FINISHED FILE

INTERNET GOVERNANCE FORUM USA 2021
FACILITATING INTEROPERABILITY - BRIDGING THE GAPS IN SUPPLY
CHANGE SECURITY
JULY 15, 2021
10:30 A.M. - 12:00 P.M. EASTERN

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1 877 825 5234
+001 719 481 9835
Www.captionfirst.com

***

***

>> MELINDA CLEM: Good morning, everyone, and welcome to day two of IGF USA. Excited to have you back here today. We have another action-packed panel of experts to start us off this morning, and a special fireside chat. But before we get started, I want to make one housekeeping update.

Just a reminder that we have a closing reception today. We will need you to register in advance. So in your email link, with today's link to Zoom, you will also find another one for the closing reception. So please remember to register in advance and join us. The cocktail -- the special session crafted cocktail menu is also available on our website. So we hope to see you all there.

So this morning, we are going to get started with a topic ripped from the headlines, cybersecurity and the safety of our supply chains.

We start today with a special fireside chat with Nathan Simington. Nathan was confirmed to the FCC at the end of last year. He brings both private and public sector experience to the Commission. Previously, he served as a senior advisor at NTIA, and in this role, he had many aspects of telecommunications policy, including spectrum allocation and planning, broadband access, and the U.S. government's role in the management of the Internet.

Prior to joining the Commission, Nathan was senior counsel to Brightstar Corporation. In that capacity, he led and negotiated communications equipment services transactions with leading providers in over 20 countries. Prior to joining Brightstar he was in the private practice.

Hailing from outside the beltway, he brings new ideas, fresh perspectives and independent thought to his role at the FCC. His bold thinking and commitment to bipartisanship will be crucial to meet the myriad challenges and for both security and growth of our communications network.

I'm delighted to welcome him on his inaugural appearance here at IGF USA, to discuss the FCC's role in securing vulnerabilities in our supply chain.

Good morning, and welcome, Nathan.

>> NATHAN SIMINGTON: Good morning, Melinda, and thank you for that very kind introduction. I'm delighted to join today, and I want to thank everyone at IGF USA for the invitation to speak.

The 5G transition has the potential to radically accelerate when it's migrated to wireless services we can build where we thought we couldn't. We can automate costly manual services and we can stay connected in an emergency, and in industry, it can be a total game changer.

Partner, a leading research and analysis company estimates, for instance that there will be over 30 billion connected IoT devices globally and many of those will be wireless, that's 30 billion devices making, testing, and shipping products to our homes. For me, that's 30 billion reasons to take security seriously. We owe it everyone to make sure they deserve our trust and reliance.

Whether it's critical infrastructure, to get power delivered to our homes tore places of businesses or receive help in a crisis or on the other hand, whether it's industrial services that deliver us the products upon which we relied every day, none of it can happen without security.

No only will 5G be viewed as unreliable and untrustworthy technology, if there are splashy security failures but the security failures themselves can be costly to remediate. And as we saw with the Colonial Pipeline hack, a large trouble can be caused with a little bit of a hack.

I'm not proposing to have the FCC step in and muddle their work, but the physical layer security of wireless devices, that is not just securing networks but securing the radio frequency signal or connection between the device and the network were between the device and another device, that is within the competency of the FCC.

And other agencies may not have the regulatory tools or in-house expertise to address the specific aspect of the problem, so it would be a dereliction of our duty no not to critically do what we can to harden the networks of which we will all rely and on which we will come to further rely as we transition to 5G.

And, because -- because there's no one else to do it, we've got to step up. This means working closely with industry to set stands for physical layer and signal security.

It means guarding against intentional interference such as signal injections. It means validating the source of transmission at the device level.

It means taking the spectrum security aspects not as promised but as carefully vouched safe. It may mean moving to lower trust structures internally within networks or between networks and it means close coordination among government agencies and industries to develop a product ecosystem that secures our vulnerable devices from critical infrastructure on down to consumer electronics.

Because as it stands wireless devices are just not difficult enough to hack. If of you folks may have heard me talk about pineapples and sting rays which probably sounds like I'm planning a trip to the Caribbean or something, but what I'm saying is anyone with an Amazon account and a high school education can build a device that interferes potentially maliciously with a wireless device, through physical layer vulnerabilities. So, we have a duty to examine these vulnerabilities critically to remediate them where possible and it is in that examination that I would ask for the help of all of those in attendance.

If you think about physical layer security, signal security, RF fingerprinting or know someone who does, please reach out. We are going to reply to your email or call. We want to develop as robust a record as we can and take notice of every fact available to us as we develop solutions. And we want to make sure that we consult thoroughly with industry to that any regulatory actions that happen at the Commission level have been thoroughly weighed and no one worried that they come out of left field, be damaging or unsettling or impact your industry.

Thank you for the invitation and I'm looking forward to the chat.

>> MELINDA CLEM: Thank you so much. And I encourage all

of our audience to take heed of that call to action and contribute because cybersecurity really is all of our responsibility.

So allow me to get started today talking about some of the executive orders that have come out over the last few months. We'll start with the order on May 12th, that directed several agencies to begin multiple efforts to modernize our nation's cyber defenses. A little context for our audience. So the White House stat sheet specifically noted that recent cyber incidents such as SolarWinds, the Microsoft Exchange and the Colonial Pipeline are sobering reminder that entities increasingly face sophisticated, malicious cyber activity from both nation state actors and others.

The agency does have oversight of our communications infrastructure and plays this essential role that you outlined especially when it comes to attacks. So within that EO, there's some things that you can see, some particularly relevant items for the FCC. I think the first is almost clear is around incident detection and reporting. So the EO outlines a need for greater disclosure, and information sharing around the cyber incidents that occur.

So are there reporting requirements currently in place between the FCC and ICT providers that you would find to be useful starting points? And if so, can you give us a little bit of detail about where you see any potential gaps and how you would encourage others to collect or facilitate data transfer throughout agencies?

>> NATHAN SIMINGTON: Yeah, absolutely, Melinda. There are a couple of reporting frameworks that could relate to outages already, such as NORS and DIRS. The NORS is probably the most relevant. Under the present framework, NORS reporting is mandated wherever there's a network outage, lasting at least 30 minutes and satisfying certain other thresholds. So this is a standard for general network reliability, which may not be directly connected to a cybersecurity incident but any

cybersecurity incident that causes a prolonged outage would be subsumed under this outage.

Most of the frameworks around best practices are focused on natural disasters. Prolonged outages of ICT outages had not been caused by the cyber attacks. And then there's an interoperation agreement where wireless carriers pledge help and capacity to one another and cooperate with the FCC during times of emergency network interruption.

So one idea of reporting of cybersecurity incidents separate and apart from NORS and using NORS as a general framework is to do wireless -- the wireless resiliency and cooperative framework. And so generally Citrix has done a lot of work on wireless network, and I think they would be the place to go around developing a reporting system.

I would want to see reporting of cybersecurity incidents affecting communication networks whenever they satisfy certain criterias. It's not obvious to me what they should be a priority, and I would want to develop this with industry cybersecurity experts, and I would want the framework to include not just cyber security incidents but incidents at the physical layers such as the ones I was discussing in my introductory remarks.

>> MELINDA CLEM: You touched on a second element of the EO that seems to have some specific importance for the FCC, and that it's to securing the Internet of Things. You mentioned that we have this potential of tens if not hundreds of billions of devices connected over the coming years, and as I like to remind people, well over 99% of them are owned and operated by people who really don't have the skills to secure them, myself included, right?

