PUBLIC-PRIVATE INITIATIVES TO SECURE THE SUPPLY CHAIN

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

OCTOBER 16, 2019

Serial No. 116–41

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
40–457 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Cedric L. Richmond, Louisiana
Donald M. Payne, Jr., New Jersey
Kathleen M. Rice, New York
J. Luis Correa, California
Xochitl Torres Small, New Mexico
Max Rose, New York
Lauren Underwood, Illinois
Elissa Slotkin, Michigan
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Dina Titus, Nevada
Bonnie Watson Coleman, New Jersey
Nanette Diaz Barragán, California
Val Butler Demings, Florida

Mike Rogers, Alabama
Peter T. King, New York
Michael T. McCaul, Texas
John Katko, New York
Mark Walker, North Carolina
Clay Higgins, Louisiana
Debbie Lesko, Arizona
Mark Green, Tennessee
Van Taylor, Texas
John Joyce, Pennsylvania
Dan Crenshaw, Texas
Michael Guest, Mississippi
Dan Bishop, North Carolina

Hope Goins, *Staff Director*
Chris Vieson, *Minority Staff Director*

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

PUBLIC-PRIVATE INITIATIVES TO SECURE THE SUPPLY CHAIN

Wednesday, October 16, 2019

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 10:03 a.m. in Room 310, Cannon House Office Building, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Langevin, Correa, Underwood, Slotkin, Barragán, Demings; Rogers, Katko, Lesko, Taylor, Joyce, and Crenshaw.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

The committee is meeting today to receive testimony on public-private initiatives to secure the supply chain.

Without objection, the Chair is authorized to declare the committee in recess at any point.

Good morning. I want to thank the witnesses for being here today to discuss an issue critical to our National security: The information and communications technology supply chain.

Concerns about the original components embedded in our ICT devices such as cell phones, computers, and satellites are nothing new. We have known that such technology produced by our adversaries could be exploited for espionage or cyber attacks for a long time.

In 2012 the Senate Intelligence Committee released a damning report about the threats products from Chinese telecom companies ZTE and Huawei pose to U.S. National security interests. Government officials had acknowledged concerns about the use of Kaspersky anti-virus software for years before the Department of Homeland Security finally directed all Federal agencies to remove it from their systems in 2018.

But the rapid evolution of the global economy, coupled with our increasing reliance on technology and anticipation of a new 5G cell network, has resulted in much-needed momentum to address risk in our ICT supply chain.

Developing sound supply chain risk management policy is not just a whole-of-Government effort, and it is all-hands-on-deck effort. That is why I am pleased that CISA is spearheading a critical public-private initiative to provide recommendations for assessing and managing ICT supply chain risk.

Last month the task force issued its interim report, and I congratulate the task force co-chairs on that accomplishment. The interim report identified practices and policies related to supply chain threat information sharing, white-listing, and threat evaluation, along with associated challenges. I am eager to discuss those issues today.

More importantly, I want to know how Congress can help advance the recommendations of the task force. I am also interested to learn how the work of the task force is being leveraged by the Federal Acquisition Security Council, and by the Department of Commerce as it executes its authorities under Executive Order 13873, which was seemingly targeted at China.

On that note, I want to commend the administration for finally taking a concrete step to mitigate the threat Chinese firms pose to the supply chain. The Chinese Government has spent years strategically investing in and promoting Chinese information and communications technology to advance its national agenda at our expense.

So I was disturbed last year when the President directed the Department of Commerce to lift the ban on ZTE buying U.S. parts, apparently to advance his trade agenda. Our National security is not a bargaining chip, and the President cannot negotiate away policies that will secure our supply chain. Toward that end I will continue to monitor the implementation of the Executive Order closely.

I look forward to the hearing and your testimony today.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

OCTOBER 16, 2019

Concerns about the origin components embedded in our ICT devices, such as cell phones, computers, and satellites, are nothing new. We have known that such technology produced by our adversaries could be exploited for espionage or cyber attacks for a long time. In 2012, the Senate Intelligence Committee released a damning report about the threats products from Chinese telecom companies ZTE and Huawei pose to U.S. National security interests. Government officials had acknowledged concerns about the use of Kaspersky anti-virus software for years before the Department of Homeland Security finally directed all Federal agencies to remove it from their systems in 2018. But the rapid evolution of the global economy coupled with our increasing reliance on technology and anticipation of a new 5G cell network has resulted in much-needed momentum to address risks to our ICT supply chain.

Developing sound supply chain risk management policy is not just a whole-of-Government effort—it's an all-hands-on-deck effort. That is why I am pleased that CISA is spearheading a critical public-private initiative to provide recommendations for assessing and managing ICT supply chain risks. Last month, the task force issued its Interim Report, and I congratulate the task force co-chairs on that accomplishment. The Interim Report identified practices and policies related to supply chain threat information sharing, whitelisting, and threat evaluation, along with associated challenges. I am eager to discuss those issues today. More importantly, I want to know how Congress can help advance the recommendations of the task force.

I am also interested to learn about how the work of the task force is being leveraged by the Federal Acquisition Security Council and by the Department of Commerce as it executes its authorities under Executive Order 13873, which was seemingly targeted at China. On that note, I want to commend the administration finally taking a concrete step to mitigate the threat Chinese firms pose to the supply chain. The Chinese government has spent years strategically investing in and promoting Chinese information and communications technology to advance its National agenda—at our expense. So I was disturbed last year when the President directed the Department of Commerce to lift the ban on ZTE buying U.S. parts, apparently to advance his trade agenda.

Our National security is not a bargaining chip, and the President cannot negotiate away policies that will secure our supply chain. Toward that end, I will continue to monitor the implementation of the Executive Order closely.

Chairman THOMPSON. The Chair now recognizes the Ranking Member of the full committee, the gentleman from Alabama, Mr. Rogers, for an opening statement.

Mr. ROGERS. Thank you, Mr. Chairman.

