Mitigating Security Risks to Emerging 5G Networks

Photo: Chip Somodevilla/Getty Images

Transcript — February 6, 2019

Available Downloads

Download Transcript of Keynote Speech	283kb
Download Transcript of Moderated Discussion	399kb

Keynote Speech

James Andrew Lewis: Good afternoon. Welcome to CSIS. Our event today is "Mitigating Security Risks to Emerging 5G Networks," a topic that continues to gain interest. We have a great panel and an amazing opening keynote speaker, Commissioner - sorry - (laughs) - Jessica Rosenworcel. I'm a little disorganized.

James Andrew Lewis: The format today will be Commissioner Rosenworcel will give opening remarks. She'll be followed by a panel of speakers that will be moderated by CSIS Fellow Clete Johnson, Senior Fellow Clete Johnson.

James Andrew Lewis: I'm going to introduce Commissioner Rosenworcel briefly. She was named as one of Politico's 50 politicians to watch over the next couple of years. That's pretty impressive. She has long experience prior to serving at the FCC in telecommunications and public service, public policy.

James Andrew Lewis: Prior to joining the agency, she was the senior communications counsel for the Senate Committee on Commerce, Science and Transportation, which is really a perfect background for this stuff.

James Andrew Lewis: So we're very fortunate to have her here to give us opening remarks today.

James Andrew Lewis: So Commissioner Rosenworcel, please. (Applause.)

Jessica Rosenworcel: Thank you, Jim, for those kind opening remarks.

Jessica Rosenworcel: And, of course, thank you to the Center for Strategic and International Studies for gathering us all here today for what is a very important conversation about security and next-generation wireless networks, known as 5G.

Jessica Rosenworcel: Now, this discussion is timely, like up to the minute. In fact, when I began thinking about how to start my remarks, I kept coming back to that familiar maxim, may you live in interesting times. And, you know, if you do a little digging online, you will find that there's a dispute about its origin. There is one school of thought that claims it is based on an old Chinese curse. But there's another school of thought that says may you live in interesting times; well, its provenance lies elsewhere, and perhaps with a British statesman.

Jessica Rosenworcel: Still, the more that I studied that saying and the dispute about where it came from, the more I thought that referencing it was an apt way to begin, because these are interesting times.

Jessica Rosenworcel: Last week the Department of Justice charged a Chinese equipment manufacturer and its chief financial officer with attempting to trade steal secrets, obstructing a criminal investigation, and evading economic sanctions on Iran.

Jessica Rosenworcel: Last year, in the National Defense Authorization Act, Congress prohibited executive-branch agencies from using or procuring telecommunications equipment or services from companies that are associated with or believed to be controlled by China. And in the meantime, key intelligence allies have joined us in restricting such equipment or are considering different ways to do so.

Jessica Rosenworcel: Closer to home, at the FCC, where I work, we have proposed rules that would prohibit the use of universal service funds to purchase equipment or services from companies identified as posing a national-security risk to communications networks or the communications supply chain.

Jessica Rosenworcel: So the stakes are undeniably high. That's because next-generation 5G wireless networks are, in fact, the unifying fabric that will connect us all to the future. This is the essential infrastructure for the next generation of digital technologies. It will feature data speeds 10 to 100 times higher than what we know today, and with latency reduced to as little as one millisecond. And that in turn will power autonomous vehicles, foster advances in robotics, and expand the potential for machine learning and the possibilities of the Internet of Things.

Jessica Rosenworcel: So what that means in practice is that the race to 5G is about so much more than the smartphones in our palms, pockets and purses. Those handsets represent the epicenter of the last wireless revolution, known as 4G. On its strength, we built the applications economy and changed the way we live life online.

Jessica Rosenworcel: But the coming changes with 5G are broader. Connecting the physical world around us will change everything from health care to entertainment to the way we work, and even what work entails. Plus deploying these networks promises a boost to our economy and millions of new jobs.

Jessica Rosenworcel: So it comes as no surprise that countries around the world are jockeying for position and control in this emerging ecosystem. In fact, I think the race to 5G has become a microcosm for the broader debate about global leadership and economic security.

Jessica Rosenworcel: So that's some heady stuff. And to understand it better, I think we'd actually benefit from a little bit of communications history. So let's rewind. Let's roll back to some interesting times roughly two centuries ago. That's when the British Empire dominated global communications through its undersea cable network. It was known as the All Red Line.

Jessica Rosenworcel: Now the All Red Line has a place in the history books because with such a vast empire, Britain had both the political need for cables to reach far-flung corners of the globe and the expertise needed to lay them deep on the ocean floor. And this tangle of undersea wires stretched from Ireland to Newfoundland, from Sydney to Singapore, and many more places in between. You can think of it as the Victorian internet.

Jessica Rosenworcel: Now, as a result, Britain led when it came to everything involving cable manufacture. It was an expert in cable operation. It dominated the supply of cable-building materials. Their engineers were at the forefront of electrical science, and so much so that they set the agenda for its research, dictated almost wholly by the needs of submarine telegraphy. No wonder, then, when other countries had their submarine cables built, laid, tested, and repaired, it was with British contractors and British ships. In fact, a single British cable manufacturer known as TC&M at one point produced more than half the cables laid worldwide. Now for other nations, that leadership had consequences. It meant they were dependent on the courtesies of a foreign government for essential communications facilities even in times of war.

Jessica Rosenworcel: But in the United States, we wanted to find another way forward. We wanted communications systems that were independent. We wanted capabilities in our networks that were less susceptible to foreign control. So what did we do? In time, we invented our way to an expanded market and a more secure future.

Jessica Rosenworcel: And the spark for that future actually came in 1901, when Guglielmo Marconi famously sent the first wireless message across the Atlantic Ocean. It wasn't much. But the message, which was simply the Morse code signal for the letter S, traveled more than 2,000 miles from England to Canada. But those three clicks of Morse code were transformative, because the United States took note. It provided a way, as it evolved, to communicate with moving ships, blast messages across international borders, and bypass nationally supported telegraph monopolies. We were all in.

Jessica Rosenworcel: But the British, they determined this new technology could never challenge their dominance in cable. Well, we all know how this story ends. The All Red Line gave way to a new era of communications. The cable system dominated, by the British, was supplanted by a more diverse system of interconnected radio networks. And in the United States, we saw an inflection point in the development of communications, and we seized it.

Jessica Rosenworcel: Today, I think we are also at an inflection point. What happens with the next generation of wireless services has vast consequences for our economic and national security. The choices we make now about how these networks are deployed can result in communications technologies that are more powerful by many magnitudes. And getting them deployed early matters. It provides advantages in scale, in standards, and in device specifications.

Jessica Rosenworcel: But I believe it is no longer enough to be first to 5G. The networks we deploy must also be secure. And to build 5G security effectively, we must build a market for more secure 5G equipment. That means making sure our companies can continue to innovate and encouraging other countries to invest in 5G security, too. Now, that's a big task, and as with all significant endeavors the hard part is where to start. But I have some ideas about where the FCC should begin.

Jessica Rosenworcel: So, first, the FCC must work with other agencies to help manage supply chain risk. Late last year, the Department of Homeland Security announced the creation of the nation's first Information and Communications Technology Supply Chain Risk Management Task force. Now, that name might not fall off the tongue quickly, but that public-private partnership is going to develop recommendations to identify and manage risk in the global supply chain, and the task force includes representatives from the Department of Homeland Security as well as experts from the Department of Defense, Department of Treasury, General Services Administration, Department of Justice, Department of Commerce, the Office of the Director of National Intelligence, and the Social Security Administration.

Jessica Rosenworcel: In addition, there is expertise brought by representatives from telecommunications carriers, equipment manufacturers, and cyber security companies. It's an impressive list, to be sure. But there is one agency that's missing. The FCC needs a seat at this table. Leaving the agency with primary oversight over communications out is neither prudent nor wise. Moreover, as I mentioned at the start, the FCC has an ongoing proceeding that speaks directly to these issues concerning equipment restrictions with the use of Universal Service Funds.

Jessica Rosenworcel: So I think good things come to those who ask and it's time for the FCC to speak up and secure a commitment from the Department of Homeland Security to participate on this task force. We should be working together. We should develop a common approach to 5G security.

