{York Stenographic Services, Inc.}

RPTS MEYERS

HIF141.160

``CYBERSECURITY: AN EXAMINATION OF THE COMMUNICATIONS SUPPLY CHAIN''

TUESDAY, MAY 21, 2013

House of Representatives,

Subcommittee on Communications and Technology

Committee on Energy and Commerce

Washington, D.C.

The Subcommittee met, pursuant to call, at 2:02 p.m., in Room 2123 of the Rayburn House Office Building, Hon. Greg Walden [Chairman of the Subcommittee] presiding.

Members present: Representatives Walden, Latta, Shimkus, Terry, Blackburn, Lance, Guthrie, Gardner, Long, Ellmers, Eshoo, Matsui, Welch, and Waxman (ex officio).

Staff present: Carl Anderson, Counsel, Oversight; Ray Baum, Senior Policy Advisor/Director of Coalitions; Neil Fried, Chief Counsel, C&T; Debbee Hancock, Press Secretary; David Redl, Counsel, Telecom; Charlotte Savercool, Executive Assistant, Legislative Clerk; Kelsey Guyselman, Telecom; Roger Sherman, Democratic Chief Counsel; Shawn Chang, Democratic Senior Counsel; Margaret McCarthy, Democratic Staff; Patrick Donovan, Democratic FCC Detail; and Kara Van Stralen, Democratic Policy Analyst.

Mr. {Walden.} We are going to call to order the Subcommittee on Communications and Technology for our hearing on ``Cybersecurity: an Examination of the Communications Supply Chain.'' And just for our witnesses--I don't know if benefit is the right word--but in about 10 minutes we are probably going to get called to the House Floor for votes. So don't flee when we do. We will plan to return and be sure and get your testimony in and our questions. But we will begin with our opening statements and, as you know, things around here aren't always certain so, who knows, we may get everything done, but I doubt it. So we will go ahead and get started, but we want to thank you all for being here and for submitting your testimony.

Our communications networks strengths--its ubiquity and interconnected nature--may actually also be a weakness. Those who wish to harm our Nation, to steal money or intellectual property, or merely to cause mischief can focus on myriad hardware and software components that make up the communications infrastructure. And they can do so anywhere in the design, the delivery, the installation, or the

operation of those components. So today's hearing will focus on securing that communications supply chain.

We are fortunate to have as a member of this subcommittee the full chairman of the House Intelligence Committee, Chairman Mike Rogers. The experience and resources he brings were invaluable to the bipartisan Cyber Security Working Group last Congress, as well as to this subcommittee's three prior cyber hearings.

Many of us have concluded that promoting information-sharing through the Cyber Intelligence Sharing and Protection Act, CISPA, that he and Representative Ruppersberger have now twice assured through the House, with large bipartisan votes, is pivotal to better securing our networks. It was also in large part this committee's 2012 report on the communications supply chain that prompted this hearing. Supply chain risk management is essential if we are to guard against those that would compromise network equipment or exploit the software that runs over and through it.

Understanding that you can never eliminate these risks, how do you minimize them without compromising the interconnectivity that makes networks useful? How secure is

the communications supply chain? Where are the vulnerabilities? How much should we focus on securing physical access to components as they make their way from design to installation? How much are the internal workings of the components themselves? How do the risks and responses differ for hardware and software? What about for internationally sourced products as opposed to domestically sourced products? What progress has been made through the public-private partnerships, standards organization, and the development of best practices and what role should the government play?

These are among the questions we will examine in this hearing, as well as through the bipartisan Supply Chain Working Group that we launch today. Representative Mike Rogers and my colleague and friend from California, Anna Eshoo, will co-chair this group, which will also include Representatives Latta, Doyle, Terry, Lujan, Kinzinger, and Matheson.

As I did last Congress, I will urge that we abide by a cyber Hippocratic Oath and first do no harm as we consider the tools available to the public and private sectors in

making our communications supply chain secure.

With that, I would yield to the vice chair of the subcommittee, Mr. Latta.

[The prepared statement of Mr. Walden follows:]

********** COMMITTEE INSERT **********

|

Mr. {Latta.} Thank you, Mr. Chairman, and I appreciate you yielding and holding this hearing today on a very critical and important topic. I want to thank our witnesses for being here and I look forward to your testimony today.

Not a day goes by that I don't seem to pick up a newspaper and read about a cyber attack or the vulnerability on the front page of a newspaper. Cyber crime and cyber warfare can affect any individual or business since we all depend on our interconnected communication networks. This is an issue not just of national security but economic security.

Again, I thank our witnesses for being here. I look forward to your comments on the communications supply chain. I also thank the Chairman for convening a bipartisan working group on this topic and I look forward to being part of the start of a very thoughtful and serious discussion on the threats of the supply chain and possible solutions. And with that, Mr. Chairman, I yield back.

[The prepared statement of Mr. Latta follows:]

********** COMMITTEE INSERT **********

|

Mr. {Walden.} Anyone else on the Republican side seeking to make a comment on the final minute-and-a-half of my time? If not, I yield back the balance and recognize my friend, the ranking member of this subcommittee, Ms. Eshoo, for 5 minutes.

Ms. {Eshoo.} Thank you, Mr. Chairman, and thank you for holding this very important hearing. Welcome to all of our witnesses.

Mr. Chairman, the implications of foreign-controlled telecommunications infrastructure companies providing equipment to the U.S. market, I think, really presents a very real threat to our country. As the Office of the National Counterintelligence Executive has noted, ``the globalization of the world economy has placed critical links in the manufacturing supply chain under the direct control of U.S. adversaries.''

Just last month, despite press reports suggesting that Huawei was leaving the U.S. market, the company now denies such reports and has stated that, ``Huawei has no connection to the cyber security issues the U.S. has encountered in the

past, current, and future.'' That is quite a statement.

These are not new threats. It in fact, more than 3 years ago as a member of the House Intelligence Committee, I wrote to the director of National Intelligence asking for an assessment of the national security implications of Chinese-origin telecommunications equipment on our law enforcement and intelligence efforts, as well as on our switch telecommunications infrastructure. While I can't discuss, obviously, the results of that assessment in an unclassified hearing, suffice it to say, the answers were troubling.

Since that time, I have reiterated my concerns with the FCC Chairman Genachowski and in late 2011 I joined colleagues in requesting that the GAO study the potential security risks of foreign manufactured equipment. The newly released GAO study recognizes that multiple points within the supply chain can create vulnerabilities for threat actors to exploit. But a combination of initiatives by both the public and private sector are being established to fight back.

The President's Executive Order issued in February is an example. NIST has been tasked with developing a framework to reduce cyber attacks to critical infrastructure, and as NIST

undertakes the development of this framework, supply chain security should be a component. In fact, this morning, Chairman Walden and myself raised this very issue with Dr. Gallagher.

Moving forward, I am very pleased to co-chair, at the chairman's request, the subcommittee's newest working group focusing on supply chain security and integrity with Representative Mike Rogers, who chairs the House Intelligence Committee. And through stakeholder meetings, I think we will be able to better understand what additional steps can be taken to protect U.S. telecommunications infrastructure from inappropriate foreign control or influence.

So again, I thank each one of our witnesses that are here today for your important testimony that you are going to give, the important answers that you are going to give to our questions, and for your steadfast commitment to securing the communications equipment supply chain for our Nation.

And I yield back, Mr. Chairman.

[The prepared statement of Ms. Eshoo follows:]

********** COMMITTEE INSERT **********

|

Mr. {Walden.} If you want to yield to--

Ms. {Eshoo.} Does anyone want me to yield my remaining time to them? Ms. Matsui or--okay. Sure.

Ms. {Matsui.} Thank you very much, Ms. Eshoo. I would like to also thank the chairman for holding today's hearing.

This year alone, we have seen significant cyber breaches to our economy. We know rogue states and skilled hackers are relentless and continue to pose a real threat breaching sensitive information stored by both the private and public sectors, as well as the American consumer.

To address the cyber threats I believe industry and government must be partners. It is not a one-way street. We live in a digital world where information is readily available on the internet and can be accessed from just about anywhere. We also live in an innovative economy where America's innovative spirit has led to new devices, equipment, and communications that penetrate the global marketplace.