The U.S. economy is the envy of many around the world. Our innovative spirit and technological advances have led the world for more than 150 years. For almost the same period of time, our adversaries and criminal actors around the world have attempted to steal our innovations, to enrich themselves, and undermine our way of life. They have sought every advantage to copy and extract information and intelligence about the U.S. Government, our industry, and our citizens.

The latest front in this battle is the supply chain. Our adversaries are actively exploiting vulnerabilities in our supply chain to undermine our economy and our National security. These vulnerabilities have led to intellectual property theft, data breaches, and the leaks of Classified information. In recent years, that threat has intensified as our intelligence community has been able to link certain foreign companies with strong presence in our commercial and Government supply chain to foreign intelligence agencies.

Protecting our supply chain from companies like Kaspersky Labs and Huawei that serve as intelligence fronts for Russia and China is a complex challenge. We need to do a better job of identifying and prohibiting companies like these from infiltrating our supply chain.

But even if we are able to fully secure technologies in the United States, our citizens' companies still operate throughout the globe in countries that make different choices about their supply chains. For this reason we must have a holistic approach to securing the supply chain.

I applaud the Information and Communications Technology Supply Chain Risk Management Task Force for taking such an approach. The ITC Task Force is a great example of public and private collaboration working to identify and understand the problem. Together they are working systematically to equip the Government and industry to mitigate risks. While the task force is focused on information and communications technology ecosystem, I hope their work will inform other areas of the supply chain risk.

Our transportation systems, manufacturing, health care, and other critical industries are increasing vulnerable—increasingly vulnerable to supply chain disruption. I think the Department of Homeland Security has the expertise to assist these industries, our Government, and other Government agencies if we fight this emerging threat. I expect the Department to continue to play a central role in the effort.

I appreciate our witnesses for being here today to discuss this important work. I look forward their recommendations on how to best equip the Government, industry, and our citizens to secure our supply chain.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF RANKING MEMBER MIKE ROGERS

OCTOBER 16, 2019

The U.S. economy is the envy of many around the world. Our innovative spirit and technological advances have led the world for more than 150 years.

And, for almost the same period of time, our global adversaries and criminal actors have attempted to steal our innovations to enrich themselves and undermine our way of life.

They have sought every advantage to copy and extract information and intelligence about the U.S. Government, our industry, and our citizens.

The latest front in this battle is the supply chain. Our adversaries are actively exploiting vulnerabilities in our supply chain to undermine our economy and our National security.

These vulnerabilities have led to intellectual property theft, data breaches, and leaks of Classified information.

In recent years, the threat has intensified as our intelligence community has been able to link certain foreign companies with a strong presence in our commercial and Government supply chain to foreign intelligence agencies.

Protecting our supply chain from companies like Kaspersky Labs and Huawei that serve as intelligence fronts for Russia and China is a complex challenge.

We need to do a better job of identifying and prohibiting companies like these from infiltrating our supply chain.

But even if we were able to fully secure technologies in the United States, our citizens and companies still operate throughout the globe, in countries that make different choices about their supply chains.

For this reason, we must have a holistic approach to securing the supply chain. I applaud the Information and Communications Technology Supply Chain Risk Management Task Force for taking such an approach.

The ICT Task Force is a great example of the public and private collaboration, working to identify and understand the problem and work systematically to equip the Government and industry to mitigate risks.

While the task force is focused on the information and communications technology ecosystem, I hope their work will inform other areas of supply chain risk. Our transportation systems, manufacturing, health care, and other critical industries are increasing vulnerable to supply chain disruption.

I think the Department of Homeland Security has the expertise to assist these industries and other Government agencies as we fight this emerging threat. I expect the Department to continue to play a central role in this effort.

I appreciate our witnesses for being here today to discuss their important work. I look forward to their recommendations on how best to equip Government, industry, and our citizens to secure our supply chain.

Mr. ROGERS. With that, Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much. Other Members of the committee are reminded that, under the committee rules, opening statements may be submitted for the record.

I welcome our panel of witnesses today.

Our first witness, Mr. Bob Kolasky, leads the Cybersecurity and Infrastructure Security Agency's National Risk Management Center at the Department of Homeland Security. As assistant director he oversees the Center's efforts to facilitate a strategic, cross-sector risk management approach to cyber and physical threats to critical infrastructure.

Mr. Robert Mayer is senior vice president of cybersecurity at USTelecom. He currently serves as co-lead of DHS' Information and Communications Technology Supply Chain Risk Management Task Force. That is a tremendous title.

We welcome you here, Mr. Mayer.

Mr. John Miller is vice president of policy, and senior policy counsel at the IT Industry Council. He serves as co-lead of DHS' ICT Supply Chain Risk Management Task Force, representing information technology companies and the task force's work. Without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Kolasky.

STATEMENT OF ROBERT KOLASKY, ASSISTANT DIRECTOR, NATIONAL RISK MANAGEMENT CENTER, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, DEPARTMENT OF HOMELAND SECURITY

Mr. KOLASKY. Thank you, Chairman Thompson. Thank you, Ranking Member Rogers. Thank you, Members of the committee, for today's opportunity to testify regarding CISA's on-going efforts to secure the supply chain of information and communications technology. I will today a little bit about the work of the ICT task force, but as well as other efforts that we are taking across this in DHS and the Federal Government.

As CISA's assistant director in charge of running the National Risk Management Center, I have the privilege of leading an organization with a vitally important mission. The National Risk Management Center is a planning, analysis, and collaboration center, working with public and private partners to better understand and manage the most strategic risks to the Nation's critical infrastructure.

We are doing this based principally through two main buckets of activity: No. 1, building lasting analytic capability for critical infrastructure risk; and No. 2, leading and catalyzing initiative planning and execution for managing risk to priority areas identified.

Since our inception at the end of last year we have steadily matured a capacity in both of these categories, particularly around risks to the Nation's supply chains.