Jessica Rosenworcel: Second, the FCC should charter a new 5G security council. Now, in past generations of wireless technology, it's been our practice to enjoy their benefits before fully preparing for their risk. With 4G and its predecessors, cyber security was often an afterthought. It was something to work on when deployment was substantial and it was something to manage when problems arose.

Jessica Rosenworcel; Though the capabilities of these earlier generations of wireless service really pale in comparison to those that will emerge with 5G, the vulnerabilities have been real. They range from risk with SS7 networks to the rogue use of cell site simulators. What we have learned is that retrofitting security after the fact is difficult and expensive. So I think we need a more forward-thinking approach to 5G. Cyber security needs to be front of mind.

Jessica Rosenworcel: Now, the good news is that 5G already features many security improvements over earlier generations of wireless technology. Plus, 5G standards are actually still in early days. Hundreds have yet to be developed. On standards and so much else, there is a lot of front-end work left to do, and that’s where what is known as the Communications Security, Reliability and Interoperability Council comes in. The council is a federal advisory committee that provides recommendations to the FCC on high-profile security-related issues. Its two-year charter comes to an end next month and I think the FCC needs to re-charter and reinvigorate this council, and when it does, it needs to identify 5G security as its primary focus.

Jessica Rosenworcel: To this end, three things need to be a part of its mandate: more study on security technologies to mitigate the risk from the Internet of Things, more study on network function virtualization to mitigate denial of service attacks, and a new study on 5G supply chain risk management that recommends specific mitigation techniques.

Jessica Rosenworcel: And third, the FCC needs to make cyber hygiene a priority. You know, with the advent of 5G services, we are going to have wireless capability built into the world around us. This will provide a whole new range of opportunities for civic and commercial life. But as they multiply, it will also increase our service exposure to attack.

Jessica Rosenworcel: And to prepare for this future, the FCC is going to have to expand its work to support cyber hygiene. Think of cyber hygiene in this way. To keep our communications systems functioning, we are going to need routine and regular practices that increase security and reduce exposure to risk. The agency must build these policies into its day-to-day work. Consider this: Every device that emits radio frequency at some point passes through the FCC. Go ahead. Pull out your smartphone, or your laptop, or your television. You will see on the back there is an identification number from the FCC. That stamp of approval means that the device complies with FCC rules and objectives before it is marketed and imported in the United States.

Jessica Rosenworcel: Now picture this: Going forward the number of devices could expand exponentially with 5G and the Internet of Things. So why doesn’t the FCC use its equipment authorization process to encourage device manufacturers to build security into new products? To this end, it could seek to disclosure from manufacturers that explain how new devices are secure throughout the expected lifecycle of the equipment. This would support better security practices on the millions of devices headed for us with the Internet of Things.

Jessica Rosenworcel: Or, consider this, telecommunications carriers are required by the agency to certify annually that they comply with privacy standards. There is, however, no equivalent agency certification required for security. What if we changed that? What if with the next generation of wireless licenses we ask that as a condition of holding this license for public airwaves licensees will have to certify that they have implemented the best practices for 5G security. For example, we could ask that licensees certify that they are using the National Institute of Standards and Technology's cybersecurity framework. That way we ensure that licensees have a structured way of thinking about network security and a common language for managing risk.

Jessica Rosenworcel: Finally, the FCC should take steps to educate citizens on cyber hygiene. In our work, we regularly interact with consumers and consumer groups. We need to find more ways to do outreach that touch on the basics of consumer cyber hygiene, from downloading software upgrades for devices to assessing connection security when using unlicensed airwaves.

Jessica Rosenworcel: So those are my ideas for getting this conversation started. These are early days in the deployment of 5G. And, as I said at the start, they are also interesting times. But they're also the right time to ensure that communication security is front and center. Thank you. (Applause.)

Moderated Discussion

Clete Johnson: I'll just start by saying that both Commissioner Rosenworcel and I left Senator Rockefeller's staff to go to the FCC. She, as the honorable Commissioner Jessica Rosenworcel. Myself as bureaucrat Clete Johnson. So - but it's an honor to have her here today. And thank you all for being here for this discussion. I want to follow up that speech, which laid out a pretty bracing look at these issues, with a panel discussion. We have some experts from a wide variety of different perspectives that I'll just quickly introduce. And then we'll go – we'll jump right into the discussion.

Clete Johnson: So immediately to my left is Ambassador Rob Strayer. He's the deputy assistant secretary for cyber and international communications. Also a Hill veteran and a lawyer.

Robert Strayer: And former colleague, yeah.

Clete Johnson: And former colleague, that's right. We've been in the trenches together on some cyber policy issues.

Clete Johnson: John Costello is the director of the Office of Strategy, Plan,s and Policy in the newly named and organized Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security. So we'd love to hear – we'll hear your thoughts on the interagency processes and the increasingly important role in the government-industry partnership.

Clete Johnson: Chris Boyer is – wears many hats at AT&T. Among those is essentially the cyber policy guru for a rather large company. He plays an important role on CSRIC issues. We'll talk about that acronym in a moment; also on the National Security Telecommunications Advisory Committee, one of, I think, three or four advisory committees that report directly to the president, and has been involved in a whole host of privacy and security issues in a variety of venues.

Clete Johnson: And finally, we have Travis Russell, who's director of cybersecurity for Oracle. And he is also the chair of the Network Security Working Group on the – as Commissioner Rosenworcel mentioned, the Council – Communications Security Reliability and Interoperability Council, or CSRIC, which may be the worst acronym in all of a town of acronyms. (Laughter.) But it's a very important body that advises the FCC, and he's been – Travis was not only the lead of that effort, writing really the only comprehensive report on 5G security that exists, but he has also literally written the book not only on SS7, Diameter, I think, a whole host of wireless protocols.

Clete Johnson: So we have a great panel here. And I just want to jump right in by – let's start with our industry representatives. Commissioner Rosenworcel laid out quite a challenge, the inflection point we're in, building a market for secure 5G. So before we get into how we're going to do that, can - would you guys walk us through how you see - what is secure 5G? And is it - that's a pretty big term that I'd ask you to deconstruct if you could.

Chris Boyer: Yeah. I mean, I'll - first of all, I want to thank Commissioner Rosenworcel for her comments. And I actually think a lot of the areas that she flagged are very similar to the areas that all of us have been talking about.

Clete Johnson: You know, when I think of 5G, I think one of the challenges we have is that we have a tendency to say, oh, my God, 5G has got all these security issues, and we kind of speak of it as if it's a monolithic thing, as if it's just, you know, 5G is one thing. But the reality of it is there's a whole host of different issues that are intertwined under that kind of 5G security umbrella.

Clete Johnson: And so, you know, I've heard people talk about issues of, like, you know, the devices. Like, are the IoT devices that are enabled by 5G, are they going to be secure? We've had discussions about the network itself. You know, is the 5G network - and even the network is not a monolithic thing. You have to break it down between the radio-access network and the core network, and even application layer. And then we've had conversations about whether or not the rate of 5G deployment in the U.S. is adequate vis-à-vis some of the countries that I won't name.

Clete Johnson: And then we've had discussion around, you know, the foreign countries' influence over the standards process and whether that creates a security vulnerability; and then, finally, you know, the elephant in the room around particular suppliers that might end up introducing vulnerabilities.

Clete Johnson: So there's a lot of different issues that are kind of all intertwined under the 5G security umbrella. I think, as an industry representative, you know, we feel like that 5G is actually an evolutionary step in terms of security, that the 5G network, for the first time, we're going to have security - and I think Commissioner Rosenworcel touched on this - is that, through the standards process, there's actual work being done to build in security into the standards themselves as they go forward, which is the first time we've really done that.

Clete Johnson: In the past, you know, security, as I think she pointed out, has been kind of layered on after the fact. But, you know, through groups like 3GPP, SA3, there's a lot of work going on to build security into the standards. So from a standards process, we feel like security is actually moving in the right direction. Now you can raise issues about whether or not the standards - that, you know, there are certain entities that are influencing the standards process. I would say that there's controls to prevent that from happening in terms of the standards themselves. There's rules around that. But we feel like we're making a lot of progress on the standards.

Clete Johnson: And then if you break it down and look at the actual device side, there's lots of different measures you can take to look at securing the IT device side.

Clete Johnson: So I really - so my main point would be that we really should look at - you have to look at one of those discrete buckets of issues and kind of think through what are the solutions there. But I think that we are trending in the right direction.