This has also created an international supply chain of technology components. Today, it is not surprising if a

product and its components originate from several different countries. That is why it is critical for industry to continue to be vigilant in assuring their manufacturing and distribution processes are not compromised. We should also be mindful of hackers trying to circumvent the supply chain by infecting botnets and malware onto popular mobile apps.

Addressing mobile security should be a priority moving forward, particularly as millions of Americans download their favorite apps, which in some cases includes personal information.

Again, I thank the chairman for holding today's hearing and I yield back the remainder of my time.

[The prepared statement of Ms. Matsui follows:]

********** COMMITTEE INSERT **********

|

Mr. {Walden.} The gentlelady yields back the remainder of her time. And seeing no one on our side seeking time, I would yield now to the gentleman from California, Mr. Waxman, for 5 minutes.

Mr. {Waxman.} Thank you very much, Mr. Chairman, for holding today's hearing on cyber security risks in the communications supply chain.

This morning, our full committee heard a ride range of perspectives on the cyber threats to our critical infrastructure, including broadband networks. While the Executive Order on cyber security protections for critical infrastructure was an important step forward, this morning's hearing demonstrated that there is much more work to be done to protect the networks that undergird the American economy.

One key area of vulnerability, the long supply chains for communications network equipment, is the subject of this afternoon's hearing. The globalization of the supply market for information and communications technology has undoubtedly created many benefits for our economy and coincided with incredible investment, competition, and innovation in the

communications marketplace. But it has also made it possible for our adversaries to exploit weaknesses during the design, production, delivery, and post-installation servicing of communications network equipment. Industry and the Federal Government are working to respond to these threats.

As several of our witnesses this afternoon will discuss, companies are taking action to respond to supply chain risks. Voluntary industry consortia and public-private partnerships are also seeking to minimize these cyber exposures and I applaud these efforts. But we should consider all options that could help minimize the cyber threats in the supply chain.

I look forward to hearing from GAO about its analysis of what other countries are doing in this area, as well as the potential benefits and drawbacks of adopting new review processes for purchases of foreign manufactured communications equipment.

And I am pleased, Mr. Chairman, that the Subcommittee is convening a working group to examine supply chain security in more depth. The co-chairs of the working group--Representative Mike Rogers, who is the chairman of the House

Intelligence Committee, and Representative Anna Eshoo, who has served on that committee, as well as the ranking member on this subcommittee--have great expertise from their service, as well as on both committees.

I look forward to our continued bipartisan work in this area. I thank all of the witnesses for being here and for their testimony. I want to apologize in advance that the conflict in schedule will keep me from being here to hear everything that is said, but I have staff listening in, I have got the testimony that I can review, and when the questions are asked and answered, I will be able to get a sense from those as well of the views that this very distinguished group will be giving to our subcommittee.

Thank you for this opportunity to give an opening statement. I thank all of you for being here today.

[The prepared statement of Mr. Waxman follows:]

********** COMMITTEE INSERT **********

|

Mr. {Walden.} And the gentleman yields back the balance of his time. The good news is the votes now aren't going to come until 2:25 to 2:30, so we may actually get to hear from some of our witnesses.

And so we are going to start with Mr. Goldstein, who is the director of Physical Infrastructure Issues for the Government Accountability Office. Turn on your microphone, pull it close, and the next 5 minutes are yours, sir. Thank you for your work.

|

^STATEMENTS OF MARK L. GOLDSTEIN, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; STEWART A. BAKER, PARTNER, STEPTOE AND JOHNSON, LLP, FORMER ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY; JENNIFER BISCEGLIE, PRESIDENT AND CEO, INTEROS SOLUTIONS, INC.; ROBERT B. DIX, JR., VICE PRESIDENT, GOVERNMENT AFFAIRS AND CRITICAL INFRASTRUCTURE PROTECTION, JUNIPER NETWORKS, INC.; DAVID ROTHENSTEIN, SENIOR VICE PRESIDENT, GENERAL COUNSEL AND SECRETARY, CIENA; JOHN LINDQUIST, PRESIDENT AND CEO, ELECTRONIC WARFARE ASSOCIATES; AND DEAN GARFIELD, PRESIDENT AND CEO, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

|

^STATEMENT OF MARK L. GOLDSTEIN

} Mr. {Goldstein.} I will try not to take all of it.

Thank you, Mr. Chairman and members of the subcommittee. I am pleased to be here this afternoon to discuss issues surrounding the communications supply chain.

The United States is increasingly reliant on commercial

communications networks for matters of national and economic security. These networks, which are primarily owned by the private sector, are highly dependent on equipment manufacturers in foreign countries. Certain entities in the Federal Government view this dependence as an emerging threat that introduces risks to the networks. GAO has requested review actions taken to respond to security risks from foreign manufactured equipment.

This testimony addresses how network providers and equipment manufacturers help ensure the security of foreign manufactured equipment used in commercial communications networks, how the Federal Government is addressing the risks of such equipment, and other approaches for addressing those risks and issues related to these approaches.

My testimony today is the public version of a national security sensitive report that GAO issued in May 2013. Information that the Department of Defense deemed sensitive has been omitted.

Let me briefly discuss the findings of the report that I may talk about today. First, the network providers and equipment manufacturers GAO spoke with reported taking steps

in their security plans and procurement processes to ensure the integrity of parts and equipment obtained from foreign sources. Although these companies do not consider foreign manufactured equipment to be their most pressing security threat, their brand image and profitability depend on providing secure, reliable service.

In the absence of industry or government standards on the use of this equipment, companies have adopted a range of voluntary risk management practices. These practices span the lifecycle of equipment and cover areas such as selecting vendors, establishing vendor security requirements, and testing and monitoring equipment. Equipment that is considered critical to the functioning of the network is likely to be subject to more stringent security requirements according to these companies.

In addition to these efforts, companies are collaborating on the development of industry security standards and best practices and participating in information-sharing efforts within industry and with the Federal Government.

Second, the Federal Government has begun efforts to

address the security of the supply chain for commercial networks. In 2013 the President issued an Executive Order to create a framework to reduce cyber risks to critical infrastructure, the National Institutes of Standards and Technologies, responsible for leading this effort, which is to provide technology-neutral guidance to critical infrastructure owners and operators.

NIST published a request for information, which it is conducting a comprehensive review to obtain stakeholder input and develop the framework. You heard testimony on this effort this morning. NIST officials said the extent to which supply chain security of commercial communication networks will be incorporated into the framework is dependant in part on the input that they receive from stakeholders.

The Department of Defense considered the other federal efforts GAO identified to be sensitive to national security, and I cannot talk about them in a public forum.

And third, there are a variety of other approaches for addressing potential risks posed by foreign manufactured equipment and commercial communications networks. For example, the Australian government is considering a proposal

to establish a risk-based regulatory framework that requires network providers to be able to demonstrate competent supervision and effective controls over their networks. The government would also have the authority to use enforcement measures to address noncompliance.

In the United Kingdom, the government requires network and service providers to manage risks and network security and can impose financial penalties for security breaches.

While these approaches are intended to improve supply chain security of communications networks, they may also create the potential for trade barriers and additional costs which the Federal Government would have to take into account if it chose to pursue such efforts.

Mr. Chairman, this concludes my oral statement. I would be happy to respond to comments. Thank you.

[The prepared statement of Mr. Goldstein follows:]

********** INSERT 1 **********

|

Mr. {Walden.} Thank you, Mr. Goldstein. We appreciate the work of your team and you--

Mr. {Goldstein.} Thank you.

Mr. {Walden.} --and we appreciate your being here.

I will now go to Mr. Stewart A. Baker who is a partner in Steptoe & Johnson, LLP, and we appreciate your being here and look forward to your comments, sir. Go ahead.

|

^STATEMENT OF STEWART A. BAKER

} Mr. {Baker.} Chairman Walden, Ranking Member Eshoo, members of the committee, it is a pleasure to be before you again. I was at the Department of Homeland Security and in charge of the CFIUS process until 2009, so I have been here before to talk about that.

I would like to start with the problem that we have. We are under massive cyber espionage attacks. There is no one who is proof against these attacks. I am willing to bet that everybody on this panel and everybody on the committee has already been the subject of intrusions aimed at stealing secrets on behalf of the People's Liberation Army or some other foreign government.

