Virtual Forum for Risks in the Information Communication Technology Supply Chain: Transcript

October 29, 2021

U.S. Government Panel Members:

- Matthew Borman, Acting Assistant Secretary for Export Administration, Bureau of Industry and Security, U.S. Department of Commerce
- Kevin Coyne, Director, Office of Technology Evaluation, Bureau of Industry and Security, U.S. Department of Commerce
- Monica Gorman, Deputy Assistant Secretary for Manufacturing, Industry and Analysis, International Trade Administration, U.S. Department of Commerce
- Sahar Hafeez, Senior Advisor, Office of Under Secretary, Bureau of Industry and Security, U.S. Department of Commerce
- Bob Kolasky, Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security

Speakers:

- Intel Corporation, Tom Quillin, Government Affairs
- Telecommunications Industry Association, Melissa Newman, Vice President of Government Affairs
- Palantir Technologies, Matthew Turpin, Senior Advisor
- MIT Industrial Performance Center, Timothy Sturgeon, Senior Researcher
- Information Technology Industry Council, Courtney Lang, Senior Director of Policy

Transcript:

MAURA WEBER: Good morning everyone and welcome to the Virtual Forum on the Risk in the ICT Supply Chain. My name is Maura Weber, I'm with the Bureau of Industry and Security, and I will serve as moderator for this forum. I would at this time like to welcome Ms. Sahar Hafeez to give opening remarks. Ms. Hafeez serves as Senior Advisor for the Office of the Under Secretary for the Industry and Security, here at the US Department of Commerce. Ms. Hafeez?

SAHAR HAFEEZ: Thank you so much Erica. Good morning everyone. I'm sorry-- can you all hear me?

MAURA WEBER: Yes.

SAHAR HAFEEZ: Okay, good sorry, I was not sure. Good morning everyone, sorry for joining a few minutes late today. We're having some technical difficulties here. Welcome to the virtual forum for risks in the ICT supply chains, we are really grateful for your participation and your input,

[00:55:00]

particularly the speakers that are going to be presenting here. Supply chain resiliency is a key component of the Biden Administration's Build Back Better agenda, which the President campaigned on. Supply chain resiliency is critical because as the pandemic has shown, structural weaknesses, and both domestic and international supply chains, threaten America's economic and national security. Over the past year and a half, our economy has experienced severe supply chain disruptions brought on by the pandemic, cyber-attacks, extreme weather events and as well as other conditions that have reduced the availability of goods and services. In view of all these challenges, on February 24th, 2021, President Biden issued an Executive Order EO 14017, entitled America's Supply Chain, which focuses on the need for resilient, diverse and secure supply chains to ensure U.S. economic prosperity and national security. Resilient supply chains will revitalize and rebuild domestic manufacturing capacity, maintain our competitive edge in research and development and create well-paying jobs in the United States. This Executive Order directs six agencies to conduct a one-year review of their respective industrial bases, with the objective of developing strategies aimed at building resilience and security throughout the supply chain supporting these six sectors. In addition, as you may know, the Executive Order also directed four 100-day studies which were completed in June of this year. For purposes of the one-year studies, the Department of Commerce and Homeland Security have been directed to conduct a one-year assessment on critical supply chains supporting the ICT industrial base. For purposes of this report, the scope of the ICT industrial base shall consist of component hardware that enables terrestrial distribution, broadcast wireless, transport, satellite support data storage to include data center and cloud technologies as well as end user devices. This is going to be a manufacturing focused report consistent with the intent of the Executive Order which focuses on the industrial base, as we understand that there are a lot of efforts going on in the ICT space in the U.S. government, so we don't want to be duplicative of those efforts. So that's how we're focusing [the report]. Some examples of hardware components include printed circuit boards, fiber optic cables, electronic manufacturing and assembly services as well as downstream products. BIS which has been organizing this effort along with DHS and a number of other bureaus across the Department of Commerce, including the International Trade Administration (ITA), National Telecommunications and Information Administration (NTIA), as well as National Institute of Standards and Technology (NIST), among others, recognizes this assessment cannot be done without industry input. So we thought we would organize this forum to complement the written comments that are due on November 4th. If you have not submitted them yet, we encourage you to do so. The deadline is coming up and we take those very seriously.

With that, I look forward to your presentations and I'll introduce my colleagues who are joining the panel. Matt Borman, he will join us -- he's a bit tied up but he will be joining us -- he's the Acting Assistant Secretary for Export Administration at the Bureau of Industry and Security, here at Commerce; Kevin Coyne is the Director of the Office of Technology evaluation within BIS at Commerce; Monica Gorman is the Deputy Assistant Secretary for Manufacturing in the International Trade Administration at Commerce. And finally last but not least, we have Bob Kolasky who's the Director of the National Risk Management Center at the Cybersecurity and Infrastructure Security Agency, CISA, at the Department of Homeland Security. Now I'll turn it over back to Erica for some housekeeping announcements. Thank you.

MAURA WEBER: Great. Thank you Sahar. Yes to address a few announcements, participants should be prepared to attend the virtual forum in its entirety. As you can already tell, speaker times are subject to change and the program will continue if a speaker is not available to speak.

[01:00:00]

today we will have five speaker presentations. Speakers will have 15 minutes to present and will hear a bell when they have reached that 15-minute time limit. At that time, please wrap up your remarks. If you do not wrap up within one minute, we will mute your microphone and continue with the program. Following each speaker presentation, the U.S. Government Panel will have five minutes to ask the speaker questions. Panelists should indicate the raise your hand function on WebEx to ask a question and I will facilitate this Q&A session. At the end of the speaker presentations the US Government Panel will then have 20 minutes to ask questions directed at all speakers as well as attendees. Panelists should indicate the raise hand function on WebEx to ask a question. In addition speakers and attendees will also use the raise hand function if they would like to respond. Please identify yourself and your organization when speaking as well as please mute your microphone when you are not speaking. This WebEx will be recorded and the transcript will be available within seven business days on the BIS website at BIS.doc.gov/ICTForum. If you need technical assistance, this will be available throughout the virtual forum, and the number which will also be provided in the chat box-- but the number for technical assistance is 210-515-0481, or toll-free number is and the 888-452-5950 is 8452104. There will be no open question and answer sessions during this forum for press. If the press has further questions, we ask that you contact the Office of Congressional and Public Affairs Director, Jeremy Horn at Publicaffairs@doc.gov. And this information will also be. So with those announcements out of the way let us begin with our first speaker Mr. Tom Quillin with Intel Corporation. Mr. Quillin, you may begin.

TOM QUILLIN: Thank you Maura, can you hear me well?

MAURA WEBER: Yes, thank you.

TOM QUILLIN: All right, thank you very much. And thank you very much for the opportunity to speak. My name is Tom Quillin, Senior Director of Government Affairs with Intel Corporation. Intel appreciates the opportunity to share comments in support of efforts by the Secretary of Commerce and the Secretary of Homeland Security to prepare the report on supply chains for critical sectors and sub-sectors of the Information and Communications Technology Industrial Base, required by the Supply Chain Executive Order 14017. First I want to acknowledge and commend the White House and the Department of Commerce and the Department of Homeland Security and other agencies, for the insightful and thorough evaluation of semiconductor supply chains and the 100-day report under Executive Order 14017. In noting the decline in share of U.S. production of semiconductors from 37 percent in 1990 to 12 today, the 100-day report noted how -- and I'm quoting from the report -- how effective industrial policy of key nations has led to geographic concentrations of key supply chains in a few nations, increasing vulnerabilities for the United States and global producers. Such concentration leaves companies vulnerable to disruption whether caused by a natural disaster geopolitical event or

indeed a global pandemic. The 100-day report recognized the important work done so far by Congress to advance the Chips Act, which by investing in US based capability and capacity for chip making advances resolution of those problems. And the report also urged Congress to fund the Chips Act. Intel strongly agrees with the Secretary of Commerce Raimondo on the emergency and the urgency of Congressional action now to address the root cause of the current chip shortages. But let me turn now to the broader issues and focus for the one-year report on the broader ICT supply chains.

[01:05:00]

Intel is deeply involved in the ICT as both a customer of ICT supply chains and a provider to many of the equipment integrators who rely on ICT supply chains. I'm confident that others are going to address the nature and severity of ICT supply chain challenges around specific materials, and including displays, batteries, materials for battery manufacturing and printed circuit boards. I'd like to speak to the broader systemic issues around trust and transparency in the ICT supply chain and supply chain security. Often conversations around supply chain security focus on more physical aspects of supply chains: employees, logistics, physical security and so on. And while these are essential focus areas, Intel sees significant opportunities to identify solutions that help ensure trust in ICT products by sharing information about a device's digital provenance. Sometimes we call that cyber supply chain risk management, but it may be more useful to think about it a little bit differently as digital supply chain security. New solutions could increase transparency and visibility up and down the supply chain about devices themselves. And while digital supply chain security measures alone would not prevent inventory issues or shortages of the types that we're seeing, for example, in the semiconductor industry, they do address other aspects that Executive Order 14017 seeks to highlight, including things like identification of an understanding of alternative suppliers or inputs by generating more visibility into specifics about inputs and suppliers for a family of devices. President Biden's Executive Order 14028 on cybersecurity issued directives on a broad scope of measures intended to address software including methods to improve software supply chain security. As an aside, I also want to note that the President's National Security Telecom Advisory Council, NSTAC, has a draft report posted on the NSTAC website at CISA.gov a report which offers deeper discussion on some of the key opportunities to improve supply software. Now the initiatives and focus on software supply chain security came partly as a result of attention and the problems that came in the aftermath of supply chain attacks against broadly used technology suppliers at the end of 2020, and in the early months of 2021. The focus on software supply chains is important and wanted, but it raises other questions too which of the methods identified in Executive Order 1428 could have benefits if extended to hardware supply chain security? Maybe what opportunities exist to link efforts to increase the robustness of hardware and software supply chains? We suggest it might be useful to focus not only on the differences between hardware and software, but also on the common goals for supply chain security across all of these digital products. And this is where thinking about digital products and digital supply chain security may help us think about common traits of ICT technologies that we want to identify traits like authenticity provenance posture, security posture and change histories. All elements which can be tracked and communicated and shared digitally across a digital supply chain, across life cycle of ICT technology. So what does it mean for supply chain security to go digital? Really it's about the benefits that come from offering integrators, IT managers, and technology owners evidence of

supply chain security and supply chain integrity throughout the life cycle versus only at build time. And this is an important point. Sometimes supply chain discussions focus only on the build and distribution phases of the ICT technology life cycles as if technology somehow becomes frozen in amber after integration or delivery. But we need only look to the compromise of it tools as in the so-called Sunspot Attack to see how essential it is to monitor supply chain integrity from build through deployment, through operation of the technology, and all the way through to retirement and end of life. So for example although