This hearing is timely and important for the reasons that you laid out in your opening statement, as well. Many and most—or most discussions around cybersecurity threats include some risk calculation around supply chain, third-party, or vendor assurance risk. In line with that reality, CISA has identified supply chain risk management to include 5G security resilience as a Top-5 priority for our agency in our recently-released strategic intent document, which we released at the end of August of this year.

Supply chain risk can broadly be understood as efforts by our adversaries to exploit ICT technologies and their related supply chains for purposes of espionage, sabotage, and foreign interference activities. Vulnerabilities in supply chains, either developed intentionally for malicious intent, or unintentionally through poor security practices, can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system and network failure.

Increasingly, our adversaries are looking at these vulnerabilities as a principal attack vector, and we are increasingly concerned with aggressive actions by potential foreign adversaries to include Russia, China, North Korea, and Iran.

In the critical infrastructure community we frequently talk about the merits of deeper integration partnership across the Government and with private-sector partners to address high-priority risks. Supply chain risks are such a priority, and a risk that can't be addressed without public-private partnerships. I think it is significant that I sit here with Robert and John, testifying on the same panel, because I can say confidently that the partnership between the ICT stakeholder community and CISA is stronger than ever before.

Through our work at the ICT Supply Chain Risk Management Task Force, we have taken on a lot of the issues that are most important in understanding and dealing with the risks to the Nation's supply chain. As a high-level snapshot of where things stand, the task force has successfully brought together 40 industry stakeholders across the IT and com sector, launched 4 working groups of key areas of priority risk management focus in supply chain, and published an interim report detailing key recommendations and next steps. John and Robert are going to talk a little bit more about those recommendations in their testimony.

This is an important reinforcement of bringing the right people to the table. We can't do this work without the partnership with industry and across the interagency. The task force can be a model for a range of public-private partnership activities in this space and beyond.

Outside of the work of the task force CISA is engaged in a wide range of supply chain risk management activity, and will be for the foreseeable future. As mentioned, our work in support of the President's Executive Order 13873—in particular, DHS has focused on assessing and identifying entities, hardware, software, and services that present vulnerabilities in the United States that pose the greatest potential consequence for our National security.

As part of us doing the assessment, we relied on the work of the task force, and particularly our engagement and partnership with the firms who participate in the task force to help us better understand the critical nodes of our supply chain.

CISA will soon release the methodology we used in the assessment and support of this Executive Order, and that we have provided—we have provided the whole report to the Secretary of Commerce. The methodology we used included a deconstruction of the ICT supply chain into 61 elements, the hardware, software, and service building blocks that collectively make up the ICT ecosystem.

Among the elements that CISA designated as critical for focusing supply chain risk reduction efforts were home subscriber services, mobile switching centers, and sensitive system software, to include software-defined networking. Untrustworthy equipment in those supply chains could create an unacceptable amount of risk to the National security of the United States.

Many of these critical elements will be part of the fifth generation communications network, 5G. 5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years. Coupled with the growth of cloud computing, automation, and the future of artificial intelligence, 5G demands focused attention today to secure tomorrow.

CISA and our interagency partners, recognizing the importance of 5G security and resilience, recognize the importance of 5G security and resilience in efforts. To demonstrate the reasons for that, the Financial Risk Management Center worked with the IT and communications sector to produce a publicly-available 5G risk characterization as a baseline-level-setting document to understand the complexities, risks, and opportunities presented by 5G deployment.

If untrusted components and suppliers take a foothold in our 5G infrastructure, there is potential for not just data integrity and privacy loss, but also public health and safety concerns due to many of the envisioned use cases of 5G connectivity. We must take these risks seriously, and I can tell you with confidence that CISA, with our partners, is doing that, both here in the United States and working with our allies globally.

In summary, a holistic understanding of critical infrastructure risk must take into account the supply chain risks stemming from an interconnected society that relies heavily on ICT technology. As CISA continues to mature its engagement in supply chain risk management and 5G security and resilience lines of efforts, the agency is also working on developing a lasting technological architecture and framework to allow for better structured supply chain risk analysis. We believe investing in this capability will be critical to fully achieving CISA's critical infrastructure mission in the years to come.

Thank you again for holding this hearing, and I look forward to your questions.

[The prepared statement of Mr. Kolasky follows:]

PREPARED STATEMENT OF ROBERT KOLASKY

OCTOBER 16, 2019

Chairman Thompson, Ranking Member Rogers, and Members of the committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) on-going efforts to secure the supply chain of information and communications technology (ICT). Thanks to Congress's leadership and passage of the Cybersecurity and Infrastructure Security Agency Act of 2018 (Pub. L. 115–278) nearly 1 year ago today. CISA is now even better poised to achieve our important critical infrastructure security and resilience mission.

UNDERSTANDING THE THREAT

Cyber threats remain one of the most significant strategic risks for the United States, threatening our National security, economic prosperity, and public health and safety. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of their attacks. In a 2018 report, *Foreign Economic Espionage in Cyberspace,* the United States' National Counterintelligence and Security Center stated, "We anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyber space." Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our National security secrets, and threaten our democratic institutions.

During his annual World-wide Threat Assessment testimony before Congress this January, the director of national intelligence stated, "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the U.S. Government, corporations, and allies." The director further stated, "We are also concerned about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies." This assessment is consistent with the fact that Chinese laws on National security and cybersecurity provide the Chinese government with a legal basis to compel technology companies operating in China to cooperate with Chinese security services.

Increasingly, many or most discussion around cybersecurity threats include some risk calculation around supply chain, third party, or vendor assurance risk. In fact, a 2018 Symantec report detailed that the number of observed supply chain attacks was 78 percent higher in 2018 than it was in 2017, as malicious actors sought to exploit vulnerabilities in third-party software, hardware, and services.