Clete Johnson: Travis, do you want to add any detail?

Travis Russell: Sure. Yeah, you know, I think the biggest thing that we face with 5G is this, for the first time, is a completely different type of network that we've never dealt with before. I've been in this business 35-some-odd years, which is why I have such gray hair. We've been trying for all of this time to do this convergence of data and voice, and trying to combine this and using IT technologies in telecommunications business. And 5G represents that culmination. We are finally bringing IT into the telecom market. And in fact, if you look at, you know, SS7 and Diameter and SIP, all of the technologies that we have been using for decades, all of that got thrown out with 5G. And it's truly cloud-based, software-based data centers instead of central offices. That's the 5G network of the future.

Travis Russell: And that presents a bunch of different challenges. And like Chris said, we have to start, you know, separating some of those. Otherwise, you know, security becomes this huge, big discussion - certainly on the device side, certainly on the IOT side. And I feel we've made quite a few inroads, I think, on the IOT side. We're seeing a lot of work already in industry. You know, we took the lessons from SS7, we took the lessons from Diameter - which by the way, the lesson we learned there is it's not SS7.

It's not a problem with Diameter. The problem that we found in the industry is that the partners that we connect to, that we trusted because they're a part of our trusted ecosystem, are not trustworthy partners. We found that a lot of these companies were complicit in providing access to rogue companies and to rogue actors.

Travis Russell: So with that in mind, that means we have to rethink our security strategy. And that's the work that has been going on in industry, is how do we secure those network boundaries. And there's been a tremendous amount of work done within industry. GSMA has done a tremendous amount of work. And if you look at SA3, the security document 33.501, it's the first 5G security specification to come out by SA3. There's a lot of content in there that was a direct result of industry through GSMA saying, hey, wait a minute, we learned our lessons around exposing PII, like MC. We've learned some lessons about being able to spoof networks and Diameter. We need to put some controls into place from the beginning in 5G that will prevent and mitigate those types of events from happening.

Travis Russell: And so that's what you'll see in 33.501. It actually has processes defined for 5G to prevent that type of activity. And so I think we're making a lot of inroads here, but we are just starting on 5G. We still have probably another year to a year and a half on Release 16, and we haven't even defined how are we going to do congestion control in a 5G network yet. So still a lot of work that has to be done in the standards. So I know everybody wants to get there as fast as they can, but we don't want to get there too fast. We want to make sure that these standards are complete and we've covered all the bases.

Clete Johnson: Travis, when Release 16 comes out, will that complete the 5G standards process?

Travis Russell: No, so the way that standards work is 3GPP, everything comes into a release. So there will be a discovery phase where we define what do we want, what content do we want into a release. That release then gets targeted towards 3G or 4G or 5G. Now everything of course is being defined for 5G.

Travis Russell In Release 15, which was the last release that just got done, the focus was on 5G radio so that we could deploy 5G services utilizing existing 4G networks.

And so that's what you see in today, by the way. It's 5G radio spectrum being used on 4G networks. The focus right now in Release 16, which we're supposed to have complete I think December, but it's not going to be December, is what about the core network functionality. What are the things that we have to build into that. And once that gets locked down, then we'll move to Release 17, where we'll fine tune that. And there will probably be three or four releases after that before we start moving to 6G.

Clete Johnson: So turn to our government panelist. John, Commissioner Rosenworcel has some thoughts about these interagency processes. Welcome to comment on that. But maybe before you get into the role of the FCC on the - on the supply chain taskforce, could you talk a little bit about how you see the industry efforts? Are they sufficient? Are they maturing? You know, does - and what role does the new - the new DHS CISA agency play? And what role do other interagency players?

John Costello: So that, honestly, is a series of really good questions. You know, supply chain over the last 10 years - I'm talking about broad supply chain efforts, have been a stopping and starting, sort of halting process in the federal government, where some progress is made, and then thing stall. And generally it goes between periods of major anxiety. What I've seen in the last year - the last few years, and the last year in particular, is really a coalition of the willing certain to be built. And you're starting to see multitudinous number of working groups within the interagency, you know, departments and agencies themselves or the White House, leading groups to try to get at the supply chain problem, whether it's, you know, a broader industrial base conversation, whether it's ICT in particular.

John Costello: And that's sort of - like, when we - last year when we were looking at, you know, reorganizing the agency and getting a - getting a new name, and leading into our cybersecurity summit up in New York, we realized that ICT in particular is what we'd refer to as a national critical function. It's where you have a confluence of different critical infrastructure sectors that come together with a complex interdependency. And a failure in one or a risk in one has cascading consequences across a number of them. So with that in mind, when we stood up the National Risk Management Center, which intended to study those national critical functions and work with industry to collectively mitigate them, we set up what we called the ICT SCRM Task Force, which Commissioner Rosenworcel mentioned. That taskforce is intended to - in part, to try to solidify a lot of the federal government efforts on ICT supply chain and extend them to industry.

John Costello: One of the biggest challenges we had is you can't do anything in supply chain environment without having industry buy-in, or at least getting a good understanding of industry, what they'll tolerate or what the reality is of supply. Acquisition and supply for telecommunication companies is obviously a huge part of their business. And anything you do that's going to affect that is going to have ripple effects. So our goal was to come together and try to identify that risk. What we're doing in particular, if you'll allow me a moment, we really have five workstreams that we're trying to push forward.

Clete Johnson: And this is on the task force?

John Costello: This is on the task force, which the FCC is a part of. They're a voting member on the taskforce. So they are participating. They are participating members.

John Costello: Number one - and this was mentioned in the CSRIC report - is that when we start talking about information sharing on supply chain, it's really difficult to really determine what that is. What does sharing threat or risk information between government agencies and between government and the private sector, what does that look like? You know, we have STIX/TAXII for cyber threats, but what does that look like for supply chain? How do we - how do we share that in way that is uniform and consistent?

John Costello: Second is threat-based evaluations of suppliers, products and services. I mean, there's a number of different proprietary ways and methods to evaluate a product or a service and its relative risk. But, you know, trying - like, the task force is really looking for a way to make that uniform and consistent, so that we're all speaking the same risk language. We're all working from the same sheet of music. The third is identifying market segments for qualified bidder and manufacturer lists. This is particularly important for the federal government as it looks to - whitelisting is a bad term - but it's trying to find trusted suppliers and reliable suppliers for government procurement and acquisition.

John Costello: Fourth is incentives, trying to incentivize security in the marketplace, working with companies to try to see what will they tolerate or what would be appealing or attractive to them that could change their purchasing or acquisition decisions towards original manufacturers or authorized resellers. And then finally, and this is germane to how I started the conversation, is an inventory - which sounds incredibly basic and elementary. But when you look across the federal government and you look across industry, you see a growing number of groups that are trying to get at the supply chain problem. We found it absolutely necessary to try to get an inventory of these efforts, what they're trying to achieve, and trying to map some of the work that we're doing in the task force to those. And how we could hook in, how we could benefit from prior work or influence other work going on in other channels.

John Costello: And what's the overlap, if any, at this point between the Supply Chain Risk Management Task Force and 5G security? There's clearly - there are some supply chain issues in 5G and we're certainly going to get to that elephant in the room. But beyond just supply chain, what about standards and, you know, some of the issues that Commissioner Rosenworcel and Travis mentioned, network function virtualization, software-defined networking, how all this ties into smart cities and other critical infrastructure? Are we there yet?

John Costello: I think - to be honest, I think, at first blush, this task force is going to go on for a few years. I mean, 2019 is looking to be like the year of 5G judging from the number of speaking events of number of conferences that are going on about it. And I think that's germane.

John Costello: But what first thing is first is, if we're going to have a really constructive and productive conversation around 5G security, both on the supply chain front and threats affecting 5G, is we have to develop and produce the hard work of that language to even have that discussion. I think there's - I know that sounds - I'm not dodging the question at all. I think we are going to get there, but first we've got to - we've got to do the basic. We have to - we have to crawl before we can walk before we can run.

John Costello: And 5G we know is coming. We know the stakes are high. And we know the manufacturers and the components we have in our 5G buildout the rest of this year and next year are going to - are going to set the stage for our risk tolerance in national security for a while. But getting it right and getting the basics right now I think is going to make a much more productive conversation later this year or early next year, absolutely.