So in terms of making security embedded in the process and then also facilitating patching and updating and all of those sort of principles, what role can the FCC play to encourage or somehow incentivize manufacturers, the device manufacturers to take those steps to both harden security and facilitate simple security.

>> NATHAN SIMINGTON: These are great points, Melinda. A huge amount of the devices deployed will not be managed devices. They are devices that may be running very little in the way of an operating system. And so I completely take your point.

I think there are a couple of ways that the FCC can encourage this at the manufacturing level. So first voluntary standard setting. The FCC doesn't always have to create rules. I mean, I know obviously we love to create rules but sometimes instead, we can act as a clearing house of information or inter-arbiter. Serving as a nerve center for -- for smart people who are working at the detail level to connect and cooperate with each other is actually one of the great soft power things that the FCC can do, and -- and we -- I think everyone can trust that we'll serve as a neutral arbiter under the circumstances and, you know, I guess the other side of it is that by engaging with us, it's a way of staving off potentially inconvenient or inappropriate regulation, and making sure that your perspective is heard.

So that's the strategy my office is focused on at present.

I think if we can just get everyone into the same room, working off the same white board we might really be able to help key industry players understand how updating manufacturing standards for the creation of more sophisticated receivers and consumer grade devices or implementations of RF fingerprinting, perhaps in a productized storm suitable for local law enforcement is in the long run to everyone's benefit and will result in efficiencies.

Regarding devices being owned and operated by security professionals, the question of devices unmanaged post deployment is a very important one. It's sort of an open question whether the FCC has a mandate to address it presently this may fall into general cybersecurity interdiction. That's the type of question that I would like to put before industry, and if there's a role in the manufacturing or the standards level then we can address that.

The second is equipment authorization. So obviously, equipment authorization is a core FCC power and it's a blank instrument and a big stick and I think it's one we have to wield very judiciously, but it's available at the Commission level, which is starting to be more active in withholding equipment authorization where devices have the risk of being a national security threat. This is a forcing function of wireless security but it's a strong one. I'm hopeful that it's enough for industry to think about how problematic it would be if this had to be routinely deployed so that we can have other conversations and -- and things don't ever get escalated to that level.

Lastly, I think the FCC can educate consumers about device security and right now, there's, I believe, actually former Chairman Wheeler had some remarks on this recently, maybe in an op ed about the difference between a minimum viable product, and a minimum viable secure product. And if security isn't really a consideration in the consumer's mind or the consumer has no way of assessing the security of a device, then they may wind up choosing a very insecure device for other reasons.

If we educate consumers the way that we have the potential to do, maybe we can change that. So when we educate consumers we often rely on third parties to get information widely disseminated but the Commission could take a more active role in this space. So if we look at the emergency broadband benefit, EBB, for instance, when we tried to get the word out to consumers about the existence of the program and how to apply to it and about its relevance to their lives we worked with churches and civic organizations to get the word out and the carriers took a prominent role. So the FCC does that type of messaging directly and effectively. This is a situation where there may be a communications role for us to play and a labeling role for us to play or the coordinating function that we have the potential to serve as, among industry may lead to industry voluntary labeling standards or other approaches that will put security on the public agenda.

>> MELINDA CLEM: Perfect.

Let's stay on the topic of IoT and let's target it a little bit more to 5G expansion.

The commission has been working to free up more bands in the spectrum to facilitate the spread of 5G across the country. Many proponents tell greater responsiveness and reliability of the 5G network, but others are raising concerns around privacy, the amount of data that's being created and any potential risk that that poses.

What do you think the FCC should be doing, if anything to mitigate these privacy-related security risks?

>> NATHAN SIMINGTON: Great question, again, Melinda and one that's very much on everyone's minds and on everyone's agendas. As we have seen with some of the fallout from the European GDPR, it's possible to -- it's possible to get activist and privacy in a way where the benefits to the consumers are potentially mixed. And I think, you know, with electronic stuff, it sort of falls between two stools because on the one hand, there's telecommunication aspects to what's going on, which sounds like the FCC, but there are also general consumer protections which sounds like the FTC and it becomes a complicated questions.

Sticking to core FCC competencies. It's about the architecture of the 5G networks themselves and we should focus on the unique strengths what distinguishes us is signal and physical layer security and the prevention of data piracy and attacks against PII on those fronts. Of course, it behooves us to work closely with other agencies as it pertains to user data storage and cross-communication infrastructure and we definitely should do, that but what the FCC really has the biggest mandate to do, the best place to burn calories on security is where it's regulatory remit is clear and where it can exert the greatest level of influence. I'm concerned that if we step too much into the privacy arena that would require us to either step outside of our jurisdiction, or -- or on the other hand, it would require us to -- to do an inadequate job or to have to -- or to raise questions about our role in the larger economy, that maybe would be unwise to raise.

So on the other hand, wireless device security at the physical layer, that's clearly within our backyard. It has implications not just for the protection of user data but for the proper functioning of the device for the intended use and also I might add for the ability to pull implicit data off of -- of the network or off of spying on the network, all of things which we clearly have jurisdiction and a role to play. As for the rest, I think that's a larger conversation and to the degree that it's not jurisdictionally clear already, it really would become a question for Congress.

>> MELINDA CLEM: Okay. Let's talk about targeted mitigation efforts quickly.

There are many approaches to security policies, protocols and myriad technical solutions. Too often as we saw in the reporting about SolarWinds is that security budgets are seen as burdensome cost centers and their resources are typically stretched too thin. What sort of technologies do you want to see adopted? What are the solutions out there that you see promising to help our supply chains and if you could, tell us where, if you are seeing, you know, more on the proactive defense side, the incident detection, or better efforts spent on the response or do you think we should spread it out evenly the solutions?

>> NATHAN SIMINGTON: Okay. So I'm going to go on just a little bit of a tangent here. I will be remiss if I didn't make a plug for receiver standards as a concept. Yes, this is related to the notion of physical layer security, some tangentially, but attenuated connection is still a connection as many of us have experienced. Without good receivers we

stand to live with a lot more interference, effective interference, device perceptible, consumer perceptible. We want mid-band spectrum to densify. That's good. That means higher utilization of a public resource, but with this densification interference will increase which might impact critical infrastructure or public safety operations in a particular band. Or alternatively legacy equipment operating in an adjacent band.

So first and foremost, let's get receiver standards right so that we don't have a constant interference sea out there, with the potential for service disruption. Let's make sure we fully close that gap. So second, I mentioned RF fingerprinting before. This is defense applications of RF fingerprinting are now standard, but what we're seeing very often is that technologies become productized down to the consumer level or at least down away from the esoteric solution level where consumer adoption is possible and agency adoption seems to be feasible outside of the -- outside the greatest centers of expertise on that particular technology.

What we're seeing is machine learning advances on RF fingerprinting are permitting devices on the receiving side to increasingly be successful at a relatively low price point at uniquely transmitting the device my view is this is a potential game changer for spoofing and repeating attacks.

This could affect insulin pumps and give local law enforcement an important tool to track down criminals. I think this will be a greater and greater concern for local law enforcement as criminals themselves gain access to more sophisticated tools for attacks such as cloning wireless key fobs for cars.

Third, supply chain integrity. They can work devices at the subatomic level and then read them with handheld devices which to me sounds like Star Trek. But there's the potential to store this on a blockchain ledger as a digital twin of the device. There's a piece in the "Wall Street Journal," I want to say just this morning, about fake chips being -- entering the market and everyone having to step up their game to ensure that they are not being sold fraudulent chips in this time of semiconductor shortages.

It's techniques to ensure the integrity of supply chain generally have to just become a bigger part of our lives, just as we have all learned to avoid clicking on the emails from foreign princes who have so much money in their bank accounts but can't get it out for some reason.