We do not know how to keep people out of our systems effectively. And that is despite the fact that we have, by and large, an IT infrastructure that is designed by U.S. companies who are doing their best to give us security. We simply have not been able to find all of the holes in the code or all of the flaws that can be exploited. That is with

the best will in the world.

At the same time, in the last 20 years, I think, as the President's efforts to name and shame China and other attackers have demonstrated, there is plenty of name but not a lot of shame on the other side. This has been an enormously productive intelligence source and it is an enormous weapon that can be used against the United States if we get into a shooting war that our adversaries would like to get us out of. Everything that can be exploited for espionage purposes can be exploited for sabotage purposes.

Our systems can be made to break causing great harm to Americans, including potentially deaths here. And we will have to face that prospect in the next serious conflict that we face internationally because the ability to cause that harm is moving down the food chain to the point where Iran and North Korea are significant powers in causing this harm.

So that is the situation that we face. The question is we are deep in a hole. Are we going to stop digging? And here is the question that we need to face as we look at our supply chain. If American companies looking at their own code and trying to give us security can't find a way to do

that, how comfortable are we having companies from countries that are not our friends provide the code, provide the hardware? We are not going to find those problems. We can't even find all of them in the products that we make ourselves here in the United States, as witnessed all of the exploitable vulnerabilities we face.

And so we face the prospect that some of this equipment simply is not going to be safe. As we have asked ourselves, how do we deal with that problem? It turns out that our tools for dealing with it are remarkably limited. I ran the CFIUS process; I ran the team telecom process for DHS. Those are very limited tools. CFIUS only applies if somebody buys something. If they want to sell something here, there is no restriction whatsoever. So telecommunications gear can be sold in the United States without any review whatsoever.

We got to the point, I think, actually in the stimulus bill where we had provided subsidies to buy telecommunications equipment to carriers and they were buying, with our money, Huawei and ZTE gear because we had no way to prevent that, but at the same time that the U.S. Government was telling Verizon and AT&T don't you buy that

stuff. So we clearly lack an ability to address the problem of infrastructure equipment being sold to the United States that we don't think is secure. That is the first thing that I think the committee should examine.

Beyond that, I think we have also discovered as we have begun looking at this problem that our procurement laws do not take account sufficiently supply chain risk, do not require that our contractors take enough account of supply chain risk. So if there were two things that I would urge the committee to address, it is, one, the limited nature of team telecom and CFIUS remedies and the still remarkably limited ability of government procurement officers to take account of this risk.

[The prepared statement of Mr. Baker follows:]

********** INSERT 2 **********

Mr. {Walden.} Mr. Baker, thank you for your testimony.

We are going to go now to Jennifer Bisceglie, who is President and CEO of Interos Solutions, Incorporated. We welcome you and look forward to your comments.

|

^STATEMENT OF JENNIFER BISCEGLIE

} Ms. {Bisceglie.} Thank you. Good afternoon, Mr. Chairman and members of the subcommittee.

Mr. {Walden.} I am going to have you moved that microphone a little closer and make sure the light is on.

Ms. {Bisceglie.} It was on.

Mr. {Walden.} Okay.

Ms. {Bisceglie.} Can you hear me now? Good afternoon, Mr. Chairman and members of the subcommittee. My name is Jennifer Bisceglie, President of Interos solutions. Thank you for inviting me to testify on behalf of our industry peers focused on supply chain risk management, or SCRM, as we like to call it.

My company Interos is built on 20 years of global supply chain and IT implementation experience. Over the past 6 years, we have seen the discussions turn from simple compliance to resiliency, which is ensuring business operations would continue even if the supply chains were interrupted; and now to product integrity, which is caused by

a manmade malicious attack.

In response to this, Interos has set up a SCRM global threat information Center, which offers capabilities to help both the public and private sector organizations implement SCRM frameworks, conduct supplier audits, and conduct open-source research to identify potential threats with current or future suppliers.

I will first share some of our observations and then follow those with some recommendations. First, a common definition for supply chain risk management and cyber security does not exist, nor is there a standard way to measure either challenge. To us, the definition of cyber security extends deep into the supply chain as cyber capabilities are increasingly reliant on globally sourced, commercially produced information technology and communications hardware, software, and services.

To us, cyber security means transparency of where things are coming from, where they are going to, and who has access to them along the way. That is also the definition of supply chain risk management.

Our second observation is that supply chain risk

management must be viewed as an investment versus an expense. Interos is working with the Department of Energy on their enterprise SCRM program. With only three Interos team members supporting the entire Department of Energy enterprise, they have an infrastructure they can share resources and information throughout their entire enterprise now.

In this case, it is a relatively low-cost investment and yields tremendous benefits. Much of the success of this program can be attributed to a strong DOE leadership, as well as having the ability to work with the Department of Defense's trusted systems and network SCRM roundtable and their interagency working groups.

Third, we feel supply chain risk management is successful when it is a cultural shift that supports current business process and reduces the need to develop new stovepipe processes that increase costs and create additional work for the risk owner. It is not an issue of being too expensive to do it. It is an issue of being too expensive to ignore it.

Now to our recommendations: from our perspective,

Congress can take four steps to better protect our Nation's critical infrastructure. First, awareness and education has to start at the top in order to be adopted by those actually executing the mission. In our experience, the level of awareness of the challenge varies across federal agencies, as does their level of attention to managing their supply chain risk. Awareness and education is critical to communicate that supply chain risk impacts everyone within the federal infrastructure.

Second, fund the program, assign someone within each agency to own the issue, and measure the success. We have seen SCRM focal points, as directed by the Bush and the Obama Administrations, being implemented in different areas within the agencies. Without the top-down support within the agency, without an owner of the concern, and without funding, these programs are being bootstrapped and implemented in various fashions, not conducive to effective protection.

Three, the low-cost, low-price technically acceptable environment is in direct opposition to a safe and secure critical infrastructure unless we are able to accurately define our acceptable supply chain risk tolerance at the

beginning of an acquisition cycle. While we understand the federal budget constraints and the temptation to fund program objectives with simply the lowest bid, when it comes to cyber security, it is not a good strategy. Failure to protect our critical infrastructure and educate risk owners on the threats that are brought into an organization by buying from un-validated sources will result in continued and increasingly harmful attacks.

Last, implement contractual language that works. We understand that as part of Executive Order 13636, GSA, NIST, and DOD are working with potential recommendations to update the FAR language. In addition, there are multiple industry associations working on standards for supply chain risk management. Doing as much as possible via internal policy changes and contractual language as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization is a much less expensive way to approach the problem than regulation and legislation.

In conclusion, the solution needs to be viewed as an investment in national security not just another expense. The key for industry and government is to work separately on

their internal enterprise risk tolerance levels through good business practices, including awareness training and contractual agreements. This will enable each to meet collaboratively and have informed discussions about where vulnerabilities lie and what it will take to protect our country.

Thank you for the opportunity to present our views. I look forward to answering any questions.

[The prepared statement of Ms. Bisceglie follows:]

********** INSERT 3 **********

|

Mr. {Walden.} Thank you very much for your testimony.

We will now go to Mr. Robert B. Dix, Jr., Vice President of Government Affairs and Critical Infrastructure Protection, Juniper Networks, Incorporated. Mr. Dix, pull that microphone right up and thanks for being with us today. We look forward to your testimony.

|

^STATEMENT OF ROBERT B. DIX, JR.

} Mr. {Dix.} Good afternoon, Chairman Walden, Ranking Member Eshoo, and members of the subcommittee. Thank you for inviting me to be a participant in today's hearing on the security of the communication supply chain.

As indicated, my name is Bob Dix and I serve as the Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks, a publicly held private corporation headquartered in Sunnyvale, California, in Congresswoman Eshoo's district.

I will attempt to address three aspects of this important subject of security and integrity of the communication supply chain: first, the risk created by government procurement practices utilizing unauthorized equipment providers; second, supply chain integrity initiatives by industry; and third, several recommendations where the government can help improve both government and private sector supply chain integrity.

The government views its commercial supply chain rightly

as a major element in its risk profile, but many of its risk management efforts are not coordinated and were not developed in collaboration with industry who shares legitimate concerns about supply chain security. Today, there are more than 100 different initiatives around supply chain in the government.