Chris Boyer**:** You know, Clete, if I might add.

John Costello: Yeah, absolutely, please.

Chris Boyer**:** The issue of supply chain risk management really is beyond just 5G.

John Costello: Right.

Chris Boyer**:** Like, the idea - like, the goal of the - of the working group should be to develop repeatable processes to - or processes to evaluate supply chain criteria and threat evaluations for a number of different technologies, of which 5G is one, but there's going to be others. And so I think from an industry perspective - you know, I serve on the executive committee of the - of the - of the supply chain group and I think - I think the task force should really focus in on, how can we develop, you know - as you mentioned, there's a whole inventory of best practices and ideas of how to do supply chain risk management. We should look at those and try to identify which of those processes stand up and are repeatable and can be used for a multitude of different technologies. 5G has its own set of issues, you know, I mentioned them before. You know, there's a lot of different nuances there.

Chris Boyer**:** But I think from a - from a best practices and standards development perspective, it should be focused more on kind of broad supply chain risk management and how do you apply that to the different technology space.

Clete Johnson: One more U.S.-focused question and then we're going to go global, Rob.

Clete Johnson: One of the things that Commissioner Rosenworcel called for, which is actually part of the recommendations of the CSRIC report, is essentially to keep studying this issue, dive deeper. So it sounds like from the DHS perspective and from the industry perspective, there's some agreement there. Is that right? We're near - we're not - do we need to - we need to dig deeper?

Travis Russell: Yeah, absolutely. Yeah. I mean, we're, like I said, we're at the infancy of 5G standardization. I mean, release 15 was the first body of work focusing on radio. There's still a bulk of work that has to be done for, you know, just the normal functions that we would have in a network, that hasn't been fully defined yet. So I think there's still a lot of work that needs to be done, not just on the standards, but also within the CSRIC, also within DHS. We need to be looking at this on a long-term basis, not a short-term basis. And so I absolutely agree, we need to extend that, but not just within CSRIC. I think it needs to be through a number of different agencies.

Chris Boyer**:** Yeah, it's an - it's an iterative process, right? I mean, you don't stop and say, oh, the standard is done, you know.

Clete Johnson: Right.

Chris Boyer**:** I mean, the issues come up. You make adjustments. So I think the - I think through the CSRIC that's how we - and we've been doing - for folks who aren't familiar with CSRIC, we've been doing CSRIC reports dating back, on security, dating back to, like, 2003, I think. You know, we're on, what, CSRIC six?

Travis Russell: Well, you can go back to network reliability -

Chris Boyer**:** Yeah, the network - yeah, the NRIC, which is the predecessor to the CSRIC, so, I mean, this has been going on a long time. So these are iterative processes, they don't just stop and say, oh, we're done, right?

John Costello: And I will say, from DHS's perspective, is we fully expect an iterative process on a lot of these things. You know, when you talk about supply chain, you get into this sort of anxious paralysis when you talk about supply chain. What if we do this, what if we do that? I don't know if that would be - that would work or not. I think what we're trying to do is we are trying to move forward to at least set a baseline. We do not want the perfect to be the enemy of the good.

John Costello: That's not to say that we don't care about quality or, like, the best that we can do, is we want to set a baseline that we can build on in the future. And so moving ahead with a supply chain task force is, to be frank with you, our primary sort of thrust to get that done.

John Costello: All right. So we've talked a lot about the inside baseball of – use some acronyms – like, CSRIC and SCRM Task Force. And we even brought in the NRIC, which we won't even – that's the old CSRIC, for those outside the inside baseball world. This is all inside baseball U.S. government talk. What about these are global companies, global supply chains, the global race to 5G? What are we doing internationally? What's the – what, if anything – and please fill us in – what is the U.S. government's and/or allied international strategy to win the race to secure 5G?

Robert Strayer: Right. I'd be happy to cover that. I'll try to avoid the use of acronyms in anything I say, although working in the government there's a lot of acronyms around us all the time. First of all, I want to thank you and thank CSIS for organizing this panel on such an important topic and tremendous –

Clete Johnson: Absolutely.

Robert Strayer: – tremendous colleagues to be with here and Commissioner Rosenworcel as well. You know, the headline that we have with our international partners is that our future, national security, and economic security depends on having a secure set of communications and networks. There is so much data flowing around the world that it's impossible to just isolate one country's network and think: that's secure, therefore I'm fine. We're all influenced because of the nature of the cloud and the competing that's occurring across borders that we need to continue to have a secure network wherever that data is flowing around the globe.

Robert Strayer: In particular, I think we need to prevent three things. One is unauthorized access to that data, second is the disruption of the functionalities that we expect to occur from the processing, the Internet of Things – all the new transformational uses that we talked about earlier in this discussion – and third, we need to make sure that networks are not a venue for the introduction of other types of malicious cyberthreats that could cause the manipulation of data or the malfunctioning of those types of systems.

Robert Strayer: So as we look about at the 5G network, we not only have that criticality of those - of those functions that will occur, we also have to think about the blurring of the line between the edge and the core in the sense that almost anywhere on that network can present a potential attack surface. So the attack surface is expanding and so we need to be much more cautious about what kinds of equipment we introduce into that.

Robert Strayer: And because the nature of 5G relies so much on software, software-defined networks, and updates to software, we need to have confidence that those who are involved in updating that software or in the management of those systems are secure and not introducing vulnerabilities through those software updates.

Robert Strayer: So with so much at stake, we talk to our partners about how important it is to continue to seek to have trusted and secure networks. We think there are country-agnostic principles that should guide us, going forward. Just with regard to tender offers and sort of bids, we think that there should be fair commercial and reasonable terms that are not influenced by corruption and that are done in a way that the public in both the country that's putting out the bids and to vendors around the world can easily see the transparency of those processes.

Robert Strayer: When it comes to the technology itself, we have significant concerns with countries that have such a close relationship between their intelligence community and their vendors. For example, Chinese law, including their intelligence law, compels their citizens and their companies to participate in intelligence activities.

Robert Strayer: Unlike the United States, there's not - there are not checks and balances on that. There's one party in charge. There are not - there's not an independent judiciary. There's not independent oversight by Congress. In particular, I think when you think about trust we also got to think about the values behind that and we've seen a company like Huawei recently indicted for numerous deceptive practices, those that relate to deception to evade the Iran sanctions laws as well as deception to steal intellectual property and to actually have a policy in place to reward those who steal intellectual property for the company. That should raise significant concerns with regard to a company that does that.

Robert Strayer: And, lastly, I'll say about values, a country that uses data in the way that China has to surveille its citizens, to set up credit scores, and to imprison more than 1 million people for their ethnic and religious background should make us – give us pause about the way that country might use data in the future. And, in particular, I think it would be naïve to think that that country and the influence it has over its companies would act in ways that would treat our citizens better than it treats its own citizens. So with that, we have substantial concerns about relationships like that related to vendors. But it's not just about that one country.

Clete Johnson: All right. So let's continue that trail with regard to the supplier issues, but also more generally to the standards and market competition that we've been talking about to date. I'll start with you, Rob, and then go down the line. What specifically is the U.S. government doing about it multilaterally, bilaterally, with regard to industry-government collaboration? I'd love to hear your take on it, and then John. And then let's hear the industry take about that question.

Robert Strayer: Yeah. We're talking –

Clete Johnson: What are we doing about?

Robert Strayer: We're talking with partners around the globe about this. The upgrade to 5G we're raising at the highest diplomatic levels. We're making sure that policymakers, the most senior policymakers in governments, are aware of the momentousness of this decision and what is at stake in the decision they're about to make.

Robert Strayer: I think we've already sort of touched on this and the sort of generational nature of 5G, the transformational nature of it, means there'll be a whole generation of sort of lock-in with regard to those products and services from particular companies going forward. So it's a big decision. So we highlight the momentousness of it as well as what we see as principles that should be applied in making those decisions.

Clete Johnson: We see there are a lot of news reports about, you know, our closest allies - Canada, U.K., Australia. There was a report last night about the European Union. I don't know if there's any light you can shed on that. But I'd love to hear if - what your take from the official perspective is.

Robert Strayer: Well, we're having, you know, individual conversations with different countries. So you are reading about them in the press. It should be no surprise that we're having these, given, you know, the very deliberative and direct impact that we want to have, thinking about these processes and the decisions that are going to be made.