Security has got to be approached as an entire life cycle. We need chip sets from receivers that we trust and supply chains to be trusted in transit, we need clearly identifiable actors at every stage so that you are not so to speak buying out of the back of a van. We need to be able to audit every physical element of devices. We need to trust devices in operation. We need to trust patching. There's always an attack at the weakest link and there has no good moment to ease off the throttle on security.

As for the larger implications I mean supply chains, those are two words that cover a lot of terrain. So the specific meaning of supply chain security, as it pertains to the FCC, and, again, I don't want to try to turn this into something that's reaching all over the world, and Congress wouldn't let us anyways. We have a mandate for secure supply chains, in various respects, and I think we need to figure out where the real attacks and threats are, where there's likely to emerge coming forward, and how we can best indict them using some of the tools that I outlined.

>> MELINDA CLEM: Great. That's a great approach. Like to hear that we are doing everything from the detection to the law enforcement to help on the attack. This is a naturally frightening topic. I want to close on something positive if you have some sort of a bright spot that you can share with us that will help us sleep a little bit better at night. Things to help truly bridge the gap off these vulnerabilities. We

would love to hear it.

>> NATHAN SIMINGTON: Yeah, absolutely.

So these are novel threats. So they alarm us in ways that past threats may not have done. Let's remember that, for example -- well, financial fraud is probably, you know, older than writing. If you see "Catch Me If You Can," checks themselves are not invulnerable. Perhaps there's a Frank Abagnale who is currently committing cybercrimes and will help us to understand the cyber threat attack surface.

All joking aside, industry takes security very, very seriously. Level of technical sophistication is astonishing. That's why as it's much outreach to players in the field, including the emerging players very often at the cutting tech edge as seriously as possible. So the resources that industry puts in this area, billions are spent to making devices more efficient, less costly to produce but also far safer.

If you look at the amount of attack space that's been closed, whether it's in your browser or cell phone, over the last decade, it's truly, truly impressive. I mean, I'm old enough and was also on the Internet early enough to remember when just, you know, very, very simple JavaScript attacks could take down a browser or a computer lab and industry is moving very fast to keep up with new threats. Sometimes these are attention. That tension may come with additional costs which is why I appreciate you highlighting the consumer security sensitivity aspect of this.

Once we have made this more visible to consumers, including consumers at scale, such as school boards, then -- then we maybe got the ability to advance the ball more systemically within the government. You know, one way that -- one way that web help at the FCC, in the broader cybersecurity world is we do fund a great deal of equipment nationally, or rather the funding at least passes through us. So there's a degree to which we can close gaps just using the power of the purse, consulting with other agencies and setting -- taking their standards and making sure that they get deployed into the next year's purchasing decisions and we can quickly propagate things through many, you know, vulnerable communities, through new infrastructure deployments and schools and libraries and it behooves us to keep our communication channels open with those agencies and make sure that their thinking is reflected in our policies where we are not the experts and on the other hand in areas where we are the experts on the physical security side, that we close the gaps there too.

The truth is a lot of it is just that there's low hanging fruit out there. If we make that difficult to pluck, if we force them to raise their games, many will drop out. They are not necessarily people with Ph.D.s in engineering. They may have bought something out off of Alibaba or eBay and running around a little unchecked but we will check them.

My colleagues across the federal government take issue -- take this issue with a very high degree of seriousness and vast resources are allocated if we step up and do our parts as well and coordinate with them, we can get to a solution. More needs to be done in certain ways, of course. Sometimes much more but the ground truth, the background rate of cybersecurity investment in the country is not low. It's high. It's our job at the SEC to take care of the things we are responsible for and to empower everyone else to whatever degree we can, to make the most out of their great achieves in cybersecurity, for a more secure future.

>> MELINDA CLEM: Great. Well, thank you so much. You have given us a lot of good things to think about and exciting to watch some of these initiatives that you can champion through the FCC. Thank you so much for your time today, Nathan.

>> NATHAN SIMINGTON: It's truly a pleasure Melinda. I'm very proud to be able to speak to you.

>> MELINDA CLEM: Thank you so much. I will hand things over to the very capable hands of moderator for our expert

panel talking about these vulnerabilities in the supply chain, Melissa Griffith.

>> MELISSA GRIFFITH: Hi. Thank you for having me. And thank you for the opportunity to follow that excellent keynote and fireside chat. I think there's a strong foundation for us to build upon. My name is Melissa Griffith, I'm a public policy fellow with the Woodrow Wilson International Center for Scholars.

We are to take the broader conversation about supply chain security and narrow us down to a still quite broad conversation on software supply chain security.

Whether this issue has risen to your attention over the past year with notable hacks, such as espionage operations and ransomware or if you are concerned about country of origin around vendors or one of those people that have been following this issue as it's gained steam and evolved over the past ten years or so, software supply chain security is a pressing issue. It's a pressing current for private organizations and businesses and it's a pressing concern for the United States, given the national security implications, including the reliable functioning of our military, our government, and our critical infrastructure.

This is the topic, the issue we'll be discussing in depth today, and over the next hour, we will be covering a lot of ground. So please bear with us. We will go from scoping out the problems we face with software supply chain security concerns to identifying paths forward and solutions.

So without further ado, it is my pleasure to introduce to you today's panelists.

I am joined by Hemu Nigam, he's with Venable working with the risk management and services group. And Tatiana Bolton is the policy director for R Street cybersecurity and emerging threats team and Greg Rattray is a partner and cofounder of Next Peak LLC, a cybersecurity and risk management firm. All of them have extremely long bios, ranging from industry and government and we are very thankful that they will be joining us.

We will start out as a little logistical note with five-minute opening remarks quite brief from each of today's panelists helping us set the scene from a variety of perspectives and then we will transition into a moderated session. This session will live or die based on the audience participation here as well. As your questions come up, please drop them up in the Q&A bucket at the bottom of the screen next to the hand raise. You can also wave, but please raise your hand. Drop them in the Q&A and I will weave those as the discussion carries forward.

So without further ado, I will go ahead and start us off with Hemu who is going to give the first five-minute, opening remarks.

>> HEMANSHU NIGAM: That was a lot of information that the Commissioner gave to us in that short amount of time, and he used the praise subatomic molecular level two times, and he didn't just screw it up like I just did.

So I wanted to actually take a few minutes and speaking of bios, I was actually told not to give my bio, because it will take the whole panel and I decided not to and I listened to my good friend Rick Lane on that.

I wanted to actually talk about what it means in real life, because people always talk about supply chain, supply chain, you hear about it in the headlines, but I think what is important is actually to bring it down to, well, what does that really mean for me? What does that really mean for businesses? What does it really mean for the people of this country or this world?

And I think the best way to do it is actual little talking about a friend of mine runs a food production company. And one of the things that she called me about was, hey, I hear about this cybersecurity stuff. Should I do something? And it was kind of a fun conversation. We were talking about the reunion coming up and things like that, but that actually then turned very serious, because what a lot of supply chain companies have is factories. And in this particular world of the food environment, they have people working to create food items and packaged and then eventually they go from the factory floor, they get put on a truck and from the truck they get put on the train and from that train they get put on another truck and eventually it reaches a destination in the back of a warehouse that then gets unpacked and eventually ends up in a freezer and somebody walked into the front of that store and opens the freezer and says, yes, I think I want this and they put it in their cart -- in their own supply chain, they put it in the cart, into the car and take it home and then they eat.

It's one of the most interesting things that if you look at that world, we're all thinking, is that food good? Does it have no poisoning? Is it going to be really tasty? All of those kinds of things. Like me in the security world, we're thinking why does that matter? Does it actually matter from a security perspective?