Also as we sit here today, the government continues to make purchases from un-trusted and unauthorized sources. The urge to save money pushes agencies to brokers and other gray market suppliers that are not part of the authorized or trusted supply chain for original equipment manufacturers. This is in also an area where much mischief takes place for both counterfeiters and those attempting to penetrate the government supply chain with malicious intent.

Interestingly, when the government purchases equipment and then identifies it as counterfeit, it often assumes the OEM has a gap in its supply chain, pointing fingers at the private sector when in many cases they need to be looking in the mirror. The government does not instead ask why it bought sensitive ICT products from and un-trusted source.

I have included in my written statement several real-life examples just that Juniper Networks has experienced

which are illustrative of this challenge, but time today does not permit me to go through each one of those. But I hope you will take a chance to look at those.

While Juniper understands the importance of improving supply chain assurance for the Federal Government, it often appears that the government itself does not understand the enormous investment that many in the private sector make to protect the integrity of their supply chain. It is in our business interest. It is a market differentiator. Juniper, like many companies, has a supply chain assurance and brand integrity program for securing our products and supply chain. We employ best practices for security from organizations including the Open Groups, Trusted Technology Forum, AGMA, and Safeco to name a few. This includes component integrity, traceability of products, anti-counterfeit measures, and much more.

As is clear from the variety and breadth of the standards, bodies, and organizations that industry relies on, many companies believe that a variety of standards and best practices contribute to supply chain integrity. But as discussed earlier, there is also compelling evidence that

there are gaps and contradictions in the government's policies and practices that contribute to supply chain risk. Here are a couple of proposals that, if addressed, could have immediate impact on securing the communication supply chain. First, the Executive Branch, at the urging of this committee, of course, should issue a directive requiring federal departments and agencies to purchase only from trusted and authorized sources, especially for mission-essential functions, unless there is some compelling reason to go outside of that channel. If there is such a compelling reason, the purchaser should be required to put a justification and authorization in writing. It is low-hanging fruit; we should do it immediately.

Second, the government should require that small business vendors be certified as authorized resellers and partners. Requirements pertaining to small business set-asides also have the secondary impact of causing procurement officers to pursue acquisitions through providers who are not part of the authorized and trusted supply chain.

We all understand the importance of small businesses to the government's industrial base and to the economy general.

It is important to recognize that bad actors also exploit our reliance on small business as a means of entry. Counterfeiters and others attempt to introduce their tainted equipment into our critical infrastructure through small business enterprises.

Third, members of this committee have been involved in attempting to pursue better information-sharing. We support CISPA and we appreciate all the good work here and hope that you will support moving that bill through the Senate.

While we are working on legislation to break down barriers to improve timely, reliable, and actionable situation awareness, there is a step we could take immediately. We continue to hear that the government has significant concerns about supply chain and the threat to national and economic security. The government has access to case studies of successful, unsuccessful, interrupted, or disrupted attempts to perpetrate network intrusions through the supply chain. We should take those lessons learned from those experiences and share the tactics, techniques, and procedures, not sources and methods that cross over into the classified space that we can learn from and better inform the

community in their own risk management decision-making.

There are a couple of others in my testimony I hope that we will get to in the questions. But on behalf of the 9,000 proud employees of Juniper Networks, I thank you again for the opportunity to participate in this important discussion. Industry looks forward to continuing the collaborative relationship with Congress and the Administration on this important issue. I welcome your questions.

[The prepared statement of Mr. Dix follows:]

********** INSERT 4 **********

|

Mr. {Walden.} Mr. Dix, thank you very much.

They have called the votes. I believe they have, right? And so we will recess at this point. So close, Mr. Rothenstein, so close. And then we will come back and start with you and get to our other two witnesses, and then Q&A. So thank you for your patience and we will be back shortly.

[Recess.]

Mr. {Latta.} [Presiding] I would like to call the subcommittee back to order. And I believe next in order of our witnesses is Mr. Rothenstein, and thanks very much for being here today. We appreciate your testimony.

|

^STATEMENT OF DAVID ROTHENSTEIN

} Mr. {Rothenstein.} My pleasure. I hope that delay only served to build anticipation of my testimony.

Vice Chairman Latta, Ranking Member Eshoo, members of the subcommittee, my name is David Rothenstein and it is my pleasure to appear before you today. I serve as senior vice president and general counsel of Ciena Corporation, a publicly held Maryland-based provider of equipment software and services that support transport and switching, aggregation management and voice, video, and data traffic on communications networks. Our products are used by communications network service providers, cable operators, governments, and enterprises across the globe.

Today, a number of current market trends, including the proliferation of smartphones, tablets, and mobile devices, are substantially increasing the demand on networks. This means that Ciena must deliver faster, more efficient, and more secure equipment to our customers to help them meet their end-user requirements.

As with most technology companies, our success is largely driven by our innovation. Our global patent portfolio is our lifeblood and it enables us to develop leading-edge solutions and get new product to market quickly. In order to support this continuous innovation and because our equipment sits in critical infrastructure networks around the world, Ciena's executive team spends a lot of time looking at the intersection of cyber security and supply chain.

Because our customers demand best-in-class product delivery lead times, quality and performance, security of supply, and product security and integrity, we have taken steps during the past few years to transform and optimize our supply chain operations. These changes have enabled us to use our supply chain as a differentiator in the market.

One example of these changes has been our focus in designing and manufacturing equipment and software that meets or exceeds the security needs of our customers. For years, our customers have generally inquired with us about the security, integrity, and assurance of their networks. With this in mind, in 2011 we performed a detailed analysis of our

supply chain that considered a range of factors.

As a result of this analysis, we decided at that time to begin a gradual exit from China of key elements of our supply chain. This was not an easy decision. China represents one of the largest and fastest-growing markets for communications equipment in the world. And the country is home to the fabrication facilities that produce many of the components that go into our products. However, based on what we knew about our products, our customers, and the business and security environment in China, we decided to make this change.

In contrast to some of our peers, we weren't as concerned about the potential adverse impact of this decision on our sales opportunities in China. Several years ago, because of the significant barriers to entry and the technology transfer requirements to do business in China, we decided not to pursue a go-to-market sales strategy in that country. We are now almost 2 years into our supply chain transformation. By the end of 2013, we will have transitioned all of the manufacture and assembly of our products and a sizable portion of our global spend on

finished and semi-finished assemblies from China to other jurisdictions, primarily Mexico and Thailand. In so doing, we have increased the velocity of our supply chain, solidified our security of supply, and insured the security and assuredness of our products. At the same time we have remained very competitive in the market from a cost standpoint.

There are some parts that we continue to source from China. We are in active discussions with our major vendors as to their plans for transitioning out of China, largely to address issues relating to counterfeit goods and intellectual property infringement. We are less concerned about the security vulnerabilities of these products even if they are primarily passive products that are neither programmable nor capable of being embedded with damaging computer code or malware.

At the same time, we have taken extensive steps to ensure the integrity of the active or programmable components in our products. We require now that these components are sourced from outside of China. We maintain rigorous and internal practices and capabilities that enable us to

identify any issues with respect to the security of our components. And by implementing strict controls over our own software developments and by ourselves performing the final testing and validation of the software loaded on to our products, we ensure the integrity of our software, which is the critical element that controls and manages our products and our customer's networks.

In conclusion, Ciena applauds the Subcommittee for taking on this issue. In our case, we proactively elected to make changes to our supply chain and not to wait for legislation, regulation, or the Administration's implementation of the recent Executive Order on cyber security. Instead, we talked to our customers, conducted a thorough business analysis and risk assessment, and made a decision that we continue to implement today. While this strategy may not necessarily work for others, it has worked effectively for us. It makes good business sense and delivers additional security for our customers and for their networks.

With that, I conclude my remarks and am pleased to take any questions.

[The prepared statement of Mr. Rothenstein follows:]

********** INSERT 5 **********

Mr. {Latta.} Well, thank you for your testimony.

And our next witness is Mr. John Lindquist, President and CEO of EWA Information and Infrastructure Technologies, Inc. Good afternoon and thanks for testifying.

|

^STATEMENT OF JOHN LINDQUIST

} Mr. {Lindquist.} Thank you, Mr. Vice Chairman, members of the committee. Thank you very much for the opportunity to testify.