Robert Strayer: And as I said before, it's not just - you know, it's in our interest to protect our own networks, but we realize the interdependency that we face in the decisions that are made around the world and what that means for future technology and the future model for open and - open, interoperable and transparent uses of data around the globe.

Clete Johnson: And what about on - so, again, supply chain and suppliers is one part of this. But what about the other elements of 5G security and how we promote that, first at home and then among likeminded or allied countries?

John Costello: Well, I mean, I will piggyback off what Rob was saying, is even just sort of in our exchange, in our discussion, and I think in a lot of cases Rob and I or people we work with are in the same room discussing these issues. We really can't emphasize enough, again, how momentous this decision is. You are making a series of decisions that are going to define the next generation, like landscape, the lifeblood of your economy, and the very environment in which you will contend likely with foreign adversaries for control. So you can't emphasize that enough.

John Costello: You know, as far as, like, messaging at home and abroad, right now a lot of our conversations with our closest allies is trying to understand the full range of options and seeing - not experimentally, but taking the opportunity to look how other nations are dealing with ICT threats now and seeing, you know, the pros and cons of particular approaches. I think the U.S. is still, is still, - we're still debating and we're still deliberatively working through, you know, how we would, you know, big picture, look to mitigate large-scale risk to telecommunications networks.

John Costello: Internally, you know, we are working on better understanding 5G risks to critical infrastructure. I think, once we get a better understanding - I mean, one of the biggest problems we have is, you know, we don't have a lack of imagination, but the more complex a network becomes, the more you add to the stack, and then you have software define the networking. The attack vectors are manifold.

John Costello: So the number of ways that - the number of ways that an attacker could get at a 5G network or manipulate it or to manipulate or steal data becomes - exponentially increases as the network becomes more complex. So it's difficult, I think, to - I think right now it's difficult - besides some of the obvious examples, such as attacking IoTs, it's difficult to really make a set of visceral examples that I think the public would understand. But I think, in discussions with industry groups, we've made it clear that it's a pressing concern. Supply chain - specifically, ICT supply chain is a number-one priority for our agency for 2019. I think once we have a better understanding and can - I think can give better concrete examples that we think the public would digest, I think you'll see more from us on that. But right now, it's discussions with industry and really trying to understand the threat better.

Clete Johnson: So I'd love to hear your take on the market, and the role that not just the U.S. government but also other allied governments can take with regard to imbalances that may exist in the market. So - and feel free to be specific, if you like.

Chris Boyer**:** I'll try to avoid that. But I will - I'll say a couple different things. You know, one is, is that if there's concerns in the U.S. government about particular suppliers - which we all know what that is - my general view is there ought to be a consistent policy that's applied across the board. I think there's a challenge right now in that there is still the potential for some disparity because there isn't a consistent policy, even domestically. So I think there should be a policy. And whatever that policy is, the second question then becomes: Does it scale? You know, our business is all about scale. You know, suppliers need to have access to broader markets. I don't think the U.S. can just do it by itself. So, A, have a policy; B, make sure that you have enough scale, that it can be applied where, you know, we really need to get allied countries or with similar views kind of all on the same page about how to deal with this issue.

Chris Boyer**:** I find it disconcerting that we hear in the news every day that, you know, one country is considering certain things, others are considering something totally different. You know, if we end up in that place, where there's different strategies all around the world, to me that's just a recipe for more of the same. And we know that there are particular entities that have stated goals to dominate certain segments of the technology industry by certain dates. And they're continuing to move in that direction. And I think we have to have a unified front to deal with those issues. And I don't think that solutions will work if we don't have - if we don't do them at scale.

Clete Johnson: Unified front is that government? Governments and companies?

Chris Boyer**:** Well, I think - I think likeminded countries need to have similar policy goals so that - because I think what's happening is you're seeing certain entities that are effectively subsidizing businesses to go into certain - to go into countries and offer products at price points that, frankly, a lot of other folks can't compete with, or investing in technology in massive ways. And if that continues to happen for the next five or 10 years, I think - you know, where are we going to be in five years? So if you're really considering a policy strategy, it has to consider making sure that it's not just the U.S., but other countries that are in similar positions have a similar view. Otherwise, we end up with the current situation, which I think - from everything I'm hearing from the administration and from members of Congress and others, is kind of untenable.

Clete Johnson: Travis.

Travis Russell: So I'm a technologist. That's real dangerous when you ask a techy guy about policy. But I'll share with you some of the things that we're seeing, though, in the global market, because, you know, we're in the position where, you know, we're bidding against some of the same opportunities Huawei and ZTE are bidding against, and everybody else in the ecosystem. And we've - over the years, we've -

Clete Johnson: Travis, who are the players? Everybody knows Huawei and ZTE. Who are the other players that you would mention?

Travis Russell: Yeah. So, by the way, it's not three. It's five. There's Ericsson, Nokia, Huawei, Samsung, and Oracle. And, I know, everybody says: Oracle? They make databases. Oracle actually has made acquisitions over the years that has placed them as one of the leading providers in critical infrastructure and telecom. So we're in AT&T, and we're in Verizon, we're in Spring, and T-Mobile, and all of the big networks globally. So we have a vested interest in all of this.

Travis Russell: I find it interesting. You know, the U.K.'s position was, well, we're not too worried because we're going to test the systems before they go into the networks. And so they actually set it up with –

Clete Johnson: I mean, U.K. is – the Huawei equipment and services in the U.K.?

Travis Russell: Right. And so NCSC started this exercise. And a few months ago, they actually sent a communication to all the operators that said: You know what? What we've discovered is that Huawei doesn't build product and then ship it to all of their customers. They send servers to the site and then they send hundreds of engineers to go custom-develop the product on location. So that means that you can't test the product that's sitting in the network until you go to that – each specific product and test it while it's in the network. And that's just not feasible. And so that's what they – actually, in their recommendation, they went back to the operators in the U.K. and said: Based upon this development model, you cannot test and make this secure.

Travis Russell: So consequently British telecom just announced that they're not only going to ban Huawei from 5G, but they're ripping them out of their 3G and 4G networks because they've now recognized that risk. And we're seeing this and hearing this in other markets as well. Everybody wants to take a conservative approach first because there's a lot of money involved here. And it's a big investment for a lot of countries. And so they're approaching this, rightfully so, in a very careful manner. But, you know, as you follow these trends, you start to see more and more countries are reversing their decisions as they start to understand a bit more about how it is that the Chinese do business.

Travis Russell: And, you know, to your point about the IPR, where they actually get paid, you know, we got Mobile World Congress coming up here in a couple of weeks. It's the largest telecom event in the world. and I will spend the entire week chasing Huawei employees out of my booth, because they get paid $5 for every picture that they take of my booth. So this - and this has been going on, by the way, for years. By the way, Mobile World Congress has called for an emergency meeting amongst its executive members in Barcelona to also address this problem with Huawei and ZTE. So be watching post-Barcelona. There'll probably be an announcement coming out of the GSMA, even, as they weigh into this.

Clete Johnson: So, digging a little bit deeper on this, we have - everybody talks about the race to 5G. And lots of countries, and groups of countries, and their companies are involved in that race. One of those - one of those countries, China, essentially has an authoritarian capitalist approach to industrial policy. And Huawei and ZTE are a big part of that. And it's a global industrial policy. The United States and its allies don't really do things that way. And I don't know if we want to. But if you have one very large country with two very large national champions that are - that are part of an industrial policy, how do the United States and its allies, and the companies that are based in those countries that don't have an authoritarian capitalist approach, how do they compete?

Robert Strayer: It's a good question. Let me say that that's one of the reasons why I emphasize that it's important that, as wireless operators and sort of regulators that influence the wireless operators in countries around the world, they go to put out solicitations for 5G and next generation telecommunications networks, that they put out transparent bids and that they seek to have any financing done on commercially reasonable terms. There are well-documented cases -including with regard to Sri Lanka, of not transparent terms, of not commercially reasonable loans being given, things used for collateral including the port of Sri Lanka - demanded as collateral to pay off debts - that nobody doing business on an international basis would consider to be the way to do business.

