentives. I'm going to volunteer sick whose idea and I have worked with him in the past from SAP. Is there anyone else interested in the incentives question? We will find someone else to help pick on incentives.
>> Is communication of elements and labeling -- we have many hands out here. I'm going to go with the bow and Aaron and we have hardly. There will be three people. I think there is a lot of work to be done.
>> [Indiscernible - to far from mic]
>> Working group B and C are so -- not so distinct and it may be worthwhile to blend them.
>> I think that makes sense.
>> Says we are not heavy on volunteers for item B.
>> I think we will leave that as an open option. That does make a lot of sense. Four working groups is even more efficient. It's easy to work through and keep track of these different initiatives. Then we have E and open and share work.
>> [Indiscernible - to far from mic]
>> Tom is in. Anyone else interested in an open extensible framework to have a voluntary model we will acknowledged that it could be -- that Todd might need some help.
>> [Indiscernible - to far from mic].
>> Now the purely practical part of logistics which is -- has everyone who signed up for lead is your name and information on one of my lists? Have you received an email from me? I need to get your card. The second approach -- the second question is, is it okay for everyone who is signed up if I said your email address to the 400 people -- you can say no. I can play the remailer. It's easier to say if you're interested. I will follow up with each of you to make sure you are okay with that. We will have to have some self coordination. NTIA has few resources. I am happy to help. Organize your working groups in any way that I can. We have called bridges that's about it. Some of the working groups that we have worked use Google Docs. I recommend keeping it simple for your collaboration tools but we are here to help. We are here to nudge, and keep progress rolling. I think -- I am impressed with all the work for today. We came in thinking and agreeing this is an important problem but not knowing how to tackle it. I think we are closer -- we have a strategy to tackle it. We do not have the solutions that if it was easy enough to solve in a room of 60 strangers in six hours it would have been solved. The easy problems in the Internet have been solved long ago. This is supposed to be a heart problem. We picked it because it was important and I am very impressed of all the work you are doing. For those of you watching at home, thank you for joining us. Please give it -- feel free to contribute. We will find ways to work together. For those of you who are representing communities that have not been a part of NTIA, feel free to reach out. I am happy to brief. If you are in DC I can come to your office or jump on a phone call and talk to a broader community. The way this is going to work is saying, this is the easy part. This meeting flying to Austin that was the easy part. The hard part comes as we go back to our world find a few slices of time to roll up our sleeves and do serious thinking. With that, I would like to close the first meeting. Thank you all for your work. I will be filling your inboxes regularly. If you have any questions or comments or anything you want on the record, and let me know and I will do what I can. Thank you and I applaud you. [Applause]. The notes will be available. The notes will be available in raw unedited form.

>> That was my question.
>> Thank you. Have a great evening and enjoy Austin.