[01:10:00]

the effort is still maturing, it's fair to say that an effort like the Commerce Department's NTIA-led Software Bill of Materials or SBOM, or it's like, may come to play a key role in moving toward digital supply chains, even though this effort is not a panacea in many key questions remain about how SBOMs can scale to the demands of broader usage. Another interesting project is Google's SLSA project - the acronym stands for Supply Chain Levels for Software Artifacts - and this is another software focused effort focused on mitigating the risk of integrity attacks but SLSA provides visibility into process and how a package is assembled not only its ingredients. Broader adoption and abrasive something like SLSA will be a significant step forward to better supply chain security. But what about hardware? Could parallel approaches be developed that can make hardware supply chains more like digital supply chains or move hardware supply chains towards becoming digital supply chains? So there are several efforts of note in this space and these are all public, but they're only beginning to receive the attention they deserve. And I want to highlight a couple of those. First the Trusted Computing Group, TCG, a global standards body developed the platform certificate specification recently updated to version 1.1. Platform certificates are digital certificates that capture and securely store key attributes of a hardware device as it makes its way through its lifecycle. What components were, used where was the system manufactured in what facility, in what country? What was the known good state of the device at the time of manufacture? The platform certificate provides a reliable and secure way of capturing and providing this data to device owners throughout the device life cycle. Second NIST has begun publishing a series of guidelines under the heading of NIST Special Publication 800-34 on validating integrity of computing devices with extensions of this series of documents anticipated to cover more types of ICT products in the months ahead. These 800-34 series of documents really complement the comprehensive work NIST is already leading under the cyber supply chain risk management bible SP-800 161, which is now in revision. Another effort that I want to highlight is a new working group in TCG -- I mentioned TCG earlier the trusted computing group. TCG recently initiated a solutions-focused work group led by Microsoft, Goldman Sachs and Intel to start framing solutions and implementation models for digital supply chain security. And this is an important complement to the platform or ingredient level specification work that has been done around the platform certificate that I mentioned. Perhaps most importantly and most encouragingly ICT integrators and manufacturers have begun to offer commercial products as IT for digital supply chain security. Based on these kinds of approaches to their end users these solutions allow ICT device integrators, IT administrators, and end users visibility into key information about an ICT product. For example evidence of authenticity of an OEM, its device or a component, the country of origin by component integration history device health and integrity, and indicators of tampering or other compromise just to name a few. Intel expects these offerings to proliferate as more risk managers and ICT

supply chain leaders understand the benefits of new risk management practices enabled by such approaches. These efforts need and deserve greater supportive focus to mature but they are going in the right direction, and they offer an essential complement to current software-based efforts, and to other measures for supply chain resilience focused on shortages of specific inputs and products.

[01:15:00]

Growing interest in these areas suggests really high awareness of the opportunity and problem. As a key supplier to the broader ICT supply chain, Intel recognizes that our fortunes are linked with the fortunes of our customers and end users and that's why we are dedicating R&D to joint projects with integrators and standards bodies to define new technical solutions to important problems like securing the ICT supply chain. In closing let me thank you for your efforts to engage the industry in new approaches and to address the risks in the ICT supply chain. And thank you again, for your ongoing efforts to address the semiconductor shortage and for reinforcing the urgency of Congress to fully fund the Chips Act. Thank you.

SAHAR HAFEEZ: Thank you so much Tom. That was really insightful. Yeah, we need we're really focusing on the Chips Act and we need everyone's support on. Hopefully we'll get that across the finish line very soon. I'll turn it over to my colleague Monica to ask the first question.

MONICA GORMAN: Great, thank you so much Sahar, and thank you Tom. This has been a really helpful and insightful presentation. Appreciate all the different efforts that you mentioned and the detail that you provided. You talked about the migration to digital supply chain risk management and a lot of the industry efforts to secure the supply chain really came through in your presentation. What can the US government do to encourage or promote wider adoption of these practices?

TOM QUILLIN: Monica, thank you very much for that question. I think one of the one of the key things that the government can do is to align incentives and to help clarify the most important areas for future research and development. So for example I think it's pretty well known and has been explored in lots of analysis that’s around the open source community for software, that the open source community thrives because so many different people are contributing for various motives and reasons. And that's one of the keys to the success of the open-source software community. Similarly in hardware, it's very important for hardware integrators to be able to rely on many alternate sources and to be able to switch very quickly between alternative suppliers for common elements of a solution when shortages occur or when problems occur with a specific supplier. But often the need to ensure that schedules are met or the cost targets are met or that performance targets are met can lead to trade-offs between security and trust and those other competing-- not competing goals but complementary goals. And so having a stronger focus on building increased focus on incentives to ensure security and trustworthiness are important. One way Monica to do that-- just one more thought on that. One way to do that might be through addressing issues like this in procurement mechanisms or updating fast procurement guidelines.

SAHAR HAFEEZ: Thank you, that's very helpful. Any other questions from the panel?

BOB KOLASKY: Yeah, can you hear me Sahar? Hi, Tom how are you? Just continuing off that, let me ask maybe a two-part question. Ultimately, do you think of building in more security, more verification, these processes, do you

[01:20:00]

think of it as adding costs to the business, the degree to which a company that is a supplier needs to prove that they have that to do business with you all? And to match the incentives that hopefully we can create within the U.S. government? How do you think of the cost factor there? And where is that cost born? And particularly as we talk about often right in the small to medium-sized business, where there are probably there are a couple considerations-- right there's cost consideration there's also it's just hard to at that level find the talent necessary to put in place security verification sometimes given other priorities. So how do you think about all that?

TOM QUILLIN: Yeah, thanks, Bob. That's a great question. I think that the question about cost needs to be linked to a question about value. And I think that the opportunity for us is to help consumers and users of technology to recognize the value that comes with and with improved trust and transparency and visibility and supply chains. And so if we can help create value for that and recognize that there may be there may be increased costs associated with the processes -- both business processes and technology processes -- associated with these kinds of transparency efforts, I think that value will generate that it'll be sufficient to cover the increased cost implied by some of these operations. You raise a great point to Bob about small and medium business, and I think that the hope would be that as the benefit of these kinds of approaches get proven out by large customers and large enterprise organizations, again, that value will be demonstrated. And once that value is demonstrated, then I think it becomes much easier for smaller and medium businesses to be able to generate solutions that serve and meet that value.

BOB KOLASKY: Appreciate it.

MAURA WEBER: Great, well thank you very much Mr. Quillin. At this time we will move on to our next panelist, and we will have more time for questions at the end. Our next speaker we will hear from will be Ms. Melissa Newman who is Vice President of the of government affairs at the Telecommunications Industry Association. Ms. Newman, you may begin.

MELISSA NEWMAN: Thank you. And thank you for having me here today this is a great forum to discuss these issues and TIA certainly appreciates being able to participate. Just some background: TIA is the Trusted Industry Association for the connected world. We represent over 400 global manufacturers and vendors of trusted information and communication technology networks worldwide. In addition to representing our members in these policy type issues affecting the industry, we are also a standards development organization, and over the past century has created thousands of telecommunications standards, aimed at building trusted, reliable ICT networks to connect the world. So I'm going to talk about four or five main things the geography of the ICT supply chain, the importance of trusted vendors in that ecosystem, how standards support security quality supply chains and the semiconductor chip shortage, and the effect on the telecom sector. But before I start, I want to first define the scope of the Information

and Communications Technology Industrial Base. ICT spans a broad range of products that connect people to the internet. From the consumer perspective, it starts with the user terminal whether that's a mobile phone, a laptop, a smart watch or other device. Those devices subsequently connect to a range of technologies through satellite, internet, cellular wi-fi routers through ethernet connections, and then signals are subsequently carried through a huge network of fiber or copper cables through switches and routers to data centers. Each of these products has different supply chains, and the risk to these supply chains are to some degree different. I can't today cover the full range of risks to everything here, but again, we're going to talk about four areas that we think are relevant to this discussion. But the reason I point this out is it is a very complex, complicated, sophisticated network throughout from beginning from the end user to the end.

[01:25:00]

So let me start with the geography of this ICT supply chain. The supply chain for the ICT sector is global with manufacturing operations that span the globe. From the design process to contract manufacturers that build the products dense networks, suppliers, subcontractors. I'm going to pull out one component, semiconductors. Semiconductors can require more than a thousand discrete steps in the manufacturing process and pass through borders more than 70 times before the chip meets the consumer. And my point on all this is, again, it is deeply global. And the reality as I see it is I know we are looking at changes to Buy America requirements, but I think at the very basic view, it will not result in a solely American ICT supply chain. And I want to put that point out there for people to consider. The second point I wanted to make is about trusted vendors. Obviously with the rise of attacks on the nation's networks, it is more than ever critical that the industry and government work together on supply chain security. We are seeing this play out through more traditional bad actors such as the recent Facebook data breach or through an increased number of attacks from state sponsor entities, such as the Russian attacks targeting Microsoft or the SolarWinds attack last year. These attacks as you probably know you utilize a hardware-software vulnerability embedded into an ICT device. And it makes it even more critical than ever to be able to trust every element of the supply chain leading to the completed ICT product. TIA was a leader in asking the government to exclude untrusted vendors from the U.S. telecom networks, and to subsequently rip and replace the existing equipment from the network. We very much support the underlying logic that led the Bureau of Industry and Security to place Huawei and ZTE on the entity list, and we further support efforts to replace equipment from untrusted vendors worldwide. These two companies will not be the only untrusted vendors in the ICT market. We are already seeing a rise of Chinese companies flooding into the Open RAN space. For example, ZTE has announced a memorandum of understanding with China Mobile Research Institute to research O-RAN applications. And other listed entities, including Inspur and Kindroid, are involved in O-RAN projects. Other Chinese companies are participating and winning awards in RFIs and markets around the world, so this is something we are going to have to continue to watch and be vigilant about. I too, like Tom, want to thank the Biden Administration for taking a strong leader position in response to these significant cyber-attacks. We support the Administration in these efforts, as well as the administration's efforts to try to create a whole of government approach to supply chain security. Many U.S. agencies have been focusing on these issues. And while we have always supported narrowly tailored government action in this area, I will be honest the sheer volume of active government efforts on this issue

has been at times overwhelming for industry experts who are in public/private partnerships, who are working on these issues. We certainly welcome the addition of Chris Inglis as the National Cyber Director, and President Biden's Executive Order on America's Supply Chains, and truly hope that the administration will use these tools to ensure that all U.S. government stakeholders are working in concert together on these issues. I do want to turn to the semiconductor chip shortage. The impact of the semiconductor ship shortage on the automobile industry has gained probably the most attention, but I want to make sure people understand that the telecommunications industry has been particularly hit hard given the dramatic increase in the need for connectivity during these last two years. ICT products are very semiconductor-intensive, and for many products, they are the single largest cost driver.