Robert Strayer: So I think what we need to do is set the conditions - the level of competitive playing field. I think if we have fair competition Western technology and others could fairly compete against these other companies. But when there is a financing mechanism that's backing them on an uncompetitive basis that is unduly influencing the playing field there is not a fair competition that can occur between different equipment vendors. So I think that's - part of the answer is just setting up the competition, the playing field on a level manner.

Clete Johnson: So do you - and this is for the - for the whole group. Do you need the united front that Chris mentioned, that is likeminded governments and companies, to come together to help create that fair playing field? Or can - does this one large bloc - China and Huawei and ZTE - compete against a whole bunch of cats that haven't been herded? Is that - is that - can it be done like that? Or does a united front need to be developed?

Robert Strayer: I think it's important that we establish that there are certain basic principles and normative standards that need to be applied in this area. Now, how that is coordinated exactly, I mean, that doesn't necessarily have to be, if you will, a united front. But I think that that sentiment needs to get into the way that countries that value competition and having the best technology for a much longer term of multiple cycles of next-generation technologies being deployed should recognize that that's going to be important for the future, that we keep competition in this field and do business as we have for, you know, many decades. And we've seen obviously internet and all kinds of information technology grow up in successful ways based on that model.

Clete Johnson: Anybody else on that?

Travis Russell: Yeah. I think, you know, we're all for obviously competition. I think it's healthy. But, you know, the challenge that we have seen - and this has been over, like, a 10, 15-year period - I'll give my Brazilian story because I love this example. There was a proposal in Brazil for a company called Oi. And Huawei won that particular proposal for the entire network. And their challenge was - because, as I mentioned, they have to send engineers to go develop this stuff - they had several hundred engineers that they had to get visas for, get them into the country so that they could then go build the product. They couldn't get those visas, so they chartered a cruise ship and they lived on this cruise ship for months anchored off of the coast of Rio and they ferried these employees back and forth so that they could go build these products. And on top of that, not only did they cut the price in half when they did that, but they also threw in there the entire network, not just the radio network, no extra charge, and service and support at no extra charge. And we see this being repeated in every single region.

Travis Russell: So, you know, it begs a couple of questions. One, how can a profitable company sustain any kind of profit if they're having to send thousands of engineers and house them, sustain them out at all of these customer sites, and at the same time do things like charter a cruise chip to house them in right?

Travis Russell: And I think another thing that we saw around loans - Carlos Slim in Mexico, when he was trying to get his 4G network built out, the Bank of China gave him a billion dollars at 1 percent interest if he spent 80 percent with Huawei. It's real hard for any vendor to compete against those types of deals when they come onto the table.

Travis Russell: And I've talked to, you know, some of the rural providers here and they've been very, very candid: We really don't care what the government says. When they come and offer me something for free, I'm taking it, it's free. Why wouldn't I?

Chris Boyer**:** Yeah, just a - I mean, I basically agree with what Rob said. I mean, I'm using the term "unified front" but that's kind of a euphemism for the idea that everybody agrees that there's some sort of strategy, right? That we have agreement with our allies in other countries on a way to deal with this issue. Because if the idea is to have fair trade or fair competition, you know, how do you do that if you don't have some sort of a broader understanding amongst other countries that this is - this is what constitutes a fair level of competition?

Chris Boyer**:** And I think the concern, I think what you're hearing what Travis is saying, is that there are at least anecdotal examples of unfair competition that's come up in many different examples. And whether it's - whether it's - whether it's financing, you also have OPEX issues and all sorts of different agreements that have been made. So I think the idea that there needs to be some sort of general understanding of how to deal with these issues from likeminded countries or institutions is really what I'm driving at. And to be successful, it does require some level of scaling beyond just the United States, in my opinion.

Clete Johnson: John?

John Costello: I think - I think this is - you know, I think some of the Chinese business practices that we've seen, which can be unscrupulous or unethical, I mean, clearly, financing is clearly supporting Chinese state interests. Those conditions of competitions are completely untenable, I think, in a - in the ideas of free market capitalism. And I do not see us changing that behavior or forcing the issue or resetting those conditions of competitions without a - without a coalition, you know, with a foundation of a common set of principles, a common set of principles that we already hold, and really holding certain companies and certain vendors in certain countries accountable to those principles. I think that that's - that that absolutely has to happen. I do not see countries going, you know, onesies and twosies trying to combat that. I think that's - the bilateral approach here does not - does not work. And I don't - I think some would prefer that it continues down a bilateral approach. And I don't think that's going to work.

Chris Boyer**:** Can I just say, like -

Clete Johnson: Yeah.

Chris Boyer**:** This is - I mean, this kind of goes back to my initial comment. This is just one - this is just one aspect of the 5G issue.

Clete Johnson: Right.

Chris Boyer**:** We're kind of going down the rabbit hole with all the -

Clete Johnson: Right.

Chris Boyer**:** - international relations side of it. But, I mean, that's why at the beginning I was saying, like, you have - you have these different buckets of issues and one of it is, how do you control for these suppliers that you may view as being, you know, having issues with them, right? Or that's a specific issue. Then you have the issue of, how do you - how do you secure the network and how do you make sure that the devices are secure, which is kind of what Travis is talking about and what we've been dealing with in terms of industry standards and the CSRIC report and those types of issues.

Clete Johnson: So we have, first of all, all of - all of these companies, that all the companies that are based in, you know, rule-of-law based market democracies compete against each other. Then all of those countries and governments, even if they're allies, they have different interests and they're kind of bumping against, you know, different equities that they're trying to advance. And then even within the U.S. government, you have disagreements about where the FCC's authorities go or the role of DHS vis-à-vis all the other agencies. You know, humanity is kind of stove piped and territorial. So how do you, how do we - specifically, how do we arrange that fair competition with all these disparate groups, competing companies, countries that are jockeying for position?

Clete Johnson: And maybe do a speed round on this. So just, what are some specific things that can be done to bring that coalition together?

Travis Russell: I don't think it's going to be that difficult. I mean, Nokia and Ericsson are likeminded and they have the same concerns. And I think, you know, I think some more tighter collaboration with them and even Samsung. I mean, we're doing a lot of work with Samsung. So I think, you know, we all have the same goal in mind, right? And I think we can all benefit from some tighter collaboration.

Clete Johnson: Anybody else on that?

Chris Boyer**:** I go back to Commissioner Rosenworcel's comments at the beginning. I do think domestically it's encouraging to see that the FCC is partnering with DHS and that - and that - I noted that you mentioned that they are participating on the supply chain task force. So I think - I think there is a locus of activity there at the - within DHS. And if I put my communications sector hat on, we've spent a lot of time partnering with DHS on a myriad of activities there. So I think there's - I'm actually encouraged that there's some movement in that direction. I think, you know, we'll see what the output of the supply chain task force is, but I think that's the right vehicle.

And I was encouraged that the FCC is seeing that also as an - as an appropriate place for them to engage as well, so I think that's a move in the right direction.

John Costello: Honestly, you know, this might sound a little glib, but harness that tribalism. I mean, one thing we tried to, you know, reinforce in the discussions with industry, discussions with government, I mean, there are interesting battles between, you know, between government departments and agencies, we all know this. And the same thing with, you know, market competitors.

John Costello: The thing we're reminded of is we - this is infrastructure, this is stuff that we share, this is stuff that we depend on, this is risk that is going to hit us. And although, you know, there might not - you know, there is going to be at some point in time a decrease in your profits, there is going to be loss, there is going to be cost, there is going to be, whether it's, you know, public perception, whether it's in profit, whether it's revenue, I don't know, but at some point it is going to hit you if there are security risks at play.

John Costello: You reinforce that - I mean, obviously, we don't want to go around fearmongering, like, banging on a, you know, banging on a pot and pan and saying, hey, the sky is falling, but reminding people that we're in this together and we're trying to protect infrastructure while also promoting, you know, something, maybe appealing a little bit to patriotism, that certainly works domestically. And then when you look at abroad or more internationally - I should probably kick it off to Rob at this point - looking at it abroad or internationally, it's really the same thing. Again, we're all in this together, risk does not stop at a - risk does not stop at a country's borders, especially in a more globally interconnected world.

John Costello: Now cue Rob.

Robert Strayer: Yeah. Like I say, John and I just didn't meet today. You know, like, we're part of this interagency that thinks about things in a comprehensive way. And I think, you know, as we've been talking about, it's a multifaceted challenge and, you know, diplomatic and international engagement is just one piece of that. And so, you know, we are all, in the interagency, bringing our best tools to the table to think about which aspects of these - of the challenges we face we can best address and we do it in a cohesive manner. So I'm quite optimistic actually about our ability to work through these types of challenges.