>> When you look at today's situation, when it means stopping a train and literally wanting to get the goods inside that container, I want that, whatever it is, or I'm going to hold it until you give me money. So one or the other. I want the goods or the money. Now when you attack, it can be as simple as a smart device is connected. That device is monitoring the big vat that has the food, that's being cooked, and this is looking at the temperature controls, because a device looking at temperature controls can do a better job than a human being saying is it warm enough or cold enough? That smart device is controlling it. They get through that smart device, through a vendor, not directly through the company. And when they are in that smart device, they can just as well say, well, you know what, let me make it look like it's actually working but I made it so that the temperature in the vat is going to a level where it's going to literally blow up.

And that's why it matters to people who are humans. There are people on that floor working every day who are thinking they're perfectly okay. They have the good hat on, the clean clothes on. They are not going to impact the food but that machine blows up.

That's a very critical issue to think about, when we think of supply chain security. Then you look at it from a different point of view, well, what if a ransomware attack happens and locks the entire thing up and you can't control anything, you can't do in addition. Now that food never makes it and that price goes up. And somebody is saying, why they are raising prices on me? I don't get this.

Well, it's because of security. At the core of it, it's because of security.

Now you fast forward and I wanted to actually literally use that phrase subatomic molecular level, because there's frankly actually a company that focuses on trying to tag -- he said subatomically molecular level tags about security measures which is a great name for a company, by the way. It actually focuses on that. So can you control that and why does that matter? Because when you look at the credits, that chip goes through the same supply chain process and ends up in the front of a military warhead.

It ends up in a smart car. It ends up inside of a house controlling a microwave or controlling a refrigerator. That chip can get all over this world and in a sense almost like a virus, during a pandemic. Except it may not be made properly, and once again you either have a national security level issue, you have a human being citizen level issue, you have a product issue, you have all of these things that you realize are in an ecosystem that are so interconnected, and at the beginning of it all, we thought, well, what is this thing called supply chain?

So I think one of the things that we have no think about is, why does it matter? It's because humans matter, society matters, we matter as people and we need to not only stay alive but we need to have products that actually are going to work the way they are supposed to, and keep our economy moving the way it's supposed to.

>> MELISSA GRIFFITH: Thank you so much, Hemu. I think you did a good job of why do we care and what does it look like in practice? Sometimes practice supply chain security sounds like a really long buzz word and it's hard to visualize it. Tatyana, you will talk about the strategic planning and the broader picture, hovering us up a little bit.

>> TATYANA BOLTON: Yeah. So if you think about it from the human aspect and knowing somebody who -- knowing someone who owns a business who is affected by supply chain outages. I think a lot of us have seen some of that become reality during the pandemic, with toilet paper shortages, which are -- which was a supply chain problem. SolarWinds and semiconductors, all of those things kind of made it real.

And so, you know, I want to -- but I want to talk about it from a broader perspective. Today, republicans and democrats alike are taking this very seriously. With have seen some recent actions like the Chips act and the NDAA, all of it is moving into a direction of making some progress on supply chain strategy.

But we still have yet to sort of accurately and crisply articulate one cohesive strategy for the United States. And so, you know, we're trying to do that with a -- with an initiative called the Secure Competitive Markets Initiative, trying to pinpoint what questions are not being answered or even addressed. So we're trying to do three things. Facilitate a discussion and build connections between people, provide some good resources and try to get people on the same page, and then -- and then sort of propose recommendations.

But what I want to focus on is, you know, there's some questions, big questions that highlight the central tensions of this issue that we haven't really considered. So, for example, what is reshoring or onshoring?

We aren't -- a lot of people have brought that up as a solution to the supply chain issues, right, bringing everything back to the United States, making sure that we are making things -- making things within the US, but if you think about, it we need to be considering our allies as well.

We need to think about what is best for our economy? Is it really going to happen bringing everything back on our shores, bringing all manufacturing back to the United States? I think that's highly unlikely.

So as we are talking about investments, we need to be thinking about more broadly what we want to do and how we are going to do that.

What is a realistic strategy and plan? And whether geography is an indicator of security.

So the next question is: What does the United States actually want to achieve? Right? So there are limited resources and there are -- there's limited time. I think where the federal government and sometimes companies get into a little bit of trouble is they try to eat the elephant whole. If everything is a priority, nothing is a priority. I think what is most important is for us as a nation to decide, you know, what is our main goal? What are we trying to achieve?

Is our goal to constrain China? Is our goal to, you know, tear down their economy, to make it harder for them to manufacture, to make it more difficult for them to trade? Or is it to build ourself up as a nation, to create resilience within our networks and secure our own supply chains and to build up our economy?

Part of the problem, I think, in the last few years has been that we can't articulate that strategy, and therefore, our policies and our tactics have been fairly, you know, undetermined. We have got some actions going on in the federal government. We have some -- at one point we banned Huawei, and then we banned TikTok, but then we don't ban TikTok.

I think it's difficult for the federal government to operate, when you don't know what is going to happen with the government from day one to day ten. I think what is most important is to answer those questions. I think for us the right answer is to have a US-centeric strategy, one that focuses on -- one that focuses on building up American resilience, on focusing on our supply chains, diversifying the supply chains and most importantly, including allies in those supply chains.

So that we have a smart strategy. And then the last piece is how can a government or parochial entity make common ground with businesses? I think we need to remember always that American strength comes from our economy, and in order to do that, that economy is based on business. And so we need to make sure that we are having those conversations, including businesses in the conversations, in the policy discussions and the strategy discussions and we talk to the people who, actually, for example, work in China, would have multinational businesses, who feel the -- feel the pain of a policy from the United States that goes back and forth on any given day and the number of man hours and dollars that are put into trying to figure out precisely where -- where the United States is going.

So you know, I think we have a lot of questions and so I'm eager to have this discussion to see where -- which ones we can answer today.

>> MELISSA GRIFFITH: Thank you so much. I think between you and Hemu, we have established what the concerns are and really grounded that and laid out the policy aperture and some of the gaps we can discuss going forward, but where we do, that I want to give Greg his five minutes who will pull us down to one particular sector around critical infrastructure. Greg, go ahead and take it away.

>> GREG RATTRAY: Thank you, Melissa. I think I will build on the prior remarks but, you know, probably put it a bit more in an operational perspective, bringing, you know, sort of both

national security operational perspective, including how national security organizations go after the supply chain as a way of achieving their objectives, and then having spent, you know, years at JP Morgan as a chief information security officer and trying to keep that highly digital enterprise, you know, rolling in the global sense that Tatyana has pointed it out across borders and keep global markets working.

I will challenge a bit the premise. Hemu, you did a very good job of giving us, you know, a very real world view of the classic thought about supply chain. I will also say that those supply chains are empowered by a digital ecosystem and when you talk about software security, you are not talking about a typical supply chain. It is not a bunch of things that move in a linear fashion. We have evolved into a digital ecosystem that's constantly interactive, and if you look at the things that have come up, you know, particularly SolarWinds, you know the Microsoft Exchange, I don't think you want to think about securing those reliances on those sorts of products and services, as a -- you know, the way you secure the movement, even of chips, let alone the movement of food, right?

Like, the movement of food depends on those digital -- that digital ecosystem functioning properly, but when we think about securing the digital ecosystem, I think the supply chain metaphor can be a little bit problematic. Hopefully over the course of the next 40 minutes or so we can discuss that.