Supply Chain Risk can broadly be understood as efforts by our adversaries to exploit ICT technologies and their related supply chains for purposes of espionage, sabotage, and foreign interference activity. Vulnerabilities in supply chains—either developed intentionally for malicious intent or unintentionally through poor security practices—can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system and network failure. Increasingly, our adversaries are looking at these vulnerabilities as a principal attack vector, and we are increasingly concerned with aggressive actions, by potential foreign adversaries to include Russia, China, North Korea, and Iran.

ROLES AND RESPONSIBILITIES

CISA, our Government partners, and the private sector are all engaging in a more strategic and unified approach toward improving our Nation's overall defensive posture against malicious cyber activity. In May 2018, the Department published the DHS Cybersecurity Strategy, outlining a strategic framework to execute our cybersecurity responsibilities during the next 5 years. The National Cyber Strategy, released in September 2018, reiterates the criticality of collaboration and strengthens the Government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the National Cyber Strategy and DHS Cybersecurity Strategy guide CISA's efforts.

CISA works across Government and critical infrastructure industry partnerships to lead the National effort to safeguard and secure cyber space. We share timely and actionable Classified and Unclassified information as well as provide training and technical assistance. Our work enhances cyber threat information sharing between and among governments and businesses across the globe to stop cyber incidents before they occur and quickly recover when they do. By bringing together the intelligence community, law enforcement, the Department of Defense, Sector-Specific Agencies, all levels of government, the private sector, international partners, and the public, we are enabling collective defense against cybersecurity risks, improving our incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

In addition to our cross-sector leadership role, CISA is the Sector-Specific Agency for numerous sectors, notably the Information Technology and Communications Sectors. In this role, we work with a range of stakeholders to address both short-term and longer-term challenges regarding risks to telecommunications networks, including supply chain risk management and 5G security. These stakeholders include the Department of Justice, Department of Commerce, Department of Defense, Federal Communications Commission, General Services Administration, the intelligence community, and the private sector.

Reducing ICT supply chain risk is a National security imperative and one that is a key pillar of CISA's Strategic Intent. While many components of CISA play some role in supporting supply chain initiatives, the National Risk Management Center (NRMC) leads the agency-wide supply chain coordination effort—providing program management and analytical support to current lines of effort. These include:

- The ICT Supply Chain Risk Management Task Force
- ICT analysis in support of Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain
- 5G mobile communications security and resilience efforts.

CISA's supply chain risk management efforts are closely integrated with the agency's broader critical infrastructure protection mission. Supply chain risk cuts across many of the 55 National Critical Functions released by CISA in April, and the National Critical Functions framework continues to be an effective platform for holistically understanding and prioritizing risk to our Nation's critical infrastructure.

ICT SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

In 2018, CISA established the Information and Communication Technology Supply Chain Risk Management Task Force as a public-private partnership jointly chaired by CISA and the chairs of the IT and Communications Sector Coordinating Councils. The task force is working to identify and manage risks to the global ICT supply chain and is comprised of 40 industry partners from the IT and Communications Sectors and 20 interagency partners from the U.S. Government.

The first year of the task force focused on 4 priority areas of policy concern for supply chain risk management, including: Information Sharing, Threat Evaluation, Qualified Bidder Lists and Qualified Manufacture Lists, and Policy Recommendations to Incentive Purchase of ICT from Original Equipment Manufacturers and Authorized Resellers.

In September of this year, the task force released an Interim Report providing a status update on activities and objectives of the task force. The report outlines the overall structure of the task force as well as the 4 Working Groups, areas of discussion, and relevant key findings. The Interim Report serves as an important building block for the second year of the task force, including strategic priorities and recommendations.

Among these priorities is enhancing the information sharing about supply chain risks with a particular focus on potential bad actors. The task force identified current gaps in the ability of Government to collect relevant information on bad actors, the ability to use that information as part of an overall evaluation of trusted vendors, and the ability for that information to be shared with the private sector. Crucially, the task force also identified limitations on private-to-private information sharing on supply chain risks because of lingering legal concerns. Going forward, the task force is establishing a Working Group of lawyers from industry and government to address these hurdles and make recommendations for legal and regulatory changes; in addition, the task force is likely to identify the necessary components of an enhanced information sharing environment that can take advantage of factors that contribute to understanding as to whether vendors can be trusted.

Another effort of the task force will be related to taking the output of a list of the Threat Evaluation Working Group—which identified 9 types of supply chain threats and related scenarios—and making recommendations as to how the identified threats and threat scenarios can inform risk management programs for Government agencies, and large and small businesses alike. These threats—whether from counterfeit parts, insider threats, poor cybersecurity practices, or market forces—need to be accounted for in effective supply chain risk management programs.

In addition to its Working Groups, the task force has emerged as a key private-sector touch point for the recently-launched Federal Acquisition Security Council (FASC). All agencies participating in the FASC also have representatives on the task force—a deliberately designed synergy. And, we recently completed an agency-wide data call for the FASC and the task force that identified supply chain risk management programs from across Government for the purpose of increasing integration and synchronization of efforts across the Executive branch.

ICT CRITICALITY ANALYSIS

On May 15, 2019, the President signed Executive Order (EO) 13873: Securing the Information and Communications Technology and Services Supply Chain. This EO declares a National emergency with respect to the threat posed by foreign adversaries to the Nation's information and communications technology supply chain. Specifically, the EO addresses concerns that "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States."

DHS, specifically CISA, plays a key role in EO 13873. Section 5(b) requires the Secretary of Homeland Security to "asses and identify entities, hardware, software, and services that present vulnerabilities in the United States that pose the greatest potential consequences to the National security of the United States." The Secretary of DHS, in coordination with sector-specific agencies and coordinating councils as appropriate, was required to submit an assessment within 80 days of issuance of the EO and annually thereafter. The assessment was required to include an "evaluation of hardware, software, or services that are relied upon by multiple information and communications technology or service providers, including the communication services relied upon by critical infrastructure entities identified pursuant to section 9 of Executive Order 13636."