As we all know, the security of our telecom systems is in fact very critical. We are aware of the myriad threats to the U.S. and the threat is real but is not limited to a single country, geographic area, or organization. Protection is made difficult because the supply chain for electronic systems and devices in general and specifically telecommunication systems is truly global. Most of the telecom system vendors have very large footprints in China and elsewhere around the globe, and many of these worldwide locations are easily and directly accessible by the various threat nations and organizations.

Furthermore, it is the nature of the system development to make use of software routines and hardware components that are generally available in the market, and it is virtually impossible to determine the pedigree of all of the hardware

and the software they goes into a telecommunications system. Our adversaries are professional, highly technically capable intelligence organizations or sophisticated criminals, neither of which would have any difficulty circumventing a trusted supplier system.

To address the security dilemma effectively, an evidence-based security process should be applied that enables an informed judgment that an adequate level of assurance has been provided that the system is free of malicious features and does not contain serious security defects; and that is without regard to origin of the system.

IIT had been selected by several telecommunications carriers as an independent evaluator to implement such a process. The process we are implementing is comprised of two major phases. The first is an in-depth security assessment of the system software, hardware, and firmware to include all patches, upgrades, and modifications as they occur.

The second phase is a delivery process that ensures that the deployed system and all patches, upgrades, and modifications are exactly the ones that were evaluated and determined to be suitable and acceptable. The key features

of the process include: willing participation of the developer and vendor; a trusted independent evaluator; direct coordination between and among the stakeholders, particularly the telecoms and the concerned government agencies and the evaluator without interference or necessarily knowledge of the vendor; correction of unintentional defects before deployment; immediate involvement of law enforcement if evidence of malicious intent is discovered; and a delivery system that ensures that the system delivered matches the evaluated system and prevents the vendor or any other un-presented party from accessing the system during or after delivery; and finally, a scheme for monitoring the system after deployment.

In our case, the vendors have been very willing to comply because compliance was a condition of the sale to the telecommunications carrier. Under those contracts, they provide us the design documentation, source code, the complete set of sample components, replication of the compilation environment for their software and firmware, advance notice of all design changes, patches, and modifications, and access to their development facilities to

provide us the understanding of their process.

We were selected because of our intimate knowledge of the threat. We have a comprehensive process with clear analytical and reporting criteria that explicitly addresses the evolving threat. We have secure facilities. We use exclusively U.S. personnel, who have been vetted through the U.S. security clearance process, and we have a staff fully qualified and equipped to perform the evaluations.

The contracts in each case specifically provide for the direct private communication between the evaluator and stakeholders. Telecommunication carriers, by contractual mandate, are the primary beneficiary of our work. A condition of acceptance is a report from us describing what we did, the faults found, the correction implemented, and any residual risk, and we are free to discuss any issues directly with the telecom and the government.

In our lab, we subject the system to a detailed analysis, both a static analysis of the software and a dynamic testing of the software and hardware. There have been thousands of defects found and mitigated, not all of these in Chinese systems; as a matter fact, many of them in

systems that currently exist in the telecommunication system.

The software is delivered directly from us to the networks. The hardware is subjected to a random sampling process, and the firmware is either delivered directly from us or the boards are re-flashed by us, all again to make sure that the delivered software is what we evaluated. Our recommendation is that some evidence-based security process like this is included in the government's approaches, including the NIST security framework and other programs across the government.

Thank you very much.

[The prepared statement of Mr. Lindquist follows:]

********** INSERT 6 **********

|

Mr. {Latta.} And thank you very much for your testimony.

Our next witness will be Dean Garfield, President and CEO, Information Technology Industry Council. And Mr. Garfield, you are recognized for 5 minutes.

|

^STATEMENT OF DEAN GARFIELD

} Mr. {Garfield.} Thank you, Mr. Chairman, since I see him walking back in, Mr. Vice Chairman, and Ranking Member Eshoo. On behalf of the world's most dynamic and innovative companies, I would like to thank you for all that this subcommittee and committee does on the issues that are most important to us and for spotlighting this issue today.

Supply chain integrity and assurance is core to who we are and what we do. It is a business imperative. And so we are encouraged to see the formation of a bipartisan working group and look forward to working with you. Your first principle, which is do no harm, is a good credo for all of the work that we do in this area.

I submitted testimony for the record and so I will focus my oral testimony today on three areas: one, providing a window into our supply chains; two is sharing some of the things we do both as individual companies but as a sector to ensure supply chain integrity; and then, third, to make some recommendations where Congress can be helpful.

I have the privilege of working for companies that are truly transforming the world. The products and mobile devices that we all walk around with every day are more powerful today than ever before. In fact, the mobile device that we all carry around has more processing power than the Apollo 11, or even more recently, the Mars rover. Those mobile devices are presented under a singular brand but they include hundreds, and in some cases, thousands of components.

To ensure that we are providing our consumers with the best products at the best prices, those components are sourced in the United States and in fact around the world as well to ensure that the services and the products that we deliver are consistently of the highest quality our global supply chains are highly integrated.

With that in mind, any change, risk mitigation, or otherwise around supply chain assurance is carefully calibrated and we would highly encourage that any advocacy or policy advance in this area be carefully calibrated as well.

The industry engages--both as individual companies and as well as a sector--in a number of steps to both manage and mitigate risk. As individual companies, they adopt and

integrate best practices on a continuous and systemic basis that includes instilling and teaching secure sourcing, instilling and teaching secure coding, instilling and teaching identification authentication among a host of steps that are taken, some of which have been talked about by the other panelists generally.

As well, those individual steps that are taken by specific companies are complemented by industry-wide, sector-wide activities both through standards activities, and so through consensus-based voluntary global standard-setting organizations, such as ISO and IEC, which has advanced a number of standards that are quite relevant in this area, including the common criteria which is focused on product assurance or through standards that are focused on not products but the processes as well that complement those products, including the Open Group Trusted Technology Forum.

It is important to note that in both instances our government and other governments have an important role to play and do engage in those consensus-based voluntary global standards-setting organizations. In fact, over 26 countries have adopted the common criteria as a part of their

government procurement practices. And so while eliminating or not mandating requirements on the private sector, which we strongly discourage, they are able to ensure that the government procurement processes benefit from the best practices of the private sector.

So where are the gaps and what can government do? We would recommend four things: one is ensuring that where you are and we are creating the proper incentives for the effective implementation of the cyber security Executive Order from the White House that was issued earlier this year. That Executive Order charges the DOD and the General Service Administration, GSA, to look at ways of integrating best practices and standards from the private sector into the government procurement practices. It would be useful to create incentives to make sure that happens appropriately.

Second is your oversight power. As Mr. Dix pointed out, there are hundreds of initiatives within the public sector focused on product assurance, gaining some order and ensuring that the private sector input is integrated into those efforts is critically important.

Third is through sourcing. Ensuring that through

government procurement, the government is sourcing from original equipment manufacturers and their authenticated suppliers is critical in order to have the kind of products assurance that we all have in mind.

And then fifth and final is making sure that we get an information-sharing bill similar to the one that has made its way through the House passed through the Senate as well.

Thank you very much.

[The prepared statement of Mr. Garfield follows:]

********** INSERT 7 **********

|

Mr. {Latta.} Thank you, Mr. Garfield, for your testimony. And, Mr. Chair, do you want to resume the chair?

Mr. {Walden.} Or I can just ask questions from here if you want to wield that big gavel there.

Mr. {Latta.} Yes. Well, with that then the vice chair will recognize the chairman of the subcommittee for his 5 minutes of questions.

Mr. {Walden.} Thank you, sir, and thanks for filling in and getting the hearing going back from the votes. I got detained, as occasionally happens on the Floor.

Mr. Garfield--first of all, thank you to all of our witnesses--but I appreciated your comments. Our networks and the threats they face are varied, as you know, and they are ever-changing, as you reference in your testimony. So how do we secure our supply chain without losing the flexibility that is critical to both how our communication networks function and then how to defend them? What do you recommend here?

Mr. {Garfield.} You put your finger on the idea of the point of drawing balance. I think building on the best

practices that are being developed in the private sector and integrating those into the government procurement efforts. There are a number of standards-based initiatives that are moving forward, specifically focused on product assurance in supply chains. And so I would strongly encourage taking advantage of those best practices and integrating them into our government procurement practice.