I think what you have to realize there is what we're moving towards and I am just of late becoming more and more -- not just concerned. I mean we are reaching a point where, you know, we knew about global warming, you know, 20 years ago. California and the West Coast is burning down. We are close to that point with our digital ecosystem. We know that the way we use the digital ecosystem is exceedingly difficult and expensive to do securely and therefore we are not doing.

You know, running a software reliant, digitally reliant business, is a -- it requires risk tradeoffs and we are going headlong into digitalization and we are not ready on the security side of things obviously.

And as adversaries, disruptive nation states, you know adversaries understand all of that and we are seeing it every day and every week.

I will tell you, it is not a new phenomena for intelligence services and cyber attackers to understand that getting inside the digital supply chain, getting inside software used by enterprises. SolarWinds is a US company. All intelligent services get inside widely used software. They understand that software is updated. And therefore, they can get in. It is scalable from the attackers side, to go inside products that you know are going to get inside of a bunch of organizations that you want to either steal information from, monetize that information if you are a criminal group, or posture it to lock up everybody's computers, whether you are a criminal in conducting ransom operations or your nation state disrupting critical infrastructure.

I think we have to struggle with the fact that the headlong rush into digitalization and the use of cyberspace and the Internet, since we are in the IGF forums, comes with risks and we have not equipped people, financial, or even the disruption of the food infrastructure that we recently had, through ransomware and the Colonial Pipeline incident. Those operators don't have the tools to equip them to keep their digital environments secure, their digital supply chain secure if we use that.

So you know, we will get into it in the discussion, but, you know, one thing that I'm going to recommend, and it was sort of -- it was brought up as a question in the first portion of the session today, but you have got to get -- part of resilience is just willing to be disruptive, even if you do all the right things.

I think we very much underestimate the ability of critical infrastructure providers, but, you know, even as an individual, your own -- if you suddenly realize your identity has been hacked, do you have a game plan? If you are colonial pipeline, and your systems your billing systems are not used -- usable, are you going to have to shut down the nation's -- the East Coast's gas supply because somebody locked up your billing system?

You know, we have got to get organizations understanding that they can't prevent that. If they are targeted, an attacker will be able to get at them, especially if they are running national security grade. So I'm a very large advocate of being ready for those bad days and thinking through that.

I actually think that's unfortunately, for a prolonged period, we will not fix our defenses in less than I decade. As we fix our defenses, one the things we should do and this gets to hopefully something we will discuss is public it private partnership. We need to make it tougher for attackers to operate in the Internet, hide there, run criminal operations, run intelligence organizations, and I think the community that's on the phone, you know -- on the phone? That shows how old I am. On the Zoom today, you know, realizes they have a role. Telecommunication providers, demanding registrar services, you know, these sorts of organizations have to be collaborative and basically making it hard for malicious activity to occur. We have to make it hard on the -- you know on the criminals and the nation states that are outside of the norms and conducting disruptive attacks.

Melissa, I will stop there for the moment and look forward to the discussion.

>> MELISSA GRIFFITH: Thank you so much, Greg. As a reminder please drop your questions in the Q&A function. Not in the chat, but the Q&A function to they pop up magically my screen. I want to talk about some of those things you mentioned, Greg. You mentioned things like public/private partnerships but you mentioned an ecosystem, trying to understand what a digital supply chain looks like and in the

ways that is different. We know that presently Congress and the Biden administration have increasingly focused on cybersecurity and critical supply chain on the software space and the hardware space. We sue the recent executive order and there's also now companion efforts coming out of NIST to implement that order, looking at defining what counts as critical software in that software supply chain.

So we have heard from Hemu that software supply chain security is critical for organizations and businesses. Greg has talked about that as a much more complicated issue than traditional software supply chain. Thinking about kind of going forward from there, how does critical software, that thread, fit into the conversation about supply chain more broadly, and kind of digital supply chains? Is that the right approach? Is that the sort of same -- borrowing these physical critical infrastructure problems and I will start with Greg and then Tatyana and then Hemu.

>> GREG RATTRAY: Sorry, I'm in Manhattan, if you can hear the police siren running down the street. That's not an uncommon sound.

I think it makes sense, you know, for the government in its role in trying to go create a more secure ecosystem to focus its efforts on the, you know, things that they probably have unique ability to pull together the information and understand, underpin critical infrastructures and? Or widely distributed. And, you know, therefore, help both the government itself and the nation as a whole, you know, understand whether those key elements of the software environment are more or less secure, work with the developers to make them more secure, but also provide, you know, information. This is something that I think we will discuss about how close the public and private sectors get together about things that might be subverted, right?

Like the government has unique insights into whether a given product or service is subverted by a foreign adversary or hopefully criminal groups as far as the law enforcement and the national security as I mentioned for that. But that won't map completely on to enterprises. And enterprises need to know where the critical infrastructures are reliant on technology, including software now increasingly dominantly software and that map could be -- it will include nichey little things that are not in the government's big list of critical software, but they could knock out an institution because of, you knoll, unique small software service, package, provider it has that does something critical in that business.

I think you are finding this at least in some industries, sometimes driven by regulatory forces to be -- understand operational resilience, which I think is a good move from sort of expectation of companies will be resilient, but you have heard that theme from me.

>> MELISSA GRIFFITH: We have the resilience buzz word in. I think we would have been terrible if we didn't say the buzz word resilience. Tatyana, do you want to take it from there?

>> TATYANA BOLTON: I completely agree with Greg. I think a lot of it has to do with mapping from one agency to another, making sure that they are all coordinated, making sure that we are addressing the issues in a coherent manner. You know, I think this is where CISA's and RMC, the National Risk Management Center comes in. They are working on or have worked on national critical functions, all of this should obviously be tied and I think has been coordinated with NIST, and their efforts on defining critical software.

I think for a long time, we didn't include software into some of those discussions. We were -- when focused on critical infrastructure, we were focused on, you know, broad sectors, but, you know, we didn't even get to, you know, like really putting in the SBOM concept, until the latest EO. I think it shows how far we are coming from where we have been.

So you know, I'm hopeful that all of these efforts will work together. I think there still needs to be more support for sort of the software supply chain, security ecosystem. You know, the UK, for example, released an IoT bill years ago. We still have not kind of -- as in the United States has not released or passed a law on IoT security and we also have not passed a data security and data privacy bill, which I think for the record is tied together and I think it's critical. I think it's critical for the FCC, as the only enforcers of that theoretical law.

I think we still have a lot of work to do.

>> MELISSA GRIFFITH: Very helpful, reflecting on how far we have come as well as how far we have to go. Sometimes we just focus on the last piece. Hemu?

>> HEMANSHU NIGAM: I think one of the things we need to keep in mind is who are we doing this for? That's people. I don't know how many times I get a call from people who says, I hear about this stuff, but what am I supposed to do? It's not give me advice, but tell me what actually to do, and that's one of the greatest challenges that we always have, because in the cybersecurity world, there's so many different things you can do, but you want to break it down to an actionable steps for that either individual business or that enterprise level organization because what they need no do are oftentimes somewhat different, but at the core, exactly the same.

And what that means is, for example, focusing on things like, are you running a tack and pen test, every time you do a major feature change or things like that.

Are you training your people so you have technology, you have policy and people, are they all kind of getting hit at in regular intervals in what would turn out to be a holistic approach to securing yourself which goes to really what Greg was talking about is make it difficult for the hackers so they move to the next, right? That's how you protect yourself. No, don't come here. Not my neighborhood because I'm actually caring about this.

But people need to understand what does it mean. If I said to a business, you need to secure your building a bit better. They will say, well, okay. They are not going to say, what do you mean? They know they will call the security or look at their locks and do all of these kinds of things. If you say that to a business or a person today, the first question is I don't even know what that means. Don't get techie on me, right?