[01:30:00]

Telecommunications is the single largest end user of chips constituting fifty percent of all semiconductor end use, split evenly pretty much between the end user devices and infrastructure. And I will compare that to the automotive industry which is about ten percent of end uses. And as we know and have been reading about -- and I don't have the latest statistics -- but we've seen cost increases on extended product lead times because of the semi-conductor chip shortage. So we too support the Chips Act. We hope government action will focus on providing positive incentives for semiconductor manufacturing and design. We think that's the better way to go than diverting chip production toward any specific end use. So again, very supportive of the Chips for America Act. I will do this plug for the telecommunications industry: connectivity is key to our future, our economic future. The deployment of nationwide 5G has the potential to create or transform 16 million jobs across all 50 states and increase the U.S. domestic product by $1.5 trillion dollars in the next five years alone. So it certainly is about jobs and the economic future of our country. The last thing I want to mention a standard that TIA has been working on for the last two years, and we intend to release it year-end in December, SCS Supply Chain Security 9001. It is the first ever supply chain security standard for the ICT industry created by the industry. And a large working group of people, volunteers, to put together a very comprehensive standard for the ICT industry. It is based on TIA's quality assurance standard and that standard is the foundation of quality assurance in the ICT industry. It is a belief of ours, you cannot have a quality product without security. I would be happy to share the standard with anyone. We are taking comments from industry and government at this time. I was happy to see in Politico this morning that Cyber Director Chris Inglis talked about public-private partnerships, and we think that this standard for the ICT industry is a big step along that public-private partnership road. So thank you very much for the opportunity to talk to you today.

SAHAR HAFEEZ: Thank you so much. That was very helpful. I'll start by saying that the chip shortage and the impact on the telecommunications industry as well sectors in addition to the that are something we are very aware of. It's top of mind for us and the Secretary [of Commerce] and high-level officials in the administration are really focused on this effort. I'm sure everybody on the on this call who's very plugged in knows about the request for information on the semiconductor conductive supply chain which should hopefully shed light on some of these challenges, so we can we can advance transparency and hopefully try to-- can you hear me?

MAURA WEBER: You are very quiet if you could please pick up, thank you.

SAHAR HAFEEZ: We're having a lot of technical issues, is this any better? Somebody else do you want to go ahead?

MAURA WEBER: Yes, do any of our panelists have a question please?

MONICA GORMAN: I'll gladly kick off with a question. And Melissa thank you very much, good to see you again, and appreciate your comments this morning. You talked a lot about the risks posed by untrusted vendors but just curious what you would say about trust for upstream suppliers, those lower tiers not the companies themselves but those upstream suppliers in the ICT supply chain. Do your members have sufficient visibility into who those suppliers are?

MELISSA NEWMAN: Thank you, Dr. Gorman. Things can always be improved, and I would say, and I'm going to do this as a plug, I do think our SCS 9001 standard will make that transparency more apparent. Because some of the stuff Tom talked about, providence and going through all that where, it's a whole host of things you have to show, verified by an independent company, but I think there could be better, yes.

[01:35:00]

KEVIN COYNE: Hi, Kevin Coyne from BIS. I'm just curious to see how do you envision that standard being applied across private and public space? What sort of interaction are you anticipating, regulatory policy changes in terms of enforcement across the far and deeper or broader type actions?

MELISSA NEWMAN: It's a voluntary industry standard, but we hope it's something the government can support. I am well aware that it's hard -- standards, rules, regulations - people don't always want to jump on top of that. But I still think a voluntary industry effort is the best way to go because you're not only balancing security of course, but you also want to continue innovation. But we certainly would appreciate input-- and it is why we sent the standard out to hundreds of government officials and happy to send it out to anyone else for their input. Because it was something we hope that the U.S. government and governments around the world -- it is a global standard -- can support.

MAURA WEBER: Are there any other panelist questions? You can either speak up or indicate by the raise of your hand.

BOB KOLASKY: Hey Melissa, how do you see the trajectory of the mix of global supply chains changing based on the direction that this Executive Order and the work is taking? Is it adding any efficiencies or burdens in trying to do business across multiple countries and with different expectations I guess for your member organizations?

MELISSA NEWMAN: Yeah, I don't know if I'm going to answer this directly but I'll tell you what our members are what people are concerned about and hopefully that will get at it. This is a global industry, and while we certainly support U.S. headquartered companies here we really think our trusted vendors, who may be headquartered overseas who have put such commitment

into the United States through the networks they build here, the plants they have in the U.S., the citizens, U.S. citizens they employ here, the taxes they pay - there is nervousness that this is being overlooked by the commitment they have made to America and they're on our side. So we talk about this in terms of trusted and untrusted vendors as opposed to country specific versus headquartered specific. It is a global supply chain. And I would say as American companies, headquartered companies get involved in the supply chain -- and we certainly hope they do -- ten years out you don't know whether they will be still American headquartered companies, or they would be bought by a foreign ally trusted company overseas. So trying to engineer that is difficult in our view if not impossible. So we do see it in terms of trusted and non-trusted vendors, with those trusted vendors with a commitment to the United States. I hope that answered your question but that's the concern we're seeing.

BOB KOLASKY: Yeah, appreciate that Melissa. Thank you.

MAURA WEBER: Great, any other questions from the panelists before moving on to our next speaker? All right, thank you very much Ms. Newman. We appreciate your remarks. And now for our next speaker we will turn to Mr. Matthew Turpin with the Palantir Technologies. Mr. Turpin you may begin.

MATT TURPIN: Maura, thanks, so much, and thanks everyone. I'm Matt Turpin senior advisor at Palantir Technologies. Great to see a number of old friends online today, and I want to thank the Department of Commerce and the Bureau of Industry and Security and its other partners for hosting this event.

[01:40:00]

The Administration's initiative to deal with supply chain vulnerabilities and the impacts that competitor nations' industrial policies have on what Melissa Newman just made the point about, this sort of a global ICT industry, is incredibly important and it's an effort that we welcome participation in. As a long-term technology partner of the US government, we see that this area is an area that requires complex, data-intensive sort of efforts to be able to get our hands around and be in and begin to be able to address. And so the President's Executive Order on supply chains I think provides an excellent venue to begin to look at this, and pull together the various actors across departments and agencies, but across industry to begin to tackle some of the problems and to begin to figure out what it is we want to be able to do. So the success of supply chain risk analysis and resiliency efforts depends on the quality and consistency of both the policy side as well as the data to be able to make decisions about how to intervene, where to intervene and what government tools and authorities can be used to shape and push supply chains, that quite frankly, are being shaped and pushed by competitors in ways that are that are largely meant to disadvantage us. The ability to effectively employ US government tools and authorities to address supply chain resiliency requires dynamic, near real-time understanding of the commercial, industrial and manufacturing ecosystems that make up the industries that we care about. And those are industries that we care about for both economic prosperity, and for national security. As my colleague just laid out in her presentation, the geography of our supply chains suggests a high degree of complexity. And that requires what I think that we would contend is a common operating picture so that various government departments and agencies --

not just BIS, but BIS is a key player in this -- can work off a common ground truth to be able to employ their tools and authorities to achieve outcomes. The ability to shape ICT supply chains requires this sort of consistent, near real-time understanding of the situation. The ability to conduct cost-benefit analysis on various government decisions of carrots and sticks to employ requires an understanding of that system. However, as I think we would all sort of understand, is right now it's very difficult to see that system, and it's very difficult to understand how that information and data is shared departments and agencies. So I would end with an appeal that as the Department of Commerce and its partners begin to contend with moving from an analysis stage to an action stage, that they are thinking about the tools that they would use to be able to sort of impact supply chains and be able to conduct their own modeling of the decisions that they're making. Certainly, industry has a part to play in this in terms of data. But this is a capability that the government requires internally to be able to see the landscape and the network. So I think I'll stop there and turn it over to questions. Thank you.

MAURA WEBER: Great thank you. If any of our panelists at this time have questions, please either speak up or use the raise your hand function.

[01:45:00]

BOB KOLASKY: I'm happy to ask one. Matt, what are the barriers to getting the visibility that you're talking about they're near real-time situational awareness? Obviously you all are investing on the technology side to get that. but what other barriers do you see in helping companies have full visibility? What's possible?

MATT TURPIN: Right. I think it's and I think we can all sort of openly admit to each other that there's often sort of cultural barriers within Departments and agencies but also between government about sort of a willingness to share an understanding of what amount of data is actually needed to be able to help improve decision making. And I think that you're thinking about this from the perspective that beginning to break down and have a common picture of even relatively small amounts of data, that are spread across sort of industry sectors, begins to improve the ability to be able to do that. You don't need full access in order to start; that you can start to share that data in sort of a beginning stage. The other part is, what are the controls that are in place so that individual industries and companies have a confidence that what they are sharing is appropriately shared with the individuals who are meant to have it, and that is not being sort of abused and passed on? And that competitors are not receiving sort of unfair advantage by having access to it? So beginning to work sort of at a small scale of initial problems and then building from there, is probably the way that we've seen it work particularly well. And certainly we've seen that these similar problems unfold in in the pandemic as we were dealing with medical and PPE and pharmaceutical supply chain shortages. And how do you gain access to that across those industries, and ensure that industry partners and government partners are each getting benefit out of that sharing of data? But ultimately it is meant to improve decision making which is an industry interest as well is that they want to be able to see more refined decision making the ability to sort of perceive cost and benefit of actions. And so to a certain degree what's necessary in that is an understanding in your real time sort of what the situation looks like to be able to make those changes.