Clete Johnson: I'll do one more question and then we'll go to the - to the audience.

Clete Johnson: So it was actually really interesting to hear Commissioner Rosenworcel essentially endorse the recommendations of re-chartering the CSRIC, focusing more deeply on a second deep dive on 5G security issues, not just supply chain, but also the network function virtualization, IOT considerations, et cetera, and also that she sees a fulsome role for the FCC in this interagency effort, which, again, is actually what the CSRIC recommended.

Clete Johnson: So to a skeptic who thinks that, you know, Huawei and ZTE are taking over this world and that the future of 5G can't be secure because of that, let me just ask, is this process of CSRIC recommendations, engagement with DHS and the interagency and public-private partnership, international engagement, is that enough?

Chris Boyer**:** I'll take a shot at that.

Chris Boyer**:** I'm going to separate the two issues. One issue is, who do you use as your suppliers in building out the network? And AT&T has announced its suppliers for its 5G network, none of which are Huawei and ZTE, none of which will be Huawei and ZTE. And so, at least for domestically in our network - and I think I can - I don't want to speak for my brethren in the industry, but none of the major carriers - they've all made announcements in this space, and none of them have announced the use of any of those particular suppliers that we've been talking about on the panel. So domestically that issue has somewhat been - is somewhat going to be cared for.

Chris Boyer**:** Now, I do think there should be a policy, as I said, and it should be somewhat consistently applied. But, you know, I think we're definitely dealing with that issue.

Chris Boyer**:** I think that the international issue is more the future of the supply chain. And what happens if the U.S. decides to forgo those opportunities and other countries continue to use them and certain entities chew up market share around the world, and what are we left with? What does that world look like in five years? That's a different question, but that's the longer-term issue that we're kind of struggling with.

Chris Boyer**:** There's a totally separate issue around how do we secure the 5G network itself and make sure that we put in place the right practices to deal with some of the threats that we're continuing to see? And that's what I think the CSRIC work is going to, which is, you know, how do you deploy Diameter? How do you build out the secure mobile edge, and how do you push these capabilities?

Chris Boyer**:** One thing on security we like to say is that, because the 5G network has more integration between the edge and the core, you have better ability to monitor traffic and apply security controls. But other people would argue that creates a different risk posture. So there's one issue on the use of suppliers. There's another issue on how do you secure the 5G network.

Chris Boyer**:** On the 5G network itself, I'm encouraged because of the work that's going on in groups like the CSRIC, but also work that's going on in places like 3GPP, SA3, and those types of entities.

Travis Russell: I think, though – I'll counter one thing there, because I agree, the big four in the U.S. certainly will not be using Huawei or ZTE. But the problem, though, is not the big four. The problem is the 400-plus telephone companies in the United States. Now, we're really an anomaly, because I don't know of any other country that has this problem historically the way that our telephone system has been built with, you know, Grandma Jones with the switchboard in her living room has just been handed down generation to generation.

Travis Russell: We have telephone companies with less than a thousand subscribers in them. And Huawei is targeting those companies today. That's why you'll see Huawei is the premier sponsor of CCA. They are the premier sponsor for the World Wireless Association. They're putting up a bunch of money in investment in the small rural market, because they see that as a way for them to get traction here in the U.S. market.

Chris Boyer**:** Yeah, I don't disagree with that. And that's why I think they're – that's why I said earlier there needs to be a policy, because right now you have a lot of companies that are making these decisions but, you know, the policy is still being developed, as best I can tell. And that's also why I think the FCC has – their proceeding is up right now on the USF issues, so.

Clete Johnson: Robert, I'd love your take. Is this enough, or does more government-directed action need to be taken?

Robert Strayer: I mean, I think there's always a spectrum of activity you can partake in. There's obviously more that we need to do and more that we're going to be doing.

Clete Johnson: Good. All right. Well, with that, I want to open it up to audience questions. I think we've got about 15 minutes left. Can I get – here we have somebody right down here.

Clete Johnson: Please identify yourself and if there's a particular person you would like to ask the question.

Q: Hi. My name is Veronica. Thanks for being here and expressing your concerns about this topic today.

Q: This question is not directed to anyone, but if anyone can answer. I have a couple of questions.

Q: So with all the concerns that we have regarding the 5G networks, how do you propose that we should translate that to the public, who may not even know what technology is about, may not even be familiar with an innovative sector? And for those people, which is the majority of the public, then the convenience and the cost-effectiveness would be their primary concern. And in that case, like you had just mentioned, Huawei would take a great lead on that because their stuff is a lot cheaper.

Q: And then my second question would be I also attended the CSIS event yesterday talking about China's digital leadership. And the statistics show that in the U.S. – actually, let me rephrase that. In ASEAN countries, people are using technology a lot, a lot more than people here in the U.S. So that brings another concern because those people in the ASEAN countries are going to rely on China for – to provide products. So that's – my second question would be how do we retaliate against such a proprietary competitor? And I know we've talked about connecting the international community, but who is willing to take that lead to sort of set up the standard for the world? Thank you.

Clete Johnson: Anybody want to take a stab at that?

Robert Strayer: I can take the second one first and then maybe let the private-sector guys handle the first. Or, John, you can jump in, too.

Robert Strayer: I'd just say that, you know, one of the reasons why, with respect to your ASEAN question, that we frame this as part of the general cybersecurity concern is that we've done tremendous work with ASEAN countries on cybersecurity. You know, they're looking at tremendous economic growth, going into the future, in their populations. So trillions of dollars of GDP is at stake in the digital area if it's not secure. So I think that's why we come in there and talk about how insecurity with digital technology just can put – can jeopardize the growth that they're looking at getting, particularly from digital technologies.

Travis Russell: Yeah. You know, going to your first one there with the consumers, I mean, we've been struggling with this question for a while when we started looking at IOT because – you know, IOT devices affect everybody, right, and there's a lot of schemes that are being defined about, you know, certification of an IOT product, for example.

Travis Russell: But what I have found is that – you know, I go to a big box store and you'll see security cameras, and I'll listen to people talking about which ones they want to buy. I have never heard in any of those conversations, you know, I think I want that one because I think it's more secure, or, hey, you know what, that one's got that UL label on it so I feel better about buying that one. It always comes down to, that's got the cheapest price and so that's the product that I want.

Travis Russell: So I see, you know, one of the biggest risks that I see in 5Gs is proliferation of IOT-connected devices being introduced into the network with zero security built into them because it's all about price.

John Costello: Yeah. Speaking on behalf of DHS, you know, one of the - one of our biggest - one of our biggest missions is educating and informing the public and letting them know security risks that are out there. This isn't a new challenge. You know, we've had the STOP.THINK.CONNECT campaign and cyber hygiene campaigns for years in the past and it is a constant never-ending battle to try to educate the general population. When DHS first started and the cyber programs were first started, getting that out there and saying, you know, don't use "password" as your password is a consistent battle.

John Costello: I mean, I don't see 5G in different - any differently. I'd say the - you know, the biggest question is, is what exactly are we trying to get across to the general public about 5G. If it's IOT devices - security of IOT devices - you know, don't buy an IOT device that - you know, that has a manufactured hardcoded user name and password. Otherwise, you're going to end up with, you know, a Mirai botnet again. You know, but how do you translate that to the general public I think is just really difficult.

John Costello: I think we're just going to have to keep reinforcing the same sort of cyber hygiene principles we have in the past and, again, scenarios, stories, and narratives are really the most powerful way to inform the general public. I think more important than that, though, is getting across to C-suite and private industry the risks of 5G and, to a greater degree, the risks of supply chain.

John Costello: I mean, that is still - that's still a challenge and you have to have a much more nuanced conversation. I mean, you look at - you know, you got to hit the C Suite, you got to hit the policy people, you've got to hit the technical operators, and you got to hit the general public and making sure all of them understand the things that are important to them and the things that they should do or the resources available to them. It is, you know, a lot of - you know, a lot of my job is, honestly, marketing and trying to figure out how to get it - how to get the message across. So -

Chris Boyer**:** Yeah. I mean, I generally agree with that sentiment. If you're talking to consumers, you have to look at it from the perspective of how are they going to interact with 5G. They're not going to interact with the core network. They're not going to deal with things like Diameter. That's way beyond what any consumer is ever going to understand. The way they're going to interact with the network is through the device, and so if you're going to try to communicate something to them, it's going to be at that level.