So that's one of the things that we have to start looking at even more, even though we say this every time, we say, every single panel I have ever been on, we talk about that, how do we simplify it so people understand, but I think we can't stop doing that, because those folks are never going to enter the world wherein they are going to be in their supply chain world on the ground, working in a factory. We will be the ones doing it. We will be teachers, educators and counselors and think like that as opposed to advisors which is a very different thing.

>> TATYANA BOLTON: If I may.

>> MELISSA GRIFFITH: Yes.

>> TATYANA BOLTON: I think that's a great point, because a lot of times people think it's about buying something, spending money on the next new technology or implement buying some kind of product that will fix -- magically fix your security. A lot of it isn't that. A lot of it still remains to this day, issues of not doing two factor authentication, having poor configuration management, and not training people for -- against phishing attacks, right?

Like, it's still some of those basic issues of training and, you know, protecting your perimeter. That is surprising, but -- and kind of sad to be fair, but it's on issue of policy, not about technology.

>> GREG RATTRAY: And I will try to build on both Hemu and Tatyana's themes, because I completely concur. With, you know, right from Tatyana, it's people, process and technology, probably in that or maybe process, people and technology, but

we are definitely at a state where there are no cybersecurity tools you can buy that are going to make you secure. Most enterprises, I will guarantee you, have too many tools, and they actually have the people expertise even to use the tools that they have.

We have a massive deficit which we all know and the actual sort of front-line technological skilled users of the tools and the network operators we have, being able to just run networks in a process, you know, as strong security process, everywhere from, you know, the user not clicking on things, to, you know, being in with teams trying to create secure edges and firewall rule sets to keep adversaries out. That's not easy. It requires technical expertise and there's not enough guys and gals on the front-line.

The other thing to Hemu's point, business leaders have to -- they all know that they have to have a digital strategy. Increasingly, you know, a great portion of most company's revenues comes through being able to operate in the digital environment. You have got to make business leaders responsible for risk management. Like, if your service -- if your ability to take customer orders and deliver products to services and customers pay you, if you are running a business and you've got profit/loss and you get knocked out, that's a business leaders problem, it's not the CIO or the CISO, the business leader should be dinged for that if he has not invested in the proper controls and resiliency necessary to keep his profits going, because he's going to get attacked, right?

Like, that is part of your norm. If you didn't have -- if you weren't investing in locks on your doors as a business leader, and your security guy goes, yeah, I told the leader that but he didn't give me any money. I didn't lock my doors an people stole all the TVs out of your warehouse, the business leader would get dinged if he didn't put the money into the locks, right? So we need to --

>> TATYANA BOLTON: It's absolutely a leadership issue. We

remain sort of focused on the CIO or the CISO, the CISO gets fired if there is a major breach. We still have this culture kind of like, you know, all hacks are bad, and it means you have terrible cybersecurity.

That needs to change. That's not necessarily true, even the best protected systems don't keep all of their attackers out.

But especially if it's a state actor, but, you know, it needs to go up to the highest levels that. Speaks today need to educate and improve the cybersecurity awareness of leaders, of CEOs. You know, as you take an accounting class in business school, I think you need to be taking a cybersecurity class as well.

You know from a leadership perspective, right, what does an organization need to broadly secure their organization? What is the bottom line? That's the age where we are now and that's not part of their general curriculum.

>> HEMANSHU NIGAM: And I want to --

>> MELISSA GRIFFITH: Go ahead, Hemu.

>> HEMANSHU NIGAM: I want to build on what Greg and Tatyana have just said. My son took a class, an online course because it ended up being online, but it ended up being how to understand business. And what they did was they took a concept and said, take this concept and go through all the different steps you need to go through, and eventually come out with a product on the other end.

Well, interestingly, that is the perfect place to insert that cybersecurity component to it. If you think about traditional business, everyone is taught you need marketing and pricing and you need to have the right kind of products and you need to figure out what is the cost of the product versus what you can sell it for, and what is your net profit, your gross profit, you are taught all of that, but no one is sitting down and saying, and by the way, you also need to figure out how you will secure it.

I'm one of those, you show me your great idea and I will tell you what the bad guys will do with it and then we'll sit down and talk about how we put in the right things at the DNA level to make it less likely that would happen.

So I think that's one of the those things that we can even think about at the pure education level of regular student who is going through without even realizing they just got trained in cybersecurity. And that goes to --

>> MELISSA GRIFFITH: I think we pulled a bunch of these different threads that have come up in these conversations from the role of government and sort of policy setting from the top to very specific sort of operational realities and resilience to education initiatives and really talking about how we approach security by design in our products and also the kind of responsibilities of businesses in this space relative to the government and other organizations.

I would like to take this public/private, which we said now several times and kind of pull it out a little bit and I will start with you, Hemu, because I know that you have some thoughts around hacker communities and visibility and intelligence. Thinking about some of the units where the private sector and the government can work more collaboratively together to achieve some of the goals and I will start with you, Hemu, and then you Tatyana and, Greg you can finish us off.

>> HEMANSHU NIGAM: When we think of the intelligence community, first thing they think of is that's the three-letter agencies no one wants to say CIA or, they live in that world. But the reality is, hackers are actually -- they have to speak to each other to figure things out.

People forget that. They are not going to meet in a coffee shop physically somewhere because they are working -- one hacker is sitting in one country and another one is 2,000 miles away in a different country. They are all working together as a team, but they have to be somewhere. And the intelligence community and the government sector has gone into those communities, and they get their intel and they know what may be coming. They think about it. They do their counter work based on, that but that's not actually something that you some be different nor the business community.

So many of those folks who do counterintelligence in the online world, I have worked with quite a few counter intel folks. They say I got out and I got out on this date. Then they will either work for a DoD as a contractor or they will have to find some other path, unless people like me come to them and say, hey, I could actually use your skill set to put you back into the world you were, and tell the business community -- tell people like me, tell people like my clients what is going on out there? What are they talking about? Am I on that list? Those are the kind of intelligence things that people are not thinking of, and yet, if you look on QR physical security. You have the security team that's working, walking through a mall. They are keeping their ears open. They are list to go what may be happening. They hear chatter and they go closer to the chatter. That's the same kind of physical work that you can bring into the online intelligence world and then bring it and use it in your business measures.

>> MELISSA GRIFFITH: Thinking about the public/private interplay and where the visibility and the situational awareness may sit and the private intelligence, and the communication that will Flay in that so we are situated in a situation to react to the types of threats. The very broad umbrella around public/private and the relationship between two. Where are some opportunities where if we could do this I think we will be in a much better position.

I'm sorry. I believe you are muted.

>> TATYANA BOLTON: Can you hear me now?

>> MELISSA GRIFFITH: We can.

>> TATYANA BOLTON: Sorry. So, you know, I think this' a lot that we can do. So I was on the cyberspace Solarium

Commission. We came out with a number of recommendations to improve private sector government coordination. One of the most important, I think is codifying this concept of systemically important critical infrastructure, whereby entities responsible for systems and assets that underpin national critical functions that I mentioned before, from the NRMC and at CISA are ensured the full support of US government, and shoulder -- on the other side, shoulder additional security requirements consistent with their unique status and importance.

So, you know, working on that broad umbrella, we have to identify and designate these entities. We have to insulate them from liability. We need to do security certification. We need to prioritize federal assistance. And identify and -- identification and warning for intelligence support is important.

So, you know, there's -- but there's more that we can do. We also talk about improving combined situational awareness of cyber threats, right? And that includes things like establishing and funding a joint collaborative environment, which would be sort of a common interoperable receive for the sharing and the fusing of threat information and other relevant data across the federal government between private sector and public sector actors.