SAHAR HAFEEZ: Hi, Thanks so much this was very helpful and insightful. Can you speak a little bit more about how we can incentivize industry to participate? This is something that is how-- we do appreciate your comments about having more visibility data to the extent that it's appropriate. Not all data off obviously, but to the extent that is appropriate it would be helpful to make more informed decisions. But how do you envision sort of the relationship with industry? How we can incentivize them to participate? If you speak a little bit more detail about that, that would be helpful. Thank you.

MATT TURPIN: Yeah, I think it requires a movement a general discussion about sharing of data to specific problems and another a degree of consensus between industry and government of what specific problems do we want to address. And if we can get down to like a specific problem that both are interested in addressing, then we can talk about the specific data that's needed for that. As opposed to a broad discussion about share your information, share your customer information, your supply chain information in total, and then we'll figure out what we need from that. I think it starts with a specific problem and then an examination of what are the actual pieces of data that are necessary to make that decision and the and the currency and the rate of updating of that data to be able to sort of address a specific set of problems. And then as you build trust around that, other problems can then be addressed. But I think we have to move very quickly to specific issues.

[01:50:00]

MONICA GORMAN: I might follow up on that a little bit. I'd just like to dig into your thoughts about the role of government versus the private sector in data. So obviously you mentioned COVID and the PPE pharma supply chain that was obviously a crisis situation which required urgent joint action. But as we think about supply chain resiliency more broadly and not necessarily in a crisis situation -- but our goal here of course is to secure the supply chain long term -- where do you see that line between private sector perhaps doing a better job of managing its own risk up and down the supply chain versus that of the government?

MATT TURPIN: I think certainly the various pronouncements and Executive Orders from the administration have laid out an understanding that sort of economic security and national security are sort of tied together and that the prosperity and success of companies has a very real relation to the way in which government participates in ensuring that sort of market outcomes are fair and we're achieving the solutions that we've agreed upon international bodies but in practice are not being followed through. And so I think for government to lay out its area of action, those are defined relatively well in terms of the authorities that various departments and agencies have right. So the Bureau of Industry and Security has a clear authority around dual use export controls for those things that are considered to be sensitive dual use items. And the certainty that they can they can have and being able to sort of apply the enforcement of those regulations provides better certainty for industry on where they should be placing things, how they should be managing their own supply chains, and be able to make that happen. So I think for government to be able to improve the execution of its authorities with greater certainty and that it's doing that in sort of near real time allows for industry to be able to adjust to what those are. Because we have laid out there are clear areas that are that are government interest to be able to sort of step in

and intervene-- and it can clearly delineate where those areas that that are fine to establish those relationships as Melissa was laying out: that we live in a complex world, that it is not every entity because of its physical location, that you have to evaluate each one. Well that requires a much more detailed understanding on government and a more sort of exquisite application of those things to be able to be able to apply that.

SAHAR HAFEEZ: Thanks, so much. That was really helpful. I think in your comments, if I may, could you talk a little bit more about the specific problems we should be looking at in terms of what we're addressing. If you could talk about in your view what those specific problems are as it relates to the focus of this report, we think that would be very useful. But your comments were very well taken as we sort of think about these issues. I wanted to if it's Okay, talk about another issue that hasn't come up yet but is very important to us is about the labor market: if you could speak to that a little bit in terms of what are the human capital gaps that you see in this sector, which is quite broad. But keeping the focus that we are here, on the industrial base. If there's anything you can elaborate on here or in comments later, that's something just wanted to highlight that we are focusing on as well as part of this effort.

MATT TURPIN: Well, in terms of sort of where are our vulnerabilities and strengths in terms of labor market across the ICT sector, I think I would defer to sort of my colleagues that sit sort of as representing sort of the broader industry sector. I think it's difficult for us to be able to comment on that. Obviously we sit and have insight into our own areas, but I think the broader ICT sector, others might be able to provide a better input in terms of sort of specific problems--

[01:55:00]

And I think ultimately this comes down to sort of where BIS and Commerce and the rest of the US government want to start. And I think to a certain degree as a company, we're a bit agnostic of what problems to help on other than it should be ones that are important. So in terms of ICT supply chains, I think even simply an understanding of sort of inputs, manufacturing processes and outputs to where sort of chips go, and what industries do they actually go into and what different types: that picture alone may provide some insight into where your attention would be best served. There may be areas that simply are generally running okay, and there may be ones that require an intervention. And that might help you all focus your attention and energy on those sorts of things. And then figure out like what is the data that you need to collect, what departments and agencies need to be involved in terms of the tools and authorities that would be brought to bear. But that requires an understanding of like where are your problems. And I think to a certain degree, we've got to look to you all to help provide some of that.

MAURA WEBER: Great, thank you Mr. Turpin. At this time we will now turn to our next speaker we have. Dr. Timothy Sturgeon from MIT Industrial Performance Center. Dr. Sturgeon you may begin.

TIMOTHY STURGEON: Thanks, Maura. And I just want to say thanks to BIS for organizing this forum and inviting me to speak. I'm the lone academic on the panel so I'm going to use a slide deck because that's what we do. I'll put that up right now, let's see if I can find it. Okay, there we go. So really I see my job as look at the big picture and develop conceptual models to

understand something as hugely complex and confusing for most people as the ICT-- broadly speaking the gigantic ICT supply chain let alone all the industries that are inside of it. And then present that to lay people, I think a lot of the things I'll mention today are well known to the experts in the room. But still experts tend to work in silos, so I'm trying to get the big picture here and then to really frame the problem. And so we're looking at this concept in this team I'm working with Eric Thun, Darla Taglioni, and Mark Dallas on this on this multi-year project looking mainly at the mobile telecom industry, but obviously is connected to the rest of the ICT sector. So we're able to give some perspective on the issues we're talking about today. So I just want to point out the special features of this industry that it's been outsourced from really for since the 60s have been engaged in outsourcing. And I'm not going to go through the sub-bullets because I don't have time, and we can look at this stuff later or you can look at the slides I'm sure they'll be available. So outsourcing but also off-shoring since the late night late 1960s and early 1970s, but this trend obviously accelerated in the 2000s and by 2011 China accounted for 41 of all ICT hardware exports. But they weren't making all everything inside of China, obviously there was a lot of imported content in those exports. Up to 80 percent for very high technology ICT goods. And for something like the iPhone the value added in China was about 1.5 percent, which some of the estimates show. Of course that's increased over time, but there's a lot of misconceptions about Chinese dominance in terms of the technology. And obviously things are moving very quickly, they're moving ahead. But this system developed in a modular fashion where components could be used and or adapted to different products over time. So no company is really doing everything. And the software side of it was modular from the beginning.

[02:00:00]

So these are baked in these: the global structure, the modular structure are baked into the industry. So today after 50 years, we have this hugely complex, multi-layered modular system is the way we're conceptualizing it with a lot of standards that are used are the glue that hold these different modules together. And these standards come from different places, from de jure multi-stakeholder initiatives as we were talking about earlier, with some of those; but also de facto standards particularly around platforms and platform APIs and also proprietary standards by strong players like Intel for example with its CPUs and for computers. So these are the standards that allow the simplification at the transaction interfaces, so you can plug and play that's basically it. So there's just a huge army of platform complementors that build to these systems. There's now open-source resources that are that is in a sense are both modules to the system but also can set standards like Linux. So in the end we have this dense ecosystem, and I think what I'm going to follow up on and stress mostly in my remarks today is the geographic patterns that have come up underneath this incredibly complex system. So we've done research on the mobile handsets, handset industry by looking at tear downs. We have about 1,000 tear downs going all the way back to 2005. But this is just the tear down structure for about 40 handsets that were produced in 2019 and we broke it down by the ownership the headquarters ownership of the of the component source. So you can see in CPUs or application processors and the modem functions of the phone, the US has a strong predominance there. Also in network functions radio functions, the RF modules then we have a whole bunch of other wireless: wi-fi, Bluetooth, et cetera, which is more disperse. I just put some names in here so we know we have shares from all the companies, but I just wanted to give you an idea of who we're talking about here. Then in memory Samsung is dominated also in displays for through these 40 mobile phone handsets.

Okay, so I just want to dig in a little bit though. Here's these same functions and just a little picture of these modules inside of the phone in different functions, but this has been a process of functional accretion over time with more and more and more functions as we all know being loaded into the phone, with more and more modules and standards within the phone. But if you dig back even deeper into the application processor, all of these things are controlled inside the application processor or with it which speaking or the CPU is being the traffic cop that's inside the phone. And this can be packaged into a system on a chip, but more likely has discrete components and high-end phones. But inside of the multi the RF function, you have a lot of specialized modules and dies and chips inside of there. And then inside of this the application processor, the main part of the application processor, you have arm which is a power management IP block so just second of software is on the hardware which is dominant in 90 percent of all mobile phones. And it has about 800 complementors that are building tools and other products to help mobile phone companies design products using ARM. So it's just a multi-layered thing. And then we have the operating system, right, don't forget that. So android is about 80 percent. So let's look at android we have another data set of commits to Google's android distribution phone OS, and all the way back to 2008 is about 10 million commits, which are basically contributions of code by engineers in an open source model. So here we have Google with about 23 percent and other US companies with 31 percent. So total US companies about 55 percent of the commits China 0.4. But of course, a lot of that 0.4 is growing in recent years. So we can talk about the motivations of why and how this all works, and the motivations of the different companies and the individual contributors, but I don't really have time to dig into all that. But basically, this is an operating system that's used in 85 percent of the world's phones.