Chris Boyer**:** So how do we go about and, you know, ensure people feel reasonably confident that the devices they're purchasing have some level of security? You know, the good news is there's a lot of active discussion in the industry side and with the government about that issue. Just a couple months ago, we put out a report from an entity that we call the Council for Securing the Digital Economy where the Consumer Technology Association and some others developed some ideas around kind of a baseline of what types of security should be built into a device. So there's work going on in that space.

Chris Boyer**:** And there's sort of – to me, there's two questions. One is: What's the basic security, the baseline of security, that should be built into the device? And then there's the second-order question of how do you communicate that to the consumer that's buying the device and what's the utility of that. There's no perfect answer to that question yet. That's still something that's being actively discussed. But I definitely think that's the area that that part of the conversation needs to go.

Travis Russell: There is some good work being done in ATIS, though, by the way, around devices, because –

Clete Johnson: You want to explain ATIS? Can you explain ATIS?

Chris Boyer**:** The Alliance for Telecommunications Industry Standards (sic; Solutions).

Travis Russell: Yeah. I mean, one of the challenges that we faced was –

Chris Boyer**:** Another acronym. (Laughter.)

Travis Russell: – you don't want to have the same level of security – my connected toothbrush doesn't need to have the same level of security as my pacemaker, for example. And so there's a lot of good work going on in the standards. First off, let's classify what these devices are. If it's a mobile device, then it probably needs a different level of security and a different treatment than my connected toothbrush or hairbrush. And I think that applies in so many different areas, whether it be a laptop or a phone or any other kind of a device, right? And I think that goes a long ways to being able to educate customers, you know, that particular device, it's pretty critical, and so you need to have these types of things. You need to take these things into consideration.

Clete Johnson: Any other questions? Oh, we have a lot. And I'm not sure whose hand was up first, but I think maybe here with the scarf.

Q: Hi. Thanks very much. Blaine Johnson from the Center for American Progress.

Q: I'm wondering, when you're talking about coordination between, like, many countries, what platforms are the best ways to do that? Are we talking about adding something to the WTO? Or what other institutionalized ways can we go about with this coordination? Thank you.

Robert Strayer: You know, frankly, a lot of our coordination happens on a daily basis through our capitals or from Washington, you know, directly to them. So, you know, we don't necessarily work through a multilateral institution to have as a coordination mechanism, so.

John Costello: And, I mean, there's a lot of cybersecurity cooperation that goes on daily and hourly between, you know, DHS cybersecurity centers and national cybersecurity centers, like, overseas. I mean, it's honestly constant contact at this point just given the nature of the threat and the need to work together. So those often are the most expedient forms in which to have a conversation on these things.

Clete Johnson: Anybody else? Yes, please.

Q: Hi. This is Kate O'Keeffe. I'm a reporter with The Wall Street Journal.

Q: And I wanted to know from the U.S.'s perspective how important is it to push back against Huawei in the Indian market in particular, given the size of that market? And I was wondering if you could characterize any conversations the U.S. and its allies may be having with India right now to engage on that issue and what the response has been. Thank you.

Robert Strayer: I'm not able to – I'm not going to characterize any particular conversations with any particular government. But I will say that, you know, over time we form close collaborations with the Indians as part of our general Indo-Pacific strategy, cybersecurity, just as I said with the ASEAN countries. You know, all these countries are going to see rapid economic growth in part based on their digital economies, so they're very interested in how they can make sure those are done in secure ways, and they're not disrupted and sort of degraded by cyber intrusion. So, you know, we're talking to them, among others – among, you know, basically the whole world – about our concerns about – and as I said earlier, we have sort of general principles. We're not making this about any one country. But we have – we have identified we think there are certain principles that should be applied when making these decisions about procurement of next-generation technologies, both on the just sort of general economic side of that, as well as with regard to the security that should be behind it, and the trust in the vendor, and the vendor's relationship with the government where they are headquartered.

Travis Russell: India actually has already pushed back. And in fact, you know, they did – a number of years ago they did a major pushback. I think at that time it was mostly because of anticompetitive behaviors. And they've come back again and said no, no more Huaweis in these networks. So I think they've already acted and have already been pushing back on that front.

Clete Johnson: That's a good – we have one minute to go and we'll do a speed round. And we'll have to – I don't know if Jim is still in the room here, but we'll have to discuss this in further depth in the next event on these – on these issues. But for all of you: Are we headed to a bifurcated ICT environment that's sort of a tech cold war where there's one bloc that uses these types of companies and another bloc that uses Huawei and ZTE, and all the things that go along with that? It's a really easy question, Rob.

Robert Strayer: It's a(n) easy question. (Laughter.) And, as you would expect, I think there's an easy answer. No, there's not.

Robert Strayer: I think that there is an active competition about the values that underpin our digital economies based on how - from the most foundational things about how we treat our own citizens, about citizens' rights online, about censorship, about how they're treated by their government, the relationship with the state, and what kinds of controls over data are then imported into such regimes.

Robert Strayer: So there is an active discussion around the world. We as the U.S. government are actively out there every day, aggressively talking about our vision, our vision, which we think will make people much more successful in the long run. But this competition that's going on is not something that's going to be resolved tomorrow. It'll be, I think, decades. And it's something that I think we constantly have to be vigilant on. And, you know, we're having one conversation about next-generation technology. Maybe you say just done 5G today, but there's a much bigger discussion, a much bigger set of values, that are - that are at stake here and that are in very active discussion at the most senior political levels.

Clete Johnson: Just to add something to that, with the turbocharging of the deployment of IoT that will come with 5G comes an exponential growth in data, which is directly relevant to AI and what the data is used for. And so you guys - cold war or just competition?

John Costello: I don't think anyone wants a globally bifurcated ICT ecosystem. But I will say this. I don't believe the U.S. is going to allow unfettered or unmitigated presence in our telecommunications network by a company controlled by a foreign power with whom we have long-term strategic competition and questionable rule of law. I think that that's like - that's as a basic principle.

John Costello: You know, I feel like Rob's echo up here. But there's a - I mean, there's a long-term strategic competition with China, and it's going to present - and we are very entangled with them. And that includes technological entanglement.

John Costello: The issue that we have is China is blocking access or mitigating market access to our technology companies at the same time they're pushing theirs, not only globally but, you know, deeper and deeper into U.S. markets. That creates a massive asymmetric vulnerability, you know, that is very concerning to the U.S. government.

John Costello: At the same time, we need to keep our moral authority and stay true to American principles of free-market capitalism and democracy and not go into authoritarian route. So it's difficult and it's going to - you know, it's going to require a lot of hard conversations, a lot of hard decisions. But I do not believe anyone wants a bifurcated system, but we have to maintain our national security and our principles as a nation.

Clete Johnson: Chris, Travis, anything to add? Two minutes over, so you get a pass if you don't.

Chris Boyer**:** I certainly - I mean, I certainly hope we don't end up in that place. But I think 5G is just one manifestation of a broader set of issues. I mean, this whole - this is the same issue that comes up in discussions around things like cross-border data flows and localization controls and those types of things. It's coming up in a lot of contexts.

Chris Boyer**:** So I'm encouraged that the U.S. government is kind of taking some leadership in that space and there's been some movement to deal with those issues. I hope we don't end up there. You know, we'll see what happens, right?

Clete Johnson: All right.

Travis Russell: I think it's competition. I mean, we're seeing that. And we're seeing countries now are starting to rethink some of their own policies as they start to reconsider, you know, the security questions, and certainly around privacy, you know. I mean, that's what we saw in the European Union when they were trying to deal with the SS7 stuff. They said really this is a privacy breach. And now we have GDPR.

Travis Russell: And so I think there's a lot of that discussion going on globally, and companies are starting to think, well, you know, we've got other choices. Do we want to make a decision based on price or do we want to pay a little bit extra and know that we don't have to be looking over our shoulders all the time?

Clete Johnson: Great. Well, thank you all. Thanks for being here.

Clete Johnson: To the folks who are watching online - I think we have well over 300 people who are either here or online.