The Secretary of DHS delegated this responsibility to CISA. To carry out this responsibility, CISA has engaged with its Federal and private-sector partners to provide assessments of ICT hardware, software, and services to determine which pose the greatest threats and vulnerabilities to U.S. critical infrastructure.

CISA will soon release the methodology it used in its assessment in support of the EO. The methodology includes a deconstruction of the ICT supply chain into 61 elements—the hardware, software, and services "building blocks"—that collectively make up the ICT ecosystem. CISA hopes that this elemental deconstruction will have lasting value for supply chain risk management activity beyond this EO.

Among the elements that CISA designated as critical for focusing supply chain risk reduction efforts were Home Subscriber Services, Mobile Switching Centers, and Sensitive Systems Software (to include software-defined networking). Untrustworthy equipment in those supply chains could create an unacceptable amount of risk to the National security of the United States. There would likely be significant regional or National impacts, including affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

5G

With that finding in mind, DHS—and our interagency partners—recognize 5G deployment as a significant area for National and economic security intention. The Fifth Generation Communications Network (5G) is the next generation of wireless technology that represents a complete transformation of telecommunication networks. Combining new and legacy technology and infrastructure, 5G will build upon previous generations in an evolution that will occur over many years, utilizing existing infrastructure and technology.

From my perspective, 5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years and, coupled with the growth of cloud computing, automation, and future of artificial intelligence, demands focused attention today to secure tomorrow.

5G builds upon existing telecommunication infrastructure by improving the bandwidth, capacity, and reliability of wireless broadband services. The evolution will take years, but the goal is to meet increasing data and communication requirements, including capacity for tens of billions of connected devices that will make up the internet of things (IoT), ultra-low latency required for critical near-real-time data transmission, and faster speeds to support emerging technologies. As of June 2019, 5G networks and technologies are in development with a limited rollout in select cities around the world, including 20 in the United States.

DHS, working with its interagency and industry partners, has an opportunity to help shape the rollout of this emerging critical infrastructure, increasing its security and resilience at the design phase and reducing National security risk from an untrustworthy 5G network. Our intent in doing so is to promote the development and deployment of a secure and resilient 5G infrastructure that enables enhanced National security, technological innovation, and economic opportunity for the United States and its allied partners.

Our work in this area will be focused on 6 lines of effort, to include:

- Support the design and deployment of 5G networks with security and resilience in mind, to include investing in Research & Development
- Promote 5G use cases that are secure and trustworthy
- Identify and communicate risks—including supply chain risks—to 5G infrastructure
- Promote development and deployment of trusted 5G components
- Advance the United States' global effort to influence direction of allied nations in 5G deployments
- Provide leadership role within USG to coordinate operational 5G security and resilience efforts.

The analogy of the space race is not entirely incorrect for 5G deployment, but I view it more as a competition between differing views of the world—one in which technology is deployed that protects the values of privacy, enables greater confidence amongst citizenry in essential services, and creates greater connectivity and economic opportunity while not undermining the ability of countries and communities to protect themselves; and, one that views technology as an enabler of illegitimate behavior.

The United States' goal needs to be to do whatever we can to lead the world to the former vision. Industry will be a partner in all of this effort—so, too, will like-minded countries. One particular focus needs to be on ensuring that State-influenced entities do not dominate a market through unfair business practices and to potentially do the work of adversary action. As such, a particular concern that the Department of Homeland Security is focusing on regards the growing presence of Chinese telecom equipment in the Radio Access Network (RAN) portion of the network where there are a limited number of RAN equipment suppliers. There are 5 main purveyors of 5G RAN technology globally, the largest of which is Chinese-based. If Chinese manufacturers continue to gain market share, there will be growing concern about the long-term viability of the existing supply chain for 5G and successor technologies. As such, it is important for the United States and its allies to continue to promote market dynamism and support existing trusted vendors in the space while investing in innovation and research and development that will help the trusted community win the quality battle in the RAN, innovate to a future 5G, and compete on a level playing field in the market. This is particularly necessary to help support deployment across the United States, including in rural communities.

DHS ADVISORY COUNCILS

CISA is working through the Critical Infrastructure Partnership Advisory Council (CIPAC) structure to engage with private-sector stakeholders, especially the Communications and Information Technology Sector Coordinating Councils and the Enduring Security Framework Operations Working Group to collaborate on the risk posed by 5G technologies.

CISA operates the Communications Sector Information Sharing and Analysis Center (ISAC), a partnership of 11 Federal agencies and over 60 private-sector communications and information technology companies. Some of these companies maintain a permanent presence in CISA's operations center. Through the Communications ISAC, Government and industry exchange vulnerability, threat, intrusion, and anomaly information. CISA also uses this mechanism to maintain situational awareness regarding the evolution of 5G standards and carrier 5G plans.

The President's National Security Telecommunications Advisory Committee (NSTAC), created in 1982, provides industry-based analyses and recommendations to the President and the Executive branch regarding policy and enhancements to National security and emergency preparedness (NS/EP) telecommunications. It is composed of up to 30 Presidentially-appointed senior executives who represent various elements of the telecommunications industry. NSTAC is supported by the Secretary of Homeland Security, who is the Executive Agent.

NSTAC has reviewed 5G security issues, including when it finalized its *NSTAC Report to the President on Emerging Technologies Strategic Vision* on July 14, 2017. The report included recommendations on how the government can adapt to "unprecedented growth and transformation in the technology ecosystem over the next decade," including 5G technology, which the NSTAC identified as a near-term transformative technology.

The NSTAC is currently examining technology capabilities that are critical to NS/EP functions in the evolving ICT ecosystem. On April 2, 2019, the NSTAC submitted a letter to the President outlining the first phase of its study to identify the technologies within the ICT ecosystem that are most critical to the Government's NS/EP functions, which include 5G, quantum computing, and artificial intelligence.