[02:05:00]

but there's other standards too and other ways I've talked about the different types of standards. If you look at the second column, de facto standards multi-stakeholder bodies and all of the folks that-- and we have and individual technologists all perceive themselves to be relatively stateless obviously not completely but we're operating global setting up global operations, serving global markets, and at the same time, ICT itself is enabling this distribution of work, the supply chain and enabling a little bit of coordination. But everything changed in 2018 really, with the Commerce Department's action but against ZTE was the signal that everything was changing. But really ZTE shut down essentially overnight about 94 percent of their CPUs are coming from Qualcomm, about $1 billion dollars in 2019. So this has changed the landscape it hasn't filtered down into open source, which is protected by First Amendment rights; it's not subject to export controls, or to these multi-stakeholder bodies. And Open RAN I think is a really interesting case. In a sense it looks like from the outside to be set up to be able to keep China out of the 5G system. But obviously as Melissa mentioned, the Chinese companies are joining, so this is part of a bigger system. Let's look at semiconductors which we mentioned several times today already. This is a great chart by our friends that created this earlier this year, by our friends at this SIA and the Boss Consulting Group. It's really in a fantastic map because it's looking at, excuse me, the whole stack of the semiconductor supply chain and allocating value added by different countries. So I guess I just want to point out that the US is very strong in many of these sectors and US allies are strong elsewhere. But if you look at the at China in terms of its contributions to the whole semiconductor ICT value-added stack of nine percent, but they're consuming 24 percent of the world's semiconductors, you can see that this mismatch is created a lot of pressure,

accelerated pressure that was already in through their own policy and five-year plans over many years, these the techno nationalist idea of developing their own technologies and coming out from under some of these licensing agreements. So what we have then is the state intervention ramps up to bolster the semiconductor industry, not just in China but across the world. So this is a system. We call this Massive Modularity with these multi-layered systems with modules tied together with standards, obviously operating in semiconductors, mobile telecom, computers servers and all digital services. But I think that it's obvious that this digitization of business process is driving itself through the entire broad economy. And I don't really need to say much more about that. I think that it's self-evident. But it means that this is an important-- so I'm just going to wrap up here. Some implications for policy... If the industries, not just ICT, but the industries that are becoming where ICT is driving more to the core are moving in the direction of massive popularity, the policy direction is right now moving in the opposite direction, if you look at it in a simplistic way at least. So China's attempt to rebuild the entire semiconductor supply chain inside of China is probably going to fail and/or cost them a lot of money and a lot of resources and further human resource development. On the other hand on the US side, the idea of picking critical components is in such a complex massively modular and global industry, it really requires a level of detailed industry knowledge or exquisite -- as Matt, it was the term he used application of policy and building a policy -- that may not be manageable. And there's a question about how to actually do that, and also come with this big price tag for various for selective reassuring, $50 billion dollars gets you about two and a half FABS. So it's an it's a question of how to pick your spots and how to build in securities in some of the in the systems that were being described earlier. But the big point I want to make is that US-based companies are in a really strong position throughout this whole supply chain, and when close allies are added, it can

[02:10:00]

be considered dominant with just a few exceptions. So I just want to say something about cyber security which is certainly not my area of expertise, but it seems to me that one of the big problems comes from this secretion of vertical and horizontal scope in the industry, requirements for backward compatibility we have legacy operating systems and compatibility built-in IP built in which just creates a whole host of back-doors. So I just think we need to consider the scale of these systems, we need to understand how specialized these systems are and the geographic specialization within them. And when you have geographic vertical specialization, geopolitical tensions follow right behind; and then to pay attention to the glue, the standards that holds us all together and the standard setting processes. So I'll stop there, thank you.

SAHAR HAFEEZ: Thanks, so much that was really helpful. I'll just make one observation and then I have a question. So as I mentioned earlier in June, we released the 100-day semiconductor study of the supply chain risk there where we did a pretty thorough overview of the sourcing risk that you mentioned looking at the various segments of the supply chain. So we're not going to be repeating that here; we'll refer to it of course, but we understand it's a critical piece of the supply chain but we will be referring to the work we did there, and picking up on it. Here, I think we might focus on the hardware security issues given that's something that's relevant to ICT, the ICT industrial base and how we can sort of pick up on the work that was already done as well as the PCB components which are pretty critical. Just wanted to point that out. But I really liked the

PowerPoint and all the great graphs that you had in there. Those are very useful for us, we love those, so thank you so much for your presentation. Because you're the academic here, we did want to ask you how we can maybe support your research and development efforts, how the government can support that? And really one of the things we're focused on is also prototyping so actually getting the great research that you do on to market. And so we'd be grateful for your views on how we could support those efforts, and really expand the part the partnerships that we have with you in this space. So thank you, that's my question.

TIMOTHY STURGEON: Should we take some other questions as well, or is there any anything else out there?

MONICA GORMAN: I've got a question if you'd like to compile a few of them. First thank you very much really just fascinating presentation and we'd love to see the study once it comes out. So look forward to you being able to share that. I think you very eloquently pointed out the challenges with massive modularity and trying to create policies around that, and so I'd be curious recognizing that reality, what advice do you have for us as we think about policy recommendations in the upcoming report?

TIMOTHY STURGEON: Okay, well I guess I'll start with that. I think that my job I thought-- was just frame the problem. I think that has already been mentioned: this is a global industry so the solutions are going to have to be global. The models are out there for international cooperation and through these extremely dynamic, but slightly siloed standard setting organizations, that companies basically cut carve out some of their time for their engineers to contribute to these to these efforts.

[02:15:00]

and I think there's it's just a question of rallying folks together to around a common problem. I think data security, device security is a problem that everyone faces but down to the individual consumer. So it's a well understood problem that we all face every day. So I think it's a Matter of taking some of the solutions that were mentioned earlier for trusted vendors, for better data, and basically, tracing devices and software through their life cycles. I think those are all great approaches to a huge problem, but it can't be done out of the US. Unless you're going to take the Chinese approach and tear the whole thing down and build it up nationally, which is one of their ideas. The other idea in China is to really ramp up their participation in these standard setting bodies so in 5G-- we did a whole study on TD-SCDMA, which is the Chinese standard back in the 80s and 90s, which it was the idea that they would have their own standard and everyone have to build it. It didn't work. But they did learn how these standard setting bodies work and so they've been much more active and now on Open RAN as well. So I think that the Chinese are there, they're active. So either we cooperate and or we do something else. I don't know exactly if it's possible to keep contributors from a particular country out. If you look at the Android chart that I showed, there's a big block of unknowns where we don't even know... We're just figuring out where folks have contributed by their email addresses, if there's a company email, for example, we assign it to a company. And so there's a huge block of unknown contributors. So these things cannot be opaque, and I think there's a lot of work to be done there. I guess my big message here -- because we're all talking about software and hardware -- is to also focus on the

standards, and the standard setting processes. Because none of this is going to would work-- when I say "none of this", none of ICT would work without the standards. So that's some it's going to have to be a multilateral engagement and the idea that any single company or country can just withdraw from this is I think a really hard sell. So I think that we will be happy to work more closely with you in our groups, relevant groups at MIT and in this these international groups I've been working with, and so I can reach out to you afterwards about that.

MAURA WEBER: Great. Thank you I understand we have some more questions, but we are going to move on to the next speaker. And note that we will have additional time following our final speaker for question and answer. So thank you Dr. Sturgeon again, for your presentation. Now we will hear from miss Courtney Lang, who serves as Senior Director of Policy with the Information Technology Industry Council. Ms. Lang, you may begin.

COURTNEY LANG: Great, thank you so much. And I actually do have a short presentation as well, so Dr. Sturgeon was not the only one to have a PowerPoint. So I will share that now as I just practiced right before this. Great, so thank you for having me here today. As mentioned, I'm with the Information Technology Industry Council. Briefly, if you are unfamiliar with us, we represent 80 of the world's most innovative technology companies, running the gamut of manufacturers, software developers, service providers, platforms. So we really have companies that are participating in all aspects of the global ICT supply chain, and that really leveraged the global ICT supply chain to provide their product services offerings, et cetera. We are a global trade association, so our companies are headquartered, again, all over the world, which I think gives us a unique perspective into global ICT supply chains as well. I will also briefly mention that ITI is the co-chair of the ICT Supply Chain Risk Management Task Force, so we are very familiar with the work of the task force, and the partnership, and collaboration, that goes on there, which also I think, allows us to have a unique perspective to bring to bear today. So we very much appreciate the opportunity to be here. Going last is always a challenge because I think many of the panelists prior to me hit on a lot of the points that we would also echo. And so perhaps what would be most useful for me to do at this point is to briefly walk some of the critical

[02:20:00]

components that we have identified in conjunction with our membership again, focusing on hardware as Sahar mentioned -- the focus of this report will be on the hardware side of things -- and then talk about some of the risks and challenges that we have identified in larger buckets. I know that Melissa talked a little bit about that earlier so I'll just go through that briefly. And then I think I'll focus the brunt of my remarks on our policy recommendations and things that we think the U.S. government can do to really facilitate supply chain resiliency more robustly. I think everybody has noted the pandemic, natural disasters things of that nature, have really I think brought into focus the critical nature of global supply chains, and really areas that might be considered particularly critical. It's also highlighted I think specific products components, et cetera, that might be at risk or face specific challenges. And so that's where I'll focus today. So starting with some of the critical components in hardware that we identified in conjunction with our membership as being particularly important to the global ICT supply chain that may also face certain set of risks or challenges, I do think that again, this was touched on in some of the

earlier remarks, depending on what product or component you're looking at, there may be different risks associated with those products. And so each of these areas some of the risks may be the same some of them might differ on my next slide I talk broadly about the risks I'll get to that in a moment. But obviously we've heard a lot about semiconductors, advanced and mature integrated circuits, as being particularly critical components to the global ICT supply chain. Of course they are foundational to pretty much every ICT product. I'm not going to get into that in great depth we've already provided a set of comments in response to the first semiconductor RFC informing the 100-day report, as well as are working on additional input now. So I won't get into that in great depth but obviously just wanted to flag that they are in fact critical. Another critical component that we identified in conjunction with our membership is displays or LCDs. This is one component that actually does require specific driver integrated circuits and there are some issues associated or challenges associated with that. Hardware that performs interconnect functions so things like USB connectors, high-speed, high-bandwidth cable connectors, IC sockets things of that nature: not a whole lot of U.S. production of those so there is a risk associated with that. Printed circuit boards of course another area that we had identified as being particularly critical, and also that may face specific risks; rechargeable batteries, I know Tom mentioned those at the outset; rare earth elements to just name a few. I know that there are several other reports that have been focused on both batteries as well as the rare earth elements. So again, we don't get into those and I won't get into those in great depth here today, since I think that the USG is already exploring those areas in great depth-- but did want to make the point that those are critical to the global ICT supply chain more broadly. So just to talk at a high level about risks to the global ICT supply chain, big buckets of areas that we and our membership identified. I would be remiss not to point out that one of the supply chains management working groups, the Threat Evaluation Working Group has taken a look at a series of threats that face the ICT supply chain. I think that this is a really solid starting point to understand the wide array of potential threats and risks to global ICT supply chains. I just highlighted some specific ones here that we also look at in our forthcoming comments, but certainly risks associated with the insertion of counterfeit parts, legal risks that might impact the supply chain. So what by that is things like weak anti-corruption laws, a questionable regulatory environment, or a weaker regulatory environment, economic risks such as the financial viability or stability of particular suppliers may then impact suppliers down the line. Obviously, cyber security risk: this is something that I think Tom talked about a lot in his presentation, among other things. So those are all areas that we think are important to note.