I think some of the efforts on the hillside right now, to try and pass a national data breach reporting act, or put, you know, a provision of that into the NDAA, is -- is key, because I think that right now, we're seeing perhaps 5 to 10% of the threats that we know about, and neither on the government side, nor on the private sector side could you possibly protect against the vulnerabilities and the threats that you are only seeing 10% of. We don't have a combined threat picture and with that, how do you defend your networks?

It seems like fighting a losing battle, which it is. So I know we had voluntary threat reporting. We have seen sort of some of the consequences of that system in the latest breaches and the continued increase in ransomware attacks. I think it's time to go to a nonvoluntary threat reporting, you know, framework so that we can get this combined threat picture.

>> MELISSA GRIFFITH: We have another plea for better situational awareness sort of starting off when thinking about the intelligence community outside of those three-letter agencies that typically come to mind and then thinking about paths forward there and the real iceberg problem of the 10 to 20% of your visibility and how do you address those threats and some questions about mandatory requirements.

We may go three for three with Greg on visibility. Greg, take it away.

>> GREG RATTRAY: I will try to reinforce a bit. Certainly what Tatyana has just mentioned. I led something recently called the New York Cyber Task Force which very closely with the Solarium Commission and even tried to reinforce the commission in the joint collaborative environment and situational awareness. So for those who are interested in sort of a more private sector look at what government private sector collaboration should look like, you know, there's that report out there, issued just this past spring, but this is building and close collaboration into some of the US government initiatives outlined by Tatyana.

I guess, you know, maybe make it -- try to make it a little more operational. You know, one thing -- three things and I will try to be very brief. There is good public/private collaboration at times on disrupting criminal botnets and the community that's online in this can be an active player in there. I'm a very big believer that the private sector should give the government the information necessary for the government to and the authorities, the disruptive authorities but we should not have the private sector doing disruptive activities and hacking back and those sorts of things.

We need to make it hard for our adversaries. So private sector -- the government has to bring the private sector in because the private sector has best information about what adversaries are doing and where they are located so the government can go after that.

So building on that, the other thing that the private sector knows is the assets and critical infrastructure, especially systemically important infrastructure as mentioned, and give that the to intelligence community to Hemu's point that those are the people out there looking in those agencies NSA, CIA at our adversaries but they should be looking if the adversaries are chatting about mainframe computers that make -- that transfer payments as well as looking for information that they are chatting, about you know, F35s and, you know, major weapon systems. And that's the private sector driving the national intelligence community's, you know, intelligence gathering and then as appropriate feeding back to private sector entities protecting themselves.

Then, you know, where this goes in trying to link it back to supply chain, software supply chain security is how are we going to build that bridge when the government understands that a certain product or service may be the risk from being, you know, infected or having added features that an adversary put into that product to service for their purposes, and how do we get that information back into the decision-making as to what's in our digital ecosystem?

I think that's a -- you know, a challenge for this decade, as this whole cybersecurity, you know, situation evolves. We are in a worsening situation. We can talk about that, given that stipulation. We have got to do more to arm the private sector and even at the individual level to secure themselves.

This is not something where the government is going to secure the private sector or the government has to help the private sector secure itself.

>> MELISSA GRIFFITH: So we have some questions coming in. Before I pivot to a much more -- so we have done the

public/private. We will do the US vs. international in a second. Let's leave the United States and talk about the global picture. But before we do that we had a question come in specifically about the conversation we just had around private sector security by design, build this in at the start. And there's acknowledgment in the question that this is widely recognized, it's not a new concept and yet it's not done. What are the tools, the carrot sticks that the government has to incentivize industry and these players that have a variety of resources at their disposal, some that are better equipped than others to do this to start to solve this problem in practice?

And since this question called out Tatyana and Greg by name, we will start with you and then you Hemu.

>> TATYANA BOLTON: Honestly, I think a lot of those issues are going to be resolved by some of the underlying fundamental things that we just need to fix in cybersecurity, like a national data breach reporting law, a data security and data privacy law. We need to do more collaboration with the private sector.

Right now, at this point we don't really use a lot of sticks, right? We don't -- and we honestly don't even have that many carrots. We, I think from the carrots perspective, we have got sort of perhaps more integration, at least for systemically important critical infrastructure entities, more intelligence support, more integration into the defend and respond piece of what the federal government does.

From the stick end, you know, we need to -- we need to hold people to sort of stronger requirements, have more sort of systemic standards that are currently put out there, but aren't -- don't hold people to account.

Specifically to -- to your question, though, I think labeling, you know, creating some sort of energy star or whatever, you know, the commission came out with NCLA, a labeling authority, basically it helps people get a sense of what they are buying, right, making it more commonplace so that you know what that -- you know, compare the iPhone and then Android device, right?

If the iPhone has a security -- a cybersecurity NIST sticker, then you know it's more secure than Android, and then perhaps that the way to get people to start putting pressure on companies to actually creating things that secured by design. Right now they don't -- they see the benefit of getting things first to market. That's the primary driver of all sort of -- all of the products that are coming out.

And so we need to include security as a demand from the consumer side for the companies to start taking it, I think, a little bit more seriously on their end.

>> MELISSA GRIFFITH: Potentially creating security as a competitive differentiator. Greg, how do we start go from this, we know we have a security problem, to having security built in.

>> GREG RATTRAY: I think the call out has been for couple of decades is to create the marketing incentives for the producers of technology to do better at security. Hopefully the -- you know, hopefully in a good way the disruptive events, it can be a combination of market itself, just because you can -- I think, you know, certain industries, cybersecurity is becoming a differentiator, right? Certainly in financial services, you have to be -- you have to be seen as secure and not vulnerable and even you will probably get some advantage from being considered at the front of the pack on security, right?

And in many industries, the technology is developed inside the industry, right? So this whole security by design thing is important for -- for companies that are digitizing and building their own tech which is, I think, is increasingly, you know, something that happens. So it's not just Microsofts or the cloud providers or the SolarWinds doing network management software.

The cautionary note I have is that you can make it as secure as possible, but if -- if you configure it improperly, it's still going to be insecure, and I think there's more vulnerability in how, you know, even a secured software package is run than it is hacking the code itself.

And, you know, if you look at what -- how breaches occur, they are not -- they are not generally going after vulnerabilities inside code. I mean, certainly, patching is important, and, you know, these -- these aspects of more secure software makes it easier to secure an enterprise, but secure -- secure a bold software is important. Making it easier for users whether they are large enterprise sys admins or individuals with IoT devices. The security features will have to be toggled on. There's security choices to be made. And I will just finish with SolarWinds, right.

Like, that was the Russians inside the software development process for an update to, you know, a continuously running network system. This secure by design is an oversimplification, because people want -- like, it would be great if they just handed us secure bricks and we just built a wall with those bricks. The problem is that they are not bricks, right? You know, they are these amorphous entities that are constantly updating themselves, that are fed by code, and that code for SolarWinds is developed all over the world, and you can get in that development, and other places like Prague.

So it's not a simple patter, but secure by design would be useful.

>> MELISSA GRIFFITH: Yes laying out the security design, and life cycle question. We will have ten minutes left and I will ask Hemu to be incredibly succinct to move on to the global question.

>> HEMANSHU NIGAM: I will make it shorter. In terms -- it is easy for us to say, government, public/private partnership but a lot of times in the business community, people often don't feel like the government is watching their back. And I

say that because one breach happens or when something happens, what is the first thing people do? Oh, you are bad. You didn't do your security. And so what the business hears is, well, maybe I should just kind of be quiet. Do those things.