Mr. {Walden.} You know, I have another question here that plays on this a bit for Ms. Bisceglie and Mr. Baker and you, Mr. Garfield. Sometimes it appears the government sort of as an ad hoc process if you will when it comes to protecting the supply chain. A high-ranking official will place a call or write a little letter to a company suggesting that the company not do business with a particular vendor or a particular piece of equipment. I have actually had experience with that with a constituent. So do we need a more formalized process, which raises all kinds of questions as to who is making those decisions and all, but both as a matter of good process for equipment buyers and sellers to ensure that the measures are effective? And then how would you formalize that process?

And I don't want to hobble, you know, the fast-paced communications industry with a lot of bureaucracy, and red tape, and approval processes either. We fight that in other sectors and you certainly don't want it here. And it gets back to the hearings that we held that said, you know, first do no harm in this area. Bad guys will get ahead of us and we will be locked into old laws and rules. So is there a way to strike a balance here? And what do you recommend?

Ms. {Bisceglie.} I am happy to go first.

So I do agree we need to have--I think it is a separate slippery slope--

Mr. {Walden.} Yes.

Ms. {Bisceglie.} --as you just mentioned. And I think that there are different levels. There is a varied way to put in a formalized process and I personally believe or we personally believe there is no one-size-fits-all, but we like to talk about frameworks.

Mr. {Walden.} Right.

Ms. {Bisceglie.} And that framework consists of training and awareness, which I talked about earlier--

Mr. {Walden.} Right.

Ms. {Bisceglie.} --which is a very big thing. Folks need to understand what the risk is that we are all talking about.

Mr. {Walden.} Right.

Ms. {Bisceglie.} Additionally, I think that the thing that we have seen over the last 6 years is that organizations, both public and private, really struggle with understanding their internal risk tolerance. So how much risk can I actually accept into my organization--

Mr. {Walden.} Like anything else.

Ms. {Bisceglie.} --and that is not necessarily a single risk number of 1 to 5. It can be based on the essential function of that organization and if it has multiple functions, then it gets prioritized, if you will, into the different programs that that organization conducts as well as the systems that support that. And then underneath that, I think you do have some sort of a formal process. It gets really simple to us and that it really goes back to just really good business practices and understanding who you are buying from.

Mr. {Walden.} Right.

Ms. {Bisceglie.} But unless you can look at an organization and understand where their vulnerabilities exist and have a process to go through that, I think it is a very difficult place to go. I do think that that last-minute, that 3:00 a.m. phone call is again a very dangerous place to be.

Mr. {Walden.} Mr. Baker?

Mr. {Baker.} So I completely agree we can't just start regulating--

Mr. {Walden.} Right.

Mr. {Baker.} --the private sector and tell them how to do this. At the same time, if we rely exclusively on the government communicating informally about its concerns, you run the risk that the people who want to make these sales will just keep lowering the price and lowering the price.

Mr. {Walden.} Right, we have seen that.

Mr. {Baker.} Hard to resist. And so I would suggest that there needs to be authority for the government at a minimum to ask questions. What is in your supply chain?

Mr. {Walden.} Right.

Mr. {Baker.} You know, what products are you buying?

And to communicate where they have a strong basis, that is not acceptable. We know enough to know that that is a risky place to buy your equipment, so don't do it.

Mr. {Walden.} I will show a little ignorance here, but is there sort of a range of equipment in the system that there is some that is more important to make sure you get right than others, or is it just everything matters?

Mr. {Baker.} There is a view abroad and in the industry as well in telecommunications that the core is your most important product--

Mr. {Walden.} Right.

Mr. {Baker.} --and you cannot compromise the core and that the edge is less risky because fewer people are--

Mr. {Walden.} Do you agree with that?

Mr. {Baker.} --for any particular system. I am not sure in an internet world as the edge gets smarter and smarter that that is a distinction that holds up as well as we would like it to. But that is certainly something that we have seen in other telecommunications decision-making.

Mr. {Walden.} I know Mr. Garfield didn't get a chance to respond but I also know my time has run out so--yes, you

have got to watch this vice chair. He is mean with that gavel. Do you have anything to add to that, Mr. Garfield?

Mr. {Garfield.} I do. I think there are two specific processes--

Mr. {Walden.} Yes.

Mr. {Garfield.} --that would be useful. One is a process that is being set up through CISPA if it is passed through the Senate--

Mr. {Walden.} Right.

Mr. {Garfield.} --which is a formal process for information-sharing through the government with the protections necessary to make sure that information-sharing takes place.

The second is that the Executive Order sets up a process through the Department of Defense and General Service Administration. And so creating ways incentivizing the success of that, which Congress can still do, I think is critically important.

Mr. {Walden.} All right. Thank you very much and I yield back the deficit balance of my time.

Mr. {Latta.} The chairman is so recognized. The chair

now recognizes the gentlelady from California and the ranking member, Ms. Eshoo, for 5 minutes.

Ms. {Eshoo.} Thank you, Mr. Chairman. It is nice to see you in the chairman seat, and you are always a gentleman and I appreciate that.

Mr. {Walden.} Reserving the right to object.

Ms. {Eshoo.} Well, the same applies to you Mr. Chairman. The same applies to you. Not to worry, not to worry. Thank you to all the witnesses. Let's see, two, four, six, seven people have, you know, each in your own way have come in with something that has some refinement to it that helps to not necessarily bring closure but get us to focus on the areas that are really important for us to focus on when it comes to a public role of national security and the integrity of the supply chain. So I thank you.

I have a lot of questions. Let me start with--and Mr. Lindquist is probably not going to be surprised with the Electronic Warfare Associates, that is quite a name. Warfare Associates. How about Peace-fare Associates? But I guess that doesn't work as well. Now, I understand that your company vetted Huawei's equipment and you gave it your seal

of approval. I might add that the more I have heard witnesses speak, the more I think the government really needs to have some kind of list of essentially a good housekeeping seal of approval on it because small companies especially really need to have some help and direction so that they are not caught in some kind of seamless web.

But can you explain the service you provided Huawei and what ongoing monitoring you have conducted to maintain your certainty that their equipment is safe to use? And did Huawei pay you for this? And, I mean, if they did, you know, I don't know where that places the veracity of the report. I mean, it could be--I am not saying that is--but it could be the equivalent of what happened on Wall Street when the rating agencies were paid to give some of these, you know, too-big-to-fail great, great ratings. But they paid for them. And so, you know, in the aftermath and the rubble of the aftermath, that didn't sound so good. It didn't feel so good and really wreaked a lot of havoc. Did Huawei pay you for the report? And then the rest of my question.

Mr. {Lindquist.} First of all no, Huawei did not pay for--

Ms. {Eshoo.} You did this voluntarily for them?

Mr. {Lindquist.} No, the telecommunications carrier paid for it.

Ms. {Eshoo.} And who was that?

Mr. {Lindquist.} I am not at liberty to disclose that because we have an NDA with them. If I get their permission, I can tell you easily who it is.

Ms. {Eshoo.} I see. That is interesting.

Mr. {Lindquist.} But it is one of the major--

Ms. {Eshoo.} Um-hum.

Mr. {Lindquist.} --telecommunications companies. And--

Ms. {Eshoo.} An American telecommunications company?

Mr. {Lindquist.} American telecommunications company.

Ms. {Eshoo.} Um-hum.

Mr. {Lindquist.} Secondly--

Ms. {Eshoo.} Can you tell us this? Is it an American telecommunications company that buys equipment from Huawei?

Mr. {Lindquist.} They are in the process of doing that. The equipment, in answer the second part of your question--

Ms. {Eshoo.} Um-hum.

Mr. {Lindquist.} --we are in the process of evaluating

their system. The evaluation is by no means complete and we are only evaluating the radio area network portion of it. There are numerous reports. We do not give a seal of approval. What we do is take the known threats and we have very good access through some of our work within the government to the agreed list of cyber threats and what--

Ms. {Eshoo.} Well, do you get your information from the intelligence community or Homeland Security?

Mr. {Lindquist.} The intelligence community.