[02:25:00]

Another bucket of risks that we identified were barriers to trade. So specifically, we look at the impact of tariffs and especially, Section 301 China Tariffs that continue to pose problems for companies in terms of sourcing specific components as well as other ongoing WTO tariff negotiations such as the moratorium on electronic transmissions. Another big bucket of risks we identified are climate change natural disasters. Again, I think we've seen the ways in which these unexpected disasters can impact global supply chains. Also related to risks in transportation and logistics throughout the global pandemic, cost of transport has obviously gone up. Beyond that, components go back and forth; it can sometimes cross over 20 borders to get into the united states and so disruption to this can definitely pose a problem or a challenge global ICT supply chains. And then the final area that I want to hit on, gaps in human capital or gaps in workforce.

Certainly one of the areas we believe is a risk at least from the U.S. perspective to global supply chains is around the necessary skill-set and training for supporting advanced manufacturing and some of these other more advanced capabilities. Certainly another area that we think the USG should consider how to focus on. Moving along and my last big pitch here is around the policy recommendations, things that we have developed in conjunction with our membership, that we hope that the USG can consider as they are figuring out how to approach and improve supply chain resiliency. I'll just talk through these briefly, there's quite a lot on here. I did not include every single one that we will include in our submission, but just some top-level ones that I thought were most important at the outset. The first one being -- and I think this is a course that you've probably heard from ITI and others quite frequently -- but the importance of streamlining supply chain security policy making activity. There is absolutely a patchwork of different supply chain security policy happening across the USG; it's made for a pretty confusing landscape. It's made it more difficult for companies to understand what they need to be doing and how to comply. So to the extent that the USG can streamline that activity, we believe that would be incredibly helpful. We did put out a set of recommendations around this earlier this year but I think one of the key ways in which we think this can happen is by designating a lead supply chain risk management agency to coordinate all of these various efforts. I'm not going to name every single one of the supply chain security or resiliency related policies at the moment-- I know the tiger team has put together a pretty robust catalog of those. But the point remains I think streamlining it would be helpful. Secondly, leveraging public-private partnerships to address ICT supply chain challenges. Once again, we are co-chairs of the SCRM Task Force. We think this has been an incredibly successful partnership model and it seeks to address challenges in a variety of different spaces. So really moving forward, continuing to leverage this this type of partnership and utilizing the SCRM Task Force for example as a focal point for this engagement, we believe will be a useful endeavor. Again, it's not just industry responsibility, it's not just the government's responsibility: it really requires communication and partnership between the two to address risks. Thirdly, we recommend strengthening the technology workforce and focusing on how to develop skill sets and capabilities to support advanced manufacturing across the ICT industrial base. As I mentioned one of the risks that we identified in collaboration with our membership was human capital gaps and so really focusing on improving stem education computer science training things of that nature, as well as ensuring that there are programs in place to attract foreign talent from around the world, recognizing that there is top talent that we can recruit from elsewhere is important.

[02:30:00]

Enhancing cooperation with global partners: I think this point has already been made already and I understand that the commerce department is also already thinking about this. It's present in the RFC asking about what allies and partner countries are doing on this, so just really making sure to continue those engagements and figuring out to the extent possible how to align approaches or how to best create a global approach to addressing some of the identified challenges or risks, will be incredibly helpful, again, because it is a global ICT supply chain. I mentioned the tariffs earlier, one of the recommendations we make is figuring out how to address the negative impacts have resulted from those. I think Melissa also made this point earlier, but avoiding the wholesale reshoring or repatriation of supply chains. Again, there are benefits that come from the global ICT supply chain, and fully repatriating global the ICT supply chain to the US will not be cost

effective; it will undermine U.S. competitiveness, and it really undermines this idea of comparative advantage international trade. And, certainly, there is a resiliency component to this as well. If you have diverse supply chains especially in terms of geography, if something happens in one portion, then you have the ability to source from another portion of the supply chain. So just wanted to make that point. And then obviously we've heard this from several folks already, but again, noting the foundational nature of semiconductors, we recommend quickly moving to fund the chips for America Act and then further implementing the FABS Act. So I will stop there. Let me end my screen sharing, and I am happy to take any questions from folks today. Thank you again.

MAURA WEBER: Great. Thank you. Any questions from the panelists please raise your hand or speak up?

KEVIN COYNE: Kevin here. We've heard a lot about trusted vendors, and obviously your recommendation was not to bring back supply chains domestically. What are your thoughts around near-shoring or other sort of trusted vendors: how would that go into that recommendation? Obviously we've talked about the global supply chain and the impacts of this industry, how do we really delineate who's trusted and who's not trusted if the there's concerns around the standards that have been set forth might have some bias in them? What can we do to really help influence that effort?

COURTNEY LANG: Yeah, so this is actually an area that we have explored in the context of our more broad policy making advocacy is this idea of trusted vendors. And I think one of the challenges that we see is that at least in the U.S. and then also with some of the conversations we've had with global partners, I think there is to some extent, a lack of agreed upon criteria for what constitutes a trusted vendor. And I do think that is an important area that requires additional conversation to try to come to some understanding of what that means and what that looks like in practice. Certainly things like the Prague Proposals are a good starting point but I think more needs to be done. I also know that in the Supply Chain Risk Management Task Force there has been some work done on vendor attestation and practices that specific vendors might undertake, that might indicate that they are doing things that may make them a more trustworthy vendor. So in terms of how it fits in, I think we do need to continue to talk not only amongst ourselves but with our global partners to try to figure out, is there some sort of criteria that we can leverage globally to understand what constitutes a trusted supplier? Certainly, we agree that leveraging those sorts of suppliers is important to facilitating resiliency in the global supply chains.

KEVIN COYNE: That's helpful, thank you. Because I know when we go out and we do our export licensing-- we trust what you what you've told us in your export license but then we have agents who go out and verify, the item ended up where it was right. And I think it's tough because industry doesn't necessarily have that authority, and then when you look across various countries, those authorities are in flux.

[02:35:00]

So I think obviously leaning on those global arrangements and international treaties is extremely important to ensure that the supply chains can be trusted and verified to a degree.

SAHAR HAFEEZ: Yeah, just picking up on that point we would be very interested in-- I think that it's a great point that you made about having those conversations and criteria, that we can agree upon not just here but with our allies and partners. I think that's a very good point. We would be interested in any recommendations you have as to what's a trusted vendor, what goes into that, what the criteria are, so we can just to inform our thinking. We appreciate that you're on the ground here working on this, so you have very useful insights to inform how we might be thinking about this. So just wanted to flag that as something that we'd be interested in your thoughts on, and if you want to come back to us with that, I think that's fine. You don't have to talk about it here if it's more conducive to a follow-up, but just wanted to flag that. But really appreciate your presentation and recommendations. Also wanted to touch on, I appreciate that you touched on the human capital gaps. We're aware of the STEM issues, that's something we're focused on. What about some of the other gaps that are in other parts of the supply chain, not just the high skills but are there others that you'd want to flag here more sort of on the manufacturing side? The tech technicians that we'll need? Any of the other sort of skills that are relevant here, that you want to highlight in terms of gaps that we have that we should focus on?

COURTNEY LANG: Yeah, so maybe just a few other areas to flag aside from the high skilled portion of things. I think beyond that, one of the areas that we've identified in conjunction with our membership is a need for additional skill-sets that support things like working the manufacturing line, things like inventory control managements, skills that can really support program process and product management, and then procurement management more generally. So those are all areas that we think are also important to address. And then additionally, I think skills that can help with administration of quality control, and other potential engineering issues as well, are areas that we think would be helpful to strengthen.

SAHAR HAFEEZ: Thanks, that's very helpful. Any other questions?

MONICA GORMAN: Just in addition to workforce, you noted in your policy recommendations once, in the importance of funding the Chips Act but also that not everything can be re-shored. I'm just curious how you see investments in the U.S. as compared to those in Europe and in Asia over the years and are there any additional steps that you might recommend for the U.S. government to take that would accelerate investment here for the production that we would like to see within our borders?

COURTNEY LANG: Sure. So unfortunately I don't have any specific statistics, though I think it has become clear especially in the semiconductor space how investment is going in Asia versus the U.S., which is one of the reasons that the Chips Act has been so important. One of the areas that we are still exploring and might be useful to consider is whether there is a way to additionally incentivize in the form of tax credits or investments: ICT protection of some of the other critical components in the U.S., or perhaps around final assembly in the U.S. That would be perhaps an easier aspect to address than specific components writ large. So thinking about whether something like the Chips Act might be beneficial for other specific or discrete components for ICT supply chains, through the course of this report, perhaps there will be a trend that emerges in terms of components that have been identified as particularly critical. So

potentially something similar to the Chips Act but for other components or for final assembly of those components.

MAURA WEBER: Great, thank you very much Ms. Lang. At this time I want to open it up now to all speakers to answer for the panelists to ask questions. So please panelists indicate who you would like to ask a question to,

[02:40:00]

whether it's a specific speaker or all the speakers, or if you would like to open it up to have the attendees respond. And please, attendees that would like to respond to a question posed to the group, please, indicate using the raised hand signal on WebEx, and I will call on you to respond. So with that panelists, do you have a question for the group?

MONICA GORMAN: I'm happy to open it up to a general question. So we've talked a lot about the need for cooperation with our allies and our global partners both public and private sector. I'm just curious would any of the panelists have recommendations in terms of specific topics, technologies, countries or regions that they would recommend that we prioritize? We talked a bit about the trusted vendor concept, but I would be interested beyond that, if there are other specific areas, countries or regions they would recommend prioritization? And I'll throw that open to all of the speakers.