During the second phase of this study, the NSTAC plans to examine how certain dependencies, market limitations, and supply chain risks began, using the deployment of 5G technologies as a case study. The NSTAC will formulate recommendations for the recommended National innovation NS/EP ICT strategy. This strategy will ensure that the United States is more resilient, has access to trusted technology to support its NS/EP mission, and leads in the development and use of ICT technology.

RESEARCH AND DEVELOPMENT

The next age of digital transformation depends on the success of the United States' National and global 5G build out. Significant research remains to be done in this area as well as hardening of the 5G network protocols, which are currently in early development. On April 22, 2019, DHS's Science and Technology Directorate and CISA announced an effort related to the development of new standards to improve the security and resilience of critical mobile communications networks. This solicitation established a research and development project for innovative approaches and technologies to protect legacy, current, and 5G mobile network communications services and equipment against all threats and vulnerabilities.

The 3d Generation Partnership Project (3GPP) and the United Nations' International Telecommunications Union (ITU) lead the global 5G standards development initiatives. CISA currently works with industry, including Nation-wide U.S. wireless carriers, in preparing technical standards for the standards development organizations to ensure Public Safety and NS/EP personnel will have priority communications services on 5G networks.

CONCLUSION

In the face of increasingly sophisticated threats, CISA employees stand on the front lines of the Federal Government's efforts to defend our Nation's Federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies.

A holistic understanding of critical infrastructure risk must take into account the supply chain risk stemming from an interconnected society that relies heavily on ICT technology as the supporting backbone of many National Critical Functions. As CISA continues to mature its engagement on supply chain risk management and 5G security and resilience lines of effort, the agency is also working on developing a lasting technological architecture and framework to allow for better-structured supply chain risk analysis. We believe investing in this capability will be critical to fully achieving CISA's critical infrastructure mission in the years to come.

I recognize and appreciate this committee's strong support and diligence as it works to understand this emerging risk and identify additional authorities and resources needed to address it head on. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient homeland through our efforts to defend today and secure tomorrow.

Thank you for the opportunity to appear before the committee today, and I look forward to your questions.

Chairman THOMPSON. Thank you very much. Thank you for your testimony.

We now recognize Mr. Mayer for 5 minutes.

STATEMENT OF ROBERT MAYER, SENIOR VICE PRESIDENT, CYBERSECURITY, USTELECOM

Mr. MAYER. Chairman Thompson, Ranking Member Rogers, and other distinguished Members of the committee, thank you for the opportunity to testify at today's hearing on public-private initiatives to secure the supply chain.

My name is Robert Mayer, I am senior vice president of cybersecurity at USTelecom. I serve as the chair of the Communications Sector Coordinating Council, and serve as co-chair of the Department of Homeland Security Information Communication Technology Supply Chain Risk Management Task Force, hereafter known as "the task force," which is the subject of today's hearing.

The term "supply chain management" only entered the business lexicon in 1983, when distributed computing power and new software applications were replacing traditional analog forms of communications and record keeping. A decade later, the invention of the internet and the proliferation of e-Commerce changed forever the pace, complexity, and scale of commerce, creating a global digital economy that now represents one-fifth of the world's total economic value.

Today we stand at the precipice of an entirely new paradigm, where technological advances in distributed computing, networking, fifth-generation wireless, big data, artificial intelligence, and machine learning promise to fundamentally change the nature of business transactions and the supply chain that is at its foundation.

The question we must now ask ourselves: What risks come with these transformational technologies, and how best can we work together to mitigate them?

It is hard to overstate the complexity of supply chain challenges. For both suppliers and buyers, the potential universe of supply chain vulnerabilities touches all aspects of information technology: Hardware and sub-components, IOT devices, operating systems, softwares, and applications of all varieties, cloud and hosting services, telecommunications equipment, and services. Essentially, any physical or logical element that can be used to generate, store, manipulate, or transport data in digital form.

That means the billions of new connected objects coming on-line will expand the risk universe exponentially. To be clear, many companies in the ICT ecosystem are incorporating high standards of supply chain risk management. Companies with large global and National footprints and have substantial dependencies on foreign inputs have dedicated teams of supply chain practitioners working tirelessly to ensure that their brand is not tarnished and their customers can continue to trust the integrity of their products and services. Rigorous internal systems and controls are applied, and expectations of downstream suppliers are often reinforced by verified attestations, audits, and contractual commitments.

In my written testimony, I described the efforts of the 4 ICT working groups and some of the Year 2 activities now being discussed among task force members.

I do want to bring to the committee's attention some insights from the information-sharing group as legislative proposals are likely to emerge. This group has identified one of the most serious obstacles to effective supply chain risk management. Information about suspect suppliers cannot be freely exchanged without—with other parties operating in the same space. Why? Because doing so could subject enterprises to a variety of legal actions, including violations of Federal or State antitrust laws, anti-competitive behaviors, or deceptive trade practices.

Private causes of action also can result from transgressions involving commercial agreements and other statutory or common law infractions. The working group is recommending that independent legal counsel study the matter more deeply, and determine to what extent liability protections are needed to facilitate sharing.

The task force's importance and value is not only reflected in the sum of its current and future work, but also because it is a model for collectively advancing policies critical to our National interest that can be operationalized in ways that have a high likelihood of success.

The task force success did not happen overnight. It is the result of more than a decade of an increasingly robust, mutually accountable, and trusted public-private partnership. The task force governance structure supports the important principles of whole-of-Government approach, and has brought an extraordinary group of private- and public-sector experts to the same table to tackle some of the most challenging supply chain issues.

I know I speak for all the members of the task force when I say we appreciate the gravity and urgency of our work, and we are committed to delivering strategies that will lead to meaningful and sustainable solutions.

Thank you for the privilege of participating in this hearing, and I look forward to answering your questions.