Ms. {Eshoo.} This is so interesting. So you do a report that vets Huawei, who wants to more than get a toehold which have for years and it is very public and deeply concerned about. You are paid by an American major telecommunications corporation that is looking to buy Huawei's equipment and you work with the intelligence community to see with the shortfalls are and vet it and say that the equipment is terrific for the American market. Have I gotten that straight?

Mr. {Lindquist.} Well, except that we don't say it is terrific or--

Ms. {Eshoo.} What did you say?

Mr. {Lindquist.} What we do say is what we looked at and what we found, and if we found things, what corrections were made.

Ms. {Eshoo.} I see. See, my issue on all of this is not whether their equipment is good or not. That is not the point. The point is is that our infrastructure is so precious to this country and it is a part of our national security. There is no question about it. And so does it pose a threat? If so, how? You know, maybe they make some of the best equipment in the world but that is not my point. That is not my point at all. So it is interesting what you just said.

And let me ask all the witnesses and you can just give me a yes or no. Should there be transparency requirements, including divestments in state ownership placed on companies seeking to sell telecommunications infrastructure equipment to U.S. network providers? And should this be a U.S. or an international standard? Maybe it is hard to answer yes or no but--

Mr. {Goldstein.} I don't think I can give you a yes or no, ma'am. I think, particularly from our perspective, we

didn't look at those issues specifically. It is something we are happy to talk to staff about.

Ms. {Eshoo.} I want to thank you for your work, too.

Mr. {Goldstein.} Thank you.

Ms. {Eshoo.} Um-hum.

Mr. {Baker.} I do think that as we adjust to a world where there really are no telecommunications integrators in the United States, we need authority to ask for quite a bit of information from the people--

Ms. {Eshoo.} Um-hum.

Mr. {Baker.} --who are supplying that technology.

Ms. {Eshoo.} Thank you.

Ms. {Bisceglie.} I absolutely agree. I think transparency is the key and you liken it to--if you look at what is happening with the pharmaceutical agencies within your actual State--

Ms. {Eshoo.} Um-hum.

Ms. {Bisceglie.} --that the pharmaceutical law, the E-Pedigree law of 2015 that has everybody looking at transparency, I think there are lessons to be learned there.

Ms. {Eshoo.} Um-hum. Okay.

Mr. {Dix.} Transparency is important and having a standard that provides certification and accreditation a whitelisting type of opportunity would be very valuable to this process.

Ms. {Eshoo.} Thank you.

Mr. {Rothenstein.} Yes, we would agree. We would support some level of transparency and I think, frankly, Ranking Member Eshoo, you hit the nail on the head. It is less about the U.S. Government and about the large service providers who have a lot of know-how--

Ms. {Eshoo.} Um-hum.

Mr. {Rothenstein.} --the resources, and are knowing smart buyers of telecom equipment understand the risks. It is more about other critical infrastructure owners and operators, the alternative operators, the enterprises who may not have the same level of understanding and resources where the transparency really is going to be important.

Ms. {Eshoo.} It is helpful. Um-hum.

Mr. {Lindquist.} As I said earlier, I would reiterate transparency is important. That is why in the process that we implement we are looking at all the design documentation

behind the various systems to ensure that there is no inexplicable capability or functionality within the system.

Mr. {Garfield.} I work in the tech sector so, of course, we believe in transparency. I don't have an answer as it relates specifically to this issue.

Ms. {Eshoo.} Thank you. Thank you, Mr. Chairman, for your patience. Thank you to all the witnesses.

Mr. {Latta.} Thank you very much. The gentlelady yields back and the chair recognizes himself now for 5 minutes.

And if I could start with Mr. Goldstein, I found it kind of interesting in your testimony on page 5 where you state that other countries such as Australia, India, and the United Kingdom are similarly concerned about emerging threats to the commercial communication networks posed by the global supply chain, have taken actions to improve their ability to address this security challenge. What exactly have those three countries done?

Mr. {Goldstein.} There are three countries--there are many others--

Mr. {Latta.} Right.

Mr. {Goldstein.} --that we don't get into here. But Australia has developed a regulatory reform proposal that they expect to put in place shortly that would allow the government to have more authority to examine what companies are doing, what they are buying, how they document their purchases, take a look to make sure that those companies are competent in putting networks together, and if the government does not feel that they are doing it in a way that can be secured, that they can ask them to do more. They can require them to do more than they are doing and it has enforcement powers and potential to find those companies that don't do it. That is a proposal that is likely to pass soon.

India has a very similar reform program in place. Where it differs is that they have also proposed requiring--certainly encouraging and in many cases requiring much of their equipment to be made and tested in the country and could not be obtained elsewhere. That particular part of the proposal has been put on hold because the United States and some other countries have objected because of potential barriers to trade.

And the United Kingdom has put in place a very similar

program to the one that Australia is now contemplating to have a greater regulatory review over the practices and actions of companies putting networks in place, which also has authorities for them to go in and look very specifically at what they have done and how they are going to get assurance that those are secure networks, as well as to be able to enforce actions that they feel would be necessary if those companies did not do as much as they probably should be doing.

Mr. {Latta.} Thank you.

Mr. Rothenstein, if I could turn to your written testimony. I thought it kind of interesting where you had also had mentioned that in 2011 your company had made a conscious decision to gradually exit key elements of your supply chain from China. And at the time over 1/5 of your global chain at that time originated in China. You go on to state that, you know, you are looking at other jurisdictions that you are moving into now in Mexico and Thailand. I am just curious. How is that working out, and what have you found so far with that transition?

Mr. {Rothenstein.} So in terms of the actual specific--

so you are right. About 20 percent at the time of our manufacturing assembly of our supply chain originated in China and it is now down to less than 1 percent. And in terms of the procurement to finished to semi-finished assemblies, that was about 65 to 70 percent of the supply chain 2 years ago. That is now below 50 percent. The part that we attacked, as I mentioned in my testimony, was that relating to active or programmable components.

In terms of how it has gone, it has gone very, very well. We have partnered effectively with two of our long-standing contract manufacturers in Mexico and one in Thailand. We have improved the velocity of our supply chain. It is a lot quicker to get equipment to our key North American market when you are driving it by truck over the border as opposed to the slow boat from China. We have been able to essentially achieve cost parity in terms of labor rates and landed cost rates largely because those contract manufacturers had existing facilities in those locations.

And as a result of that, we have been able to, in addition to velocity maintaining cost parity, we have gotten tremendous positive feedback from our customer base in terms

of that supply chain strategy. They viewed very positively our thought process, our decision, and they have given us direct feedback that they view with a greater level of comfort, security, and assuredness of the risk profile of our equipment to their networks.

Mr. {Latta.} And in the balance of my last 27 seconds if I could turn to Mr. Lindquist, what are the different challenges in protecting the software and hardware supply chain and is one more vulnerable than the other?

Mr. {Lindquist.} What are the different challenges in protecting it?

Mr. {Latta.} In protecting the software and hardware supply chains and is one more vulnerable than the other?

Mr. {Lindquist.} I think the current state of affairs--and it is referring to the second question first--I think the software is more vulnerable. I think there are more people who have perfected techniques for exploiting software than in the hardware. It is also easier to do at any stage in the process.

And what we are endeavoring to do is to separate the vendor from the products so that once the system has been

determined to be secure enough, and there is always some residual risk, that the vendor no longer has access to that system to introduce any new malicious capability into the system.

Mr. {Latta.} Well, thank you very much. And my time has expired.

And the chair would now recognize the gentleman from Illinois, Mr. Shimkus, for 5 minutes.

Mr. {Shimkus.} Thank you, Mr. Chairman. Thank you all for being here. It is a great committee with high-tech things. I always joke that for my colleagues who don't have teenagers, then the government ought to issue them one because that helps you figure out how this stuff works.

The hearing this morning was on cyber security, too, with the electric grid and the like. So we had a little debate about the cloud, which I understand are server farms and that brings some, especially when the government is contracting. And my son and I are together on concerns about the cloud. You know, everybody thinks it is--but, you know, there are some issues there, cyber security and especially if the government is being involved and really contracting that

space.

We differ on CISPA and we have had numerous debates. So the last time we cast the vote I was home that next morning and he comes into the room and he is all grouchy and he is reading all of his internet stuff. And he says I don't have to ask how you voted on CISPA, Dad. I know how you voted--which I supported. And he was none too pleased.