TOM QUILLIN: Hi. This Tom Quillin. And I'll take a shot at some thoughts on this topic. I think there have been some interesting initiatives in the space of tech diplomacy over the past year or so, and one notable one from Purdue University's Center for Tech Diplomacy, and other efforts that I think are really important to highlight the need for the need to supplement or augment trade focused conversations with our diplomatic focused conversations. And I think that's an area that maybe hasn't been explored enough quite yet and that's a key opportunity. Another opportunity I would look at-- I would reinforce Dr. Sturgeon's points about global standards bodies. And while there might be debate about the right role for governments and in global standards bodies, it's clear that those are vehicles for arriving at common solutions, driving costs from novel technology approaches to commercial product. And especially in the space in some of the initiatives that I talked about where some of the approaches are new, and solutions are not mature quite yet, in many cases, I think it's going to be really important for standards bodies to support work that is implementation-focused and drives towards commercializable, valuable solutions. I appreciated Bob Kolasky's point about small medium business and value: I think that's really a key area of opportunity.

SAHAR HAFEEZ: Any other thoughts on this question?

TIMOTHY STURGEON: Yeah, this is Tim Sturgeon. Just to come behind that a little bit. I think that one of the things-- it's in my presentation but I didn't stress it very much is the consolidation of the individual markets within ICT. So because of the specialization and the high technical capabilities required to be at the leading edge and to be successful in the market within these niches of ICT, plus some companies are really good at playing the patent game and protecting their position; there's big platforms that have these network effects that drive out have

winner-take-most effects. So you see consolidation within each of these. So you don't have consolidation overall in ICT but you have you have consolidation in each piece. So you already have a situation you have a series of concentrated markets. You also have all the complementors.

[02:45:00]

It's very open so you have complementors building to these, to the standards that are developed by these leaders. I'm just coming back to Bob Kolasky's question to Tom Quillin about small to medium-sized companies, and a lot of the innovation happens in those types of organizations. The risk really is that you the compliance through trusted vendor and other types of onerous requirements for supply chain visibility which sounds like a fantastic thing, can really drive this consolidation further. And I just want to point out that consolidation is really-- it's not just a geographic-- just if things were geographically dispersed into tiny organizations everywhere, there'd be a lot less risk. The problem is the risk and the geopolitical tension comes from the fact that you have concentrated markets that are that are concentrated in particular countries. So I think there's a huge tension there between setting up these systems and keeping the innovation engine running, and not driving this consolidation further, which would maybe exacerbate the problem.

SAHAR HAFEEZ: That's a really good point. And that's something we're really looking at in terms of diversification of sub-supply chains, because there is the concentration anywhere creates challenges even in partner countries. Because we've seen with weather events and things like that they can just have impacts that really run through the entire supply chain. We saw that particularly with the Delta spike recently and the impact that it had in the packaging segment of the supply chain, which is really geographically concentrated. So that's a very good point. Another question-- oh sorry we're were you going to say something Matt? Why don't you go ahead on the international cooperation. I wanted to talk about a more specific topic. Thanks.

MATT TURPIN: Yeah, I think to a certain degree a rationalization of the various actions and lists in terms of trusted vendors of where the US government has taken action already and is sort of communicating through sanction or other regulatory actions against a vendor-- and making that commonly known across industry. Right now you would have to search across sort of multiple lists to be able to find where that overlaps. And the other part is an understanding of sort of subsidiary parent company relationships so that you can see that much more easily and lay that out. And obviously, for some for some countries, that's easier to be able to do and others seek to conceal that. And really having government to weigh in and sort of make a determination, this is what we see as the as the parent subsidiary relationship, and therefore, folks can be able to sort of make better determinations of their own risk.

SAHAR HAFEEZ: No, that's a good point. I'll just put in a plug for… I there is a consolidated list that includes the BIS entity list, the OFAC, SDN list as well as other lists; there is that consolidated list. But I take your point about the subs that is, sometimes, that it's -- I don't believe -- part of that list. But also sometimes it's not clear who the subs are, so that's a good point, and that's a well-taken point. So I appreciate that. I wanted to ask about this issue I think we've touched upon this a little bit but I just wanted to get everybody's views on the issue of how we could advance transparency in the supply chain and if anybody has could comment on one of the

we've talked about the semiconductor supply chain and lack of transparency there, and there's a whole we're trying to focus on that. But more broadly, I think there's just so many tiers here and there's opacity there's not a lot of visibility into your suppliers and the sub-suppliers. And curious if anybody has thoughts on that piece; and also how as we're looking at, to Monica's question, about engaging with our partners and allies, how we can leverage those fora that we have to move forward on transparency?

[02:50:00]

Whether there's useful and appropriate ways to share some data that regarding suppliers and just having more visibility into supply chains if there's any-- just your thoughts on how we might proceed on that issue and how we could leverage our existing dialogues and other dialogues with our partners on to advance transparency? Thanks.

MAURA WEBER: Any speakers that would like to take this question?

MELISSA NEWMAN: This is Melissa I will speak up and I'm going to talk about this in terms of our SCS 9001 standard, our standard, and I did not mention this when I talked, has actually benchmarking capabilities which anonymize benchmarking capabilities, which can show trends and show areas where you need improvement. And that is an element of transparency. And we are actually very excited about that because we have seen in the quality programs that we manage, it's that benchmarking and system that actually leads to continuous improvement.

TOM QUILLIN: Hi Sahar, this is Tom Quillin. I'd like to just share a couple of thoughts as well on this one. I think one issue isn't transparent. There are several sort of sub-issues and transparency, there are issues around understanding the status of inventory and inputs and outputs, the kinds of issues that the Department of Commerce is tackling and the semiconductor study. But then there are other issues around, as you said, upstream and downstream suppliers and having insight into tier-2, tier-3 suppliers. I think a challenge that's common across approaches to trying to address these issues is that there are initiatives that aim to provide greater transparency, and in some cases, the beginnings of commercial products that help address those. There are commercial vendors today who have risk analysis tools and apply an AI technology to digesting information about the thousands of suppliers who go into a product integrators supply chain and work to identify trouble spots or weak spots or points of vulnerability down out to 2nd or 3rd tier. And there are other approaches around doing things like stress testing. There's another professor at MIT, David Simchi-Levy, who has an approach around stress testing, that is a systematic way to look at supply chain nodes. And there are some of the some of the tools that I talked about around having the capability to have a device own its provenance information throughout its life cycle, or having that information be available to the point where it can communicate suppliers and country of origin of those suppliers throughout the lifecycle of the device. All of those things are I think novel and important approaches to addressing these kinds of questions about transparency. But I think there is a lot of room and opportunity to advance those solutions, to increase automation in the process, to mature them to have broader use of those kinds of tools, so that, they become they become more cost-effective solutions and are easier for more and more companies to adopt.

SAHAR HAFEEZ: Yeah, and that's very helpful: it also gets to the role of government versus the industry and private sector.

[02:55:00]

One thing is maybe we could have, with our international partners, some sort of standards and then the industry should follow when it comes to transparency standards that we can endorse collectively. That might be one way we could be helpful, recognizing that industry is best suited to address some of these issues and challenges as well. So see it as a part partnership. And this is a question we ask a lot, what is the role of government? How can we be rather than unhelpful? Because that that can happen as well. So any other thoughts or questions?

MAURA WEBER: Yes, I believe Courtney has a comment and then I'll turn to Bob Kolasky for the next question. Thank you.

COURTNEY LANG: Thank you, sure. Just to quickly touch on a different facet of that. But I think it's worth noting is earlier you asked questions about sharing data information with partners and allies. I think that's an area worth exploring. I know that at least in the context again, of the Supply Chain Risk Management Task Force, there was a working group that focused specifically on challenges around supply chain risk information sharing. Whether information is available in a standardized format is this except is it accessible, et cetera. And so in the U.S. I think challenges still present around that and around sharing that information. So when you're thinking about how do you share that with allies and partners, I think it's something that's worth exploring: is there a mechanism by which this sharing can occur, and are there particular things that need to be in place to ensure that folks that are sharing that information are sufficiently protected? How do you best allow for that information sharing with partners that are outside of the United States they might be considered allies? But exactly how that mechanism would work I think is something worth exploring, but really be being able to share that information freely back and forth I think will be a helpful way to further improve transparency as well.

SAHAR HAFEEZ: Great. I think the only comment I'd make is we have to obviously be careful about the sensitivity of information. I think one of the things that is useful in that regard is looking at what our capabilities are versus other countries; that's something that doesn't get into company-specific information which we share, but it does talk more broadly about our capabilities versus risks and that is something. So we're very cognizant of that issue as well when we look at information sharing and what we are comfortable sharing. But that's a something we're thinking about as well, and that's a well-taken point. Yeah, I think Bob had a question?

BOB KOLASKY: Thanks, Sahar. On the information sharing, I think the word Courtney referred to it has a good sort of frame of different types of information and different levels of risk and where there should be willingness across that, so I do reference that to everyone. My question returning to small businesses but coming at it from a different direction. We've been talking about existing small medium-sized suppliers, but I think one other aim should be to encourage more small and medium-sized suppliers here in the U.S. to stand up businesses, to innovate, right, that's such a source of innovation. And so what can we do? One of our goals is to have a stronger industrial base, what can we do as government and industry to send the message

that there is more opportunity here? And really signal to that these supplies, like ICT stuff, is something that we want innovation from American small businesses.

COURTNEY LANG: I'm happy to jump in first if no one else wants to, and then we can go from there. So I think one of the ways in which signaling this to small and medium businesses can occur is, I think there are a number of ways part of it-- I think is a communications messaging type of scheme, in addition to them taking action that backs up those words. But really I think focusing investment and elevating investment in critical technologies and making it clear that is a national priority will signal to some of those small and medium-sized businesses that it truly is of great importance to the Administration and to the USG, and will hopefully from there spur them to further invest. But I do think figuring out where those strategic investments make sense and what baseline capabilities are required in order to underpin the ICT industrial base will help small and medium-sized businesses understand where those opportunities are and where they might be able to be most competitive or innovative in the US market.