[The prepared statement of Mr. Mayer follows:]

PREPARED STATEMENT OF ROBERT MAYER

OCTOBER 16, 2019

Chairman Thompson, Ranking Member Rogers, and other distinguished Members of the committee, thank you for the opportunity to testify at today's hearing on Public-Private Initiatives to Secure the Supply Chain. My name is Robert Mayer and I am the senior vice-president cybersecurity at USTelecom, the Nation's trade association representing broadband providers, suppliers, and innovators connecting our families, communities, and enterprises to the future. Our diverse membership ranges from large publicly-traded global communications providers, manufacturers, and technology enterprises, to small companies and cooperatives—all providing advanced communications services to markets, both urban and rural and everything in between.

I also serve as the chair of the Communications Sector Coordinating Council. I currently serve as co-chair of the Department of Homeland Security Information and Communications Technology (ICT) Supply Chain Risk Management Task Force which is the subject of today's hearing.

The term supply chain management only entered the business lexicon in 1983—when distributed computing power and new software applications were replacing traditional analogue forms of communications and record keeping. A decade later, the invention of the internet and the proliferation of e-commerce changed forever the pace, complexity, and scale of commerce creating a global digital economy that now represents one-fifth of the world's total economic value.

Today we stand at the precipice of an entirely new paradigm where technological advances in distributed computing, networking, fifth-generation wireless, big data, artificial intelligence, and machine learning promise to fundamentally change the nature of business transactions and the supply chain that is its foundation. The question we must now ask ourselves. What risks come with these transformational technologies and how best can we work together to mitigate them?

It's hard to overstate the complexity of supply chain challenges. For both suppliers and buyers, the potential universe of supply chain vulnerabilities touches all aspects of information technology—hardware and sub-components, IoT devices, operating systems, software and applications of all varieties, cloud and hosting services, telecommunications equipment or services. Essentially, any physical or logical element that can be used to generate, store, manipulate, or transport data in digital form. That means the billions of new connected objects coming on-line will expand the risk universe exponentially.

To be clear, many companies in the ICT ecosystem are incorporating high standards of supply chain risk management practices. Companies with large global and National footprints and substantial dependencies on foreign inputs, have dedicated teams of supply chain practitioners working tirelessly to ensure their brand is not tarnished and that their customers can continue to trust the integrity of their products and services. Rigorous internal systems and controls are applied and expectations of downstream suppliers are often reinforced by verified attestations, audits, and contractual commitments.

The task force has addressed a small, but very important slice of the supply chain risk management universe. Working group 1, the information-sharing group, has identified one of the most serious obstacles to effective risk management. Information about suspect suppliers cannot be freely exchanged when enterprises are subject to a variety of legal actions, including violations of Federal or State anti-trust laws, anti-completive behaviors, or deceptive trade practices. The working group has recommended that independent legal counsel study the matter more deeply with possible legislative or regulatory recommendations to reduce liability risk.

Working group 2 focused on the identification of processes and criteria to better understand and evaluate threats to ICT suppliers. That working group identified 9 major threat categories comprising approximately 200 unique threats. The working group currently is framing work that might include examples of how enterprises can leverage the task force threat assessment as an information feed into their own company-specific risk management program.

Working Group 3 examined how Qualified Bidder and Manufacturer lists might help mitigate supply chain risk. The group examined 5 programs within the Federal Government that make use of such lists and identified several potential follow-up activities that would advance current and future use of such qualified lists.

Finally, Working Group 4 explored concerns related to deployment of counterfeit ICT products and recommended adding a new section to the Federal Acquisition Regulation (FAR). The section would be titled "Procurement of Information and Communications Technology from a trusted Original Manufacturer, the Authorized Channels or other Approved Source." That recommendation has been submitted to the Federal Acquisition Security Council for Review.

The task force's importance and value is not only reflected in the sum of its current and future work but also because it is a model for collectively advancing policies critical to our National interests that can be operationalized in ways that have a high likelihood of success. The task force's success did not happen overnight; it is the result of more than a decade of an increasingly robust, mutually accountable and trusted public-private partnership. The task force's governance structure supports the important principle of a whole-of-Government approach and has brought an extraordinary group of private- and public-sector experts to the same table to tackle some of the most challenging supply chain issues. I know I speak for all of the members of the task force when I say we appreciate the gravity and urgency of our work, and we are committed to delivering strategies that will lead to meaningful and sustainable solutions.

Thank you for the privilege of participating in this hearing. I look forward to answering your questions.

Chairman THOMPSON. Thank you for your testimony.

I now recognize Mr. Miller to summarize his statement for 5 minutes.

STATEMENT OF JOHN S. MILLER, VICE PRESIDENT OF POLICY AND SENIOR COUNSEL, INFORMATION AND TECHNOLOGY INDUSTRY COUNCIL

Mr. MILLER. Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee, on behalf of the Information Technology Industry Council, or ITI, thank you for the opportunity to testify today.

As the current chair of the Information Technology Sector Coordinating Council and co-chair of the task force, I welcome the committee's interest on the importance of public-private initiatives to secure the supply chain.

ITI is a global policy and advocacy organization representing nearly 70 of the world's leading ICT companies. The global ICT industry respects and takes seriously the U.S. Government's obligation to address risks to global supply chains and its responsibility to protect National security more broadly.

Public-private partnerships are an essential mechanism for addressing our shared security challenges. Working together to leverage the public-private partnership structures that were pioneered in the United States, industry and Government can seize this moment and lead on developing supply chain security policy solutions that also support innovation and economic growth.

Two key factors are making supply chain security a growing challenge.

First, while managing risk to global supply chains has always been complex, our increasingly connected global ICT infrastructure is powering every segment of the economy as we move toward surpassing 20 billion connected devices in 2020, illustrating the vast scope of the challenge. Nation-state threats, too, are now a greater part of the conversation, implicating not only National security, but also economic security and U.S. competitiveness.

Second, the rise of the 5G networks and the data-centric world they will power has magnified supply chain security challenges and anticipated risks, driving governments to more intensely focus on the issue. Specifically, the increased speed and volume of data that will soon flow through networks raises significant questions regarding data access that implicate not only National security, but individual privacy, technological leadership, and economic competitiveness.