But my debate or discussion with him is information-sharing, really on the code system so you could have firewalls. And if our intel communities or you guys know something is crazy going on out there, you can build a firewall. At least you have an idea of what you might expect.

So, Mr. Garfield, I don't know if it was in your statement but in question-and-answers you also talked about information-sharing. And were you referring to that in the supply chain debate that we are having here, that there ought to be information-sharing like we would have in firewall protection a la like CISPA?

Mr. {Garfield.} Yes is the simple answer. Information-sharing and passing of risk mitigation information is

critical to protecting our cyber security generally but also for risk assurance in the context of supply chains as well. And so, I think, moving CISPA and the information components of that was critically important in getting and through the Senate is critically important--

Mr. {Shimkus.} But the CISPA bill that we are passing--you know, correct me if I am wrong--I thought it was just on code. Was it also on the supply chain? It could be?

Mr. {Garfield.} Yes, it is around sharing actionable intelligence--

Mr. {Shimkus.} Here on--

Mr. {Garfield.} --on threats and mitigating threats.

Mr. {Shimkus.} I got another good point for my son then, right? I got another good point.

Mr. {Garfield.} You can give him my phone number.

Mr. {Shimkus.} Good. Great. Good, I always need a little help.

And Ms. Bisceglie, SCRM, now, I have got a new acronym. Just what we need, another acronym here in Washington, SCRM, which was supply chain--

Ms. {Bisceglie.} Risk management.

Mr. {Shimkus.} --risk management, which is all tied into this. I want to follow up with you on this cost pressure issue that you raised and how do you think we can really address it? I mean if you really want to make sure that your equipment is secure, you are willing to pay for it, but if you are in a competitive, very fast-moving technological field and you want to get market entry and you want to have a low-cost provider, there is risk involved in that, correct?

Ms. {Bisceglie.} There is, and actually, that is when the chairman asked his question earlier when we talked about putting a framework in place, something that is repeatable and scalable. I personally think that is the key, an effort to keep the acquisition costs down, because I totally understand the need to get procurements done faster, technology to the street faster, and into users' hands faster. But unless we have ways of understanding what our organizational risk tolerance is so that we know what protectionisms we already have in place, it is going to be very difficult to really take risky endeavors like you are mentioning.

Mr. {Shimkus.} And I was also caught by the whole debate. There was a pharmaceutical reference which we are involved with and the Track-and-Trace legislation--

Ms. {Bisceglie.} Um-hum.

Mr. {Shimkus.} --in maybe some States. Just for the record, when some States move to a very controlled system, they have to then postpone the enactment date because they can't do it--

Ms. {Bisceglie.} Um-hum.

Mr. {Shimkus.} --in that time, which then would affect the market in delivery of goods and services. So the question is--because what the chairman said to begin with was, first do no harm.

Ms. {Bisceglie.} Um-hum.

Mr. {Shimkus.} So does the Executive Order and its process have the opportunity to do harm in this process? Does anyone want to comment? Is there a concern that the Executive Order and this rollout and their involvement has an opportunity to do harm? Mr. Garfield?

Mr. {Garfield.} Yes, there is always risk, right? We are in the business of risk mitigation but overall our view

is that the Executive Order actually creates a framework that advances the ball in a very positive way. The fundamental question for us is how can Congress complement that and that is what I tried to articulate in talking about the things that Congress can do to ensure it continues to move in a positive direction.

Mr. {Shimkus.} Mr. Chairman, my time is up but I think there are a couple more that want to comment.

Mr. {Dix.} I would just add many of us want to approach the answer to that question with an open mind, but we are taking a wait-and-see approach because it is not at the endgame yet and there are opportunities along the way for this not to be as good as it might be.

Mr. {Shimkus.} Always good to trust but verify.

Mr. {Dix.} Yes, sir.

Mr. {Shimkus.} If no one else wants to jump in, I yield back my time. Thank you, Mr. Chairman.

Mr. {Walden.} Thank you. Now, I will turn to the gentleman from Colorado, Mr. Gardner, for 5 minutes.

Mr. {Gardner.} Thank you, Mr. Chairman, and thank you to the witnesses for joining us today.

And, Mr. Baker, I will direct this question to you. Questions raised by foreign-directed cyber attacks on U.S. institutions suggest that the United States Government must give careful consideration to how the national security interests are controlled, monitored, and regulated. How concerned should we be by the prospect that any critical infrastructure provider that serves the core of our national security interests could come under foreign control and therefore outside the supervision of the U.S. Government?

Mr. {Baker.} We have to be concerned about that. It is not likely that we will be able to stop globalization of this industry so the idea that we can simply say no I think is not realistic. But we have to then put in place transparency and regulatory authority that makes sure that those companies do not serve other nations' interests when they supply us with that equipment.

Mr. {Gardner.} And in keeping those kinds of concerns in mind--and we have seen in the past the mergers of U.S. companies with foreign companies--what are some of the national security implications of such a purchase then?

Mr. {Baker.} So I did this a lot when I was at DHS and

indeed when I was at NSA. In the telecommunications industry we have a well-developed set of rules in which we negotiate a mitigation agreement with the buyer if the buyer is a foreign buyer, which gives us some control. It is not perfect by any means, and I am often unenthusiastic about the results. But it is the tool that we have.

In the context of companies selling products to the United States, we have none of those controls unless they actually buy a U.S. company so that any company can sell products into our critical infrastructure without any regulation or transparency. It is only when they try to buy a U.S. company that we have any authority at all.

Mr. {Gardner.} Reports of stories of foreign-directed cyber attacks against U.S. institutions provoke difficult questions about the control reaching oversight of the United States national security interests. Do you agree that the idea of surrendering control of a critical infrastructure provider like Sprint to a foreign entity Softbank beyond full U.S. oversight deserves very careful consideration and should not be hurried?

Mr. {Baker.} It certainly deserves careful

consideration. I would point out, as I answered to the last question, for many the security agencies there will be a temptation to say the only way we will be able to tell Sprint the products they can buy, what they can have in their infrastructure, is if we enter into a negotiated agreement. That is a negotiated agreement with a foreign buyer. They have no authority at all in the other context so it is an odd set, currently, of incentives for the U.S. Government in which they might actually have more regulatory authority if they let the transaction go through.

Mr. {Gardner.} You mentioned in your testimony a little bit about CFIUS, whether it is adequate or not. That is relied on by Congress, by the FCC. Where are the pitfalls? What are the problems?

Mr. {Baker.} The problem is that if you want to introduce products that are not reliable into the U.S. market, you can just walk in and start taking orders. Even if it is going right into the core of the telecommunications industry, there is no authority anywhere in the U.S. Government to say no to that today. Only if unreliable buyer or seller actually tries to acquire a U.S. company is there

any authority at all.

Team Telecom at the FCC has some authority over foreign carriers but not over foreign suppliers of equipment. CFIUS gives authority only over buyers of U.S. companies. So there is a real regulatory gap there with respect to some of this equipment that we have not yet found a solution for.

Mr. {Garfield.} May I weigh in on this?

Mr. {Gardner.} Please.

Mr. {Garfield.} I think we have to be exceptionally careful about developing prophylactic rules around private sector agreements as it relates to supply chain assurances. India was used as a reference earlier in talking about an example of countries moving in a particular direction. There are a whole host of companies that I represent in the technology sector that are being foreclosed from the Indian market because of those types of rules. And so I just think that those types of rules have to be carefully calibrated and, from my perspective, discouraged.

Mr. {Gardner.} Thank you. I yield back my time.

Mr. {Walden.} I thank the gentleman. I thank all of our witnesses and committee members for their participation

today, really a superb panel of witnesses. Your information that you shared has been very, very valuable. Your written testimony is helpful to us and to our staffs as we wrestle with this issue going forward in protecting the country and trying also not to stifle innovation and technology being developed in America. So we have got to get this right. And your depths of experience and your willingness to come here and share that with us is a great benefit to the American people. And so we thank you for your participation; we thank you for your assistance.

And the record will remain open for additional questions, I am sure. And we hope that you will accept our invitation to work with us even further as we go forward. We want to get this right. So thank you very much. With that, the Subcommittee stands adjourned.

[Whereupon, at 4:12 p.m., the Subcommittee was adjourned.]