On the other hand, a storefront gets attack and someone steals everything. What the government does, I'm sorry a bad guy attacked you, and let me hunt down the bad guy. I'm sorry that happened to you. Right?

So there's the notion that what happens in the online world, what happens to the victim. Don't leave the door open and dot kinds of things that we are talking about on this panel about being secure, but at least come from the approach of yes, there are bad people out there. There are criminals who are attacking people who are trying to run a business, make money, live in this world, feed their family, do those kinds of things and yet we are making them the criminal. And I think that shift will go a long way in helping the public/private partnership.

>> MELISSA GRIFFITH: The shifts and the narrative and the operatives here and the other thing that's danced around is having utility for the private sector where everything goes in doesn't come back out.

We will spend about five minutes on global. We will finally leave the United States and look at some of these global questions. This' a question in the chat specifically about EU policy, NIS2.0 directive. I will broad than out a little bit and ask us about that EU policy in particular, but how consistent is the United States' approach with key allies and partners also trying to tackle this software supply chain question?

Because as we know, no supply chain is US or one country, and digital issues kind of take that tenfold. So I will start with you, Greg and then go to Hemu and end with Tatyana.

>> GREG RATTRAY: I will try to be quick. The current administration has a much more collaborative approach with most

nations but certainly using alliances and trying to get on the same sheet of music across the globe on issues like supply chain security. So I think it is a very positive development.

I do think just the -- I want to move it away from government. On the private sector side, I see, again -- and I'm not an optimist in most things but I see progress on the -- the adoption of the NIST approach and the cybersecurity framework becoming a more global approach and being used as a benchmark across the globe as good practice. And I think that's a very useful thing, where expectations of, you know, an organization can be graded by, you know, regulators and entities around the globe in a similar fashion.

On a collaborative front, I do see some progress and I think there needs to be hope from and I see the US hopefully, you know, resuming its role as a global leader in this regard, but listening and enabling not just telling, you know, people what to do.

>> MELISSA GRIFFITH: Hemu NIS2.0 and globe directives more globally.

>> HEMANSHU NIGAM: I want to take what Greg said to another level. It hints about this. When we hear about international, people say, what are they doing over there? What are the Europeans doing? What are the Asians doing? We are almost creating a conversation that's us vs. them and in the security space, it should be what is anyone doing in that will be the kind of thing that use what we want to do? In other words, it's not about are they doing this better? It's about finding the best solutions no matter where in the world they are coming from. When the administration takes that approach, a collaborative approach, it's not so much us versus them. We are all in this to go. We all face them from different places around the world. So it doesn't even matter where any of us is. And that's, I think, where the true conversation needs to turn to. That actually happens in the business community already, and the business community, people

aren't thinking, well, in the US, let's figure out what are they doing?

They think what is the best thing out there to solve this problem? Can I get that over here where I'm sitting right now? I think that's the approach we need to look at.

>> MELISSA GRIFFITH: Being far more collaborative and being magpies and taking good practices and implementing them at home.

Tatyana, finish us on the global perspective.

>> TATYANA BOLTON: So I agree with everything that Hemu and Greg said. I think that it's really good to see some international adoption of our standards, that's consistently been an issue. Because everything is global. I think it's erroneous to think about networks right now, where your company or anything, as within a certain country.

So you know, I -- about the ex U directives and all of the efforts that they are doing, you know, I applaud the -- the forward-leaning nature of the work that the ex U tries to -- tries to push forward. I think we have seen both positive and negative aspects of some of that. Obviously, GDPR was one of the first data security privacy laws but then at the same time, we also saw them taking that step. We also some errors, right, that we -- you know, some issues with the GDPR legislation and things we can learn from here in the United States.

I think all of the efforts that the EU takes and then we also see efforts in China, across a variety of these areas, I think it -- it -- I think this goes to show that the United States really, you know, needs to step up and be a leader in this space, you know, the way I see it is that, we are a participant in the global economy. We cannot retrench and we cannot pull back. We need to continue to participate in standard setting bodies, in various international agreements and organizations.

I think it's critical to maintain, you know, global norms to enforce those norms such as we see President Biden attempting to do with President Putin for the recent criminal activity and ransomware gains within the Russian states borders. I think all of that is important as we work in a global environment. Everything is global now.

>> MELISSA GRIFFITH: Everything is global. There is the bumper sticker for the panel.

So one of the ways in the last three minutes that I want to make sure that we hit on that I like to end these sessions, including this type of session where we cover so much ground, we are dealing with an incredibly complex issue that bridges silo, public, private, short term, long term-type thinking is to each one of our panels to prepare a rapid fire one thing that they would like us to prioritize. Where would you focus your energy and resources today or put another way, what is your top wish list item to bolster software supply chain security?

And we will go through from starting lineups. Hemu and Tatyana and end with dreg. The last three minutes.

>> HEMANSHU NIGAM: That means I have to talk as fast as you do, Melissa. One of the things we will -- I look at is that core question of tell me what to do. We have a lot of panel discussions a lot of conversations, and we all come together. We're all experts but I think we can use this opportunity because it's different than what it used to be when if you weren't at the conference, you didn't get to see it.

Now, the public can actually watch these kinds of things and we should, I think, be inviting the public in and saying let us spend our entire time telling you what to do. And they may take only 10% away, but that 10% can have a critical impact on their day-to-day business and their day-to-day success.

>> MELISSA GRIFFITH: Better communication and outreach. Tatyana.

>> TATYANA BOLTON: So I would say -- I will go back to my opening statement and sort of talk about the importance of a strategy. We need to answer some of the central points of

tension and the questions that have remained unanswered, and unverified in the United States strategy. We have not answered the question of what we want to achieve. What our goal is. Whether we want to reshore all of our manufacturing. Where are we going with this? I think we need a US-centric focus strategy that answers some of these questions.

And if I had a second one -- and I'm so sorry, but I got to say workforce. We need more people in the workforce. We need more diverse people in the workforce. We need to pull everybody in. This is an all hands on deck issue. We have got consist ransomware attacks. We have 460,000 openings in cybersecurity. We need to pull more people in. All of these things are going to be done by humans, and -- and that means we need to pull more people in.

>> MELISSA GRIFFITH: Strategic planning and we will give you the second one workforce, because it's such a good one. Greg, you have the final word.

>> GREG RATTRAY: I agree with those and then I will just say be resilient and, you know, when -- the way to do that, be ready for a bad day in cyberspace for the foreseeable future. We are not -- even if we dot right things, which we need to do and make this ecosystem safer for a long time, whether you get hacked or whether somebody you rely on gets hacked and you don't have services you need to do what you need no do, you need to be ready for those, you know -- understand what situations are most impactful on you, and how you are going to work around and work through those situations, and you need to put resources and time and attention to resiliency and exercising for a bad day in cyberspace.

>> MELISSA GRIFFITH: Prepare for bad weather. On that note, I want to thank the Commissioner and Melinda for starting us offer strong with the fireside chat and thank all three of the panelists for covering a lot of ground in the hour and everyone who sort of participated in the chat section which was lively and dropped some questions in the Q&A. On that note, I

will hand it back over to the session organizers.

>> DUSTIN LOUP: Thank you, Melissa and thank you, everyone, for making that a great panel. We'll take a quick break now, and we'll be back at 12:15 Eastern Time for more security discussion, focused on the internet of things.

During this break, there is the opportunity, again, to use Remo for a little bit of networking and we'll have a special guest in there talking about the IGF's Dynamic Coalition on Internet standards, security and safety. Very suiting for the topics of day here. So go ahead and look for that table labeled DC-ISS and have a chat in there.

And we'll see you back here shortly.