[03:00:00]

TOM QUILLIN: I really appreciate Courtney's comments and would agree with those; and Bob I think that I don't know that small businesses are scanning the annals and journals of standards bodies to for their best start-up ideas. But when standards are working well, they are making innovation easier and removing barriers to innovation for all kinds of companies, including small medium businesses. And so I'm hopeful that as standards for transparency in all of its flavors matures, that what we're really doing is seeing more ways for, and more methods for, start-up businesses to create a solution that is that is commercializable and scalable. One example of this I think is there there's a lot of work around different data formats. And data formats for sharing information are really important, and there are several different data formats for sharing information about what's inside ICT technology. But what gets lost sometimes in the debate over which data format to use is-- the goodness that comes from having those data formats is that they they're they could be the sort of core functionality that fuels innovations around tool sets for IT to use, for example, in digesting, storing and updating and maintaining information about what's deployed out in the enterprise, for example. If these kinds of concepts that we're driving for greater supply chain transparency are going to be important, we have to make sure that those tools are easy to build and adding value to large organizations, whether they come from start-ups or are mature companies. So I'm excited about that prospect to see those kinds of standards fueling innovation.

MATT TURPIN: And Bob, one thing I'd add is going back to Tim Sturgeon's slides, the business models that that we have sort of existing today as sort of he pointed out in the middle there, was set up around a certain set of sort of geopolitical realities. And as those change, different business models become viable. And so to a certain degree, I think what we're seeing is a degree of experimentation and an effort to understand the degree of certainty that there is of whether sort of this changing sort of international landscape is something that's permanent, or whether or not you're going to go back to sort of an old normal. But as it becomes sort of more ingrained that fundamentally sort of the assumptions of how an ICT industry was set up, over the past two or three decades, that a number of key assumptions are beginning to change. Well that will cause new business models to arise right. And I think to a certain degree, from government's

perspective, it's probably the interest to sort of observe that happening, think about those sorts of characteristics that you would want to encourage, and then, think about the tools and authorities you have that would shape those sorts of outcomes. What are the sorts of attributes that you'd want to see from those business models come out, right? And it is highly likely that those small medium-sized businesses that are that are rapidly trying to take advantage of sort of these this new landscape aren't necessarily going to raise their hands and advertise the world of an opportunity they're taking advantage of. And so to a certain degree seeing what that new landscape will look like is a bit of a trailing right: we're only going to observe that sort of after the fact right after there is a new model that's been established and sort of been proven.

[03:05:00]

I think to a certain degree that's the reality of sort of where we live in today in the changing landscape of how this is being set up is that folks are experimenting on what it looks like. I think for you all thinking about the attributes you want right what; or, what are what are the sort of the boundaries of what you would want? You want a diversified supply chain that comes from a number of different areas that certainly the US has a piece of, but it is diversified and we've got sort of multiple areas to go through. What are those sort of critical vulnerabilities that you would you would want to make sure that are minimized as much as possible? That would be the things that I would think focusing on right now would be the key.

MAURA WEBER: Great, thank you. And I think Tim has a comment as well and then I'll turn it over to Monica Gorman for one of our last questions. Thank you.

TIMOTHY STURGEON: I just want to follow up. I think that standards absolutely create business opportunities, but standards come in different flavors as I was trying to point out. If you think about Apple's iPhone, came on 2007, and Android in 2008. By 2011 or so, Android was dominant it created a huge opportunity for apps producers across the world. I guess there's government regulations which also create opportunities. But the international and modular nature of the industry-- modular and that folks work on their own inside their own module. And then who knows who what other folks do with their module. That's why this industry is so innovative. I think that government, regulated approach is going to be created with a lot of skepticism. So between the dominant FANG companies, following their lead, whoever vendor comes out with the best model software for doing the trusted vendor for example or tracing supply chains and government regulation, again, I think the organizations that folks are used to working with are these international standard setting bodies. So they're international; they're not owned by anybody necessarily, although individual companies have strong hands in some of them, like 3GPP. But I think that's maybe the place to focus in terms of developing these types of standards. But once those are in place, absolutely innovative. I just want to take a very brief moment to talk about the workforce issue and say the obvious thing that immigration policy is crucial for innovativeness of the United States. I've been doing a lot of research on AI implementations in manufacturing and in financial services in the last few months, and again and again, run into key technologists that are not or they're foreign born either South Asia, China, Turkey, Mexico, you name it. But this is a these are crucial people and I think they need to be made to feel welcome.

MAURA WEBER: Thank you for that. Monica, do you have a question for the group?

MONICA GORMAN: I do we've had a lot of discussion here about standards. It's been very helpful and I'd like to drill down into that a little bit more, and just hear the speakers' thoughts on are there specific steps that you would like to see the U.S. government take? And if we think about representation in these standards bodies, we could be talking about government representation whether that's U.S. or otherwise; we could be talking about large multinational representation; or we could be talking about SMEs. There's a variety of different types of representation: what would you recommend we think about as we think about the influence of these standards bodies?

MATT TURPIN: Maybe I'll take a real quick bite so others have a chance to think about it as well. I think certainly taking a look at what Beijing has been doing to insert itself into standards bodies, and for the U.S. government to simply examine that closely and determine what we think is sort of inbounds and out of bounds and be able to talk very publicly about that-- we've seen a significant effort by the Chinese government to insert itself

[03:10:00]

into various technology companies headquartered inside the PRC, with increasing sort of influence control over those. The status quo is not static; their participation is likely becoming much more state directed. And so analyzing that and understanding what that is, and what impact that might have, that should then maybe determine the level of influence or participation or assistance that the US government provides to maintaining what is supposed to be sort of an apolitical, technology-based, technical based consensual process. So and I think you're thinking about those independent bodies and then to a certain degree how they relate to various sort of UN bodies like the ITU and others that increasingly appear to have some degree of influence and control by powers that don't necessarily ascribe to that broader concept of sort of a multi-stakeholder, technical standards being the basis. And so I think what's needed is that the U.S. government is sort of thinking through what that looks like, and then being able to take steps. And that doesn't necessarily mean you have a seat, at that body, but maybe you're making it much more public about others' sort of manipulation of those bodies to achieve outcomes. And we may find that in fact it hasn't been successful, which could then reassure us all that these things are still being conducted fairly and we're getting the right outcomes.

TIMOTHY STURGEON: If I can just follow up on that I think Matt's comments are incredibly right on. And I think taking a close look at this process, it reminds me of the internet it came at first isn't this great and then also uh-oh. So there's a lot of the folks who are participating in these standard setting bodies, they're engineers, they tend to be relatively political. And if there's a there are groups that are behind the scenes being driven by state actors, these folks are not equipped necessarily understand that or react to it at all. So it's I think overdue to. And we've seen this in other areas too international standards or international bodies like this flap over the WTO a few years ago and China's influence there. So I think it's overdue to take a close look. But having a government official sitting at the table: what are they doing there? Because what's happening is engineers are hashing out these incredibly arcane technological details in order to come to this consensus over-- and it's a very long process in many cases. So I just think that and then we haven't even talked about open source which is even less structured. So if you think

about Linux running everything under the sun except for your computer, what's happening there? It seems like something that is overdue to be looked at.

COURTNEY LANG: I'm happy to also jump in with some perspectives on that question. I think in general as Dr. Sturgeon was just saying, there are generally engineers that are participating in these standard setting or standards developing organizations. So there may be some areas where it is appropriate for the USG to be involved, but certainly in our view what the USG can do is really support those standards development organizations where there transparent rules-based processes already in place, and making sure that industry is able to participate in those accordingly is one way in which we really think the USG should be supportive. Beyond that I think one of the things that we've seen more recently is that policies and regulations have in some cases unintentionally prohibited US companies from participating in standards bodies. So moving forward, making sure that any regulations or policy measures don't do that, whether unintentionally or otherwise--

[03:15:00]

because that does create problems for companies, U.S. companies, other companies that are seeking to participate in these rules-based organizations. So I think those are two areas that are worth considering. And really beyond that I think one of the challenges is there is meetings, or there are meetings, that take place all over the world, so figuring out how to make the US a more attractive location for some of these standards development organization meetings things like that, just, logistically making it easier for US participants to get there I think is something to consider as well just on a really base level. So those are a couple of areas that I would highlight.

SAHAR HAFEEZ: Logistics are very important as we're realizing, but it's not something I would have thought of in this context. But it's actually a very good point so I'm glad you brought that up. I do want to say, we really support U.S. participation in standards. That's a very important goal for us for all the reasons that have been talked about-- I don't need to repeat them. But I'll say that your point Courtney, in addition to the logistics points which was very good, the point on making sure that any actions we take don't impede U.S. participation in the standards is also something that we are focusing on, and it's important to us. As you know, couple of years ago we did make some changes to make sure that does happen and we and that's something that we keep in mind as we as we take some of the actions, the regulatory actions, against parties of concern. But we totally agree with that sentiment and support that. So yeah, was that the last question? Or any other comments questions?

MAURA WEBER: Yes. I believe we are at time for our questions; thank you all very much, to our speakers for your thoughtful presentations and remarks. I'm going to hand it over to the U.S. Government Panel for to provide any final remarks. So please indicate with the raised hand function if you'd like to give some final remarks. Thank you.

SAHAR HAFEEZ: Okay, hearing none, I'll just close us out here. I want to, first of all, really apologize for the technical difficulties in the beginning. I'm sorry that we started late but this was a very useful and robust discussion. I want to thank my colleagues on the panel, and want to specially thank Maura and Erica and everyone for doing such a great job with organizing this

forum. It's not easy to do, so really want to thank you all. And I want to thank the speakers as well as everybody that log logged on. We had a number of people here. These conversations are very important to us to inform our efforts, and we see this as a partnership with industry as well as a dialogue that will continue and expand. I guess one of the key themes that came out of this is that we can't do this ourselves and we really need to work with you and in partnership with you to achieve our shared goals. And so we want to continue the discussion and really appreciate these opportunities. We learned a lot and we look forward to the comments that are due on November 4th and incorporating your insights into the report that is due in February. I assume you all have the information the docket number, which I see Erica put on the chat. So in closing, I'll just say a transcript and recording of this forum will be available on the BIS website in the next seven business days. So look out for that. And just want to thank you all and hope you have a good weekend. This this concludes this session. Thanks, again, bye.