The Supply Chain Task Force was established to address these evolving threats, and brings together stakeholders from across the communications and IT sectors and multiple Federal agencies to enable targeted resource investment, share technical and policy expertise, and identify actionable policy solutions.

DHS's Cybersecurity and Infrastructure Security Agency recently published an interim report detailing the task force's progress to date.

Two key takeaways from the report that I would like to highlight are, No. 1, information sharing remains a top priority. The task force determined that the highest-value supply chain threat information relates to suspected, known, or proven bad actors in the supplier context, but that legal and policy issues often prevent the sharing of such information. This insight suggests the need for further legal analysis and foreshadows the potential need for future legislative action.

No. 2, the supply chain threat landscape is vast and diverse. The task force evaluated the global supply chain threat landscape, compiling nearly 200 supplier-related threats, and categorizing those threats into 9 categories, ranging from cybersecurity to economic to legal to external threats such as natural disasters. This work illustrates how adequately managing supply chain risk requires a fact-based and contextual analysis of multiple identifiable threats and potential mitigations.

I would like to conclude by offering 3 concrete recommendations.

First, continue using the task force as a key resource for public-private collaboration on supply chain risk management. The task force's work to inform the ICT risk assessment required by the supply chain Executive Order demonstrates it can be deployed as a resource to help inform supply chain policy efforts beyond the task force's core work streams.

A significant opportunity exists to leverage the connective tissue established between the task force and the Federal Acquisition Security Council to help build out the rules to implement last year's Secure Technology Act in a way that achieves its security objectives while minimizing unintended impacts to continued technology innovation and the technological leadership of U.S. companies.

Second, target future U.S. supply chain measures to identified gaps. While we appreciate the focus of policy makers globally on the urgency of addressing supply chain risk, the sheer volume of policy making activity has, in some instances, overwhelmed the ability of private-sector actors to effectively keep up.

The task force realized early on that conducting an inventory of public-sector supply chain activities would be useful for helping the task force and other stakeholders identify what tasks weren't being done, and to prioritize those that were most important. Once complete, we should share the task force inventory results with key stakeholders, and leverage those results to inform supply chain policy making across the board.

Finally, we encourage the U.S. Government to continue to deepen engagement with international partners and pursue a coordinated approach. Global supply chain security challenges ultimately call for globally scalable solutions, and we encourage cross-border collaboration to avoid harmful fragmentation. The Prague principles on 5G security provide a good blueprint for such activity.

Thank you again for the opportunity to testify today. I look forward to your questions.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF JOHN S. MILLER

OCTOBER 16, 2019

Chairman Thompson, Ranking Member Rogers, and distinguished Members of the Committee on Homeland Security, thank you for the opportunity to testify today. I am John Miller, vice president of policy and senior counsel at the Information Technology Industry Council (ITI).[1] I have deep experience working on public-private security initiatives in the United States, including serving as the current chair of the Information Technology Sector Coordinating Council (ITSCC)[2] and co-chair of the Information and Communications Technology Supply Chain Risk Management Task Force (task force). I am honored to testify before your committee today on the important topic of "Public-Private Initiatives to Secure the Supply Chain." The global ICT industry respects and takes seriously the U.S. Government's—and other governments'—obligation to address risks to global information and communications technology (ICT) supply chains, and the responsibility of governments to protect National security more broadly. We believe government and industry must work together to achieve the trusted, secure, and reliable global supply chain that is a necessary priority for protecting National security and is also an indispensable building block for supporting innovation and economic growth. We welcome the committee's interest and engagement on this subject.

ITI represents nearly 70[3] of the world's leading ICT companies. Robust security is a key pillar of building and maintaining trust in the global ICT ecosystem, and is thus essential to our businesses and customers. Supply chain security and cybersecurity are rightly priority issues for governments and our industry, and we share the common goals of improving cybersecurity and supply chain security, protecting the privacy of individuals' data, and maintaining strong intellectual property protections. Further, our members are global companies and do business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, such as financial services, health care, and energy. We thus acutely understand the importance of securing global ICT supply chains as not only a global business imperative for companies and customers alike, but as critical to our collective security. As a result, our industry has devoted significant resources, including expertise, initiative, and investment in cybersecurity and supply chain risk management efforts to create a more secure and resilient internet ecosystem.

Our members also understand we cannot tackle current and future cybersecurity challenges on our own. We recognize public-private partnerships and other multistakeholder approaches are essential to addressing our shared security challenges and have thus prioritized working with governments around the world to help develop cybersecurity and supply chain security policy solutions. We believe the emergence of supply chain security as a priority issue amongst government policy makers globally highlights the urgency with which like-minded nations must address this issue. It also represents an important opportunity for U.S. policy makers to advance supply chain security policy approaches that are not only compatible with, but indeed drive, global policy making in this space. Working together to leverage the public-private partnership structures that were pioneered in the United States, as well as sound risk-management based approaches that we have long advocated as best cybersecurity practices, industry and Government can seize this moment to lead on supply chain security policy together.

I will focus my written testimony on 4 areas: (1) The evolving supply chain threat and the need for public-private action; (2) the creation of the task force grounded

[1] The Information Technology Industry Council (ITI) is the premier advocacy and policy organization for the world's leading innovation companies. ITI navigates the constantly-changing relationships between policy makers, companies, and non-governmental organizations to promote creative policy solutions that advance the development and deployment of technology and the spread of digitization around the world. Visit *https://www.itic.org/* to learn more.

[2] The Information Technology Sector Coordinating Council (IT SCC) serves as the principal entity for coordinating with the Government on a wide range of critical infrastructure protection and cybersecurity activities and issues. The IT SCC brings together companies, associations, and other key IT sector participants, to work collaboratively with the Department of Homeland Security, Government agencies, and other industry partners. Through this collaboration, the IT SCC works to facilitate a secure, resilient, and protected global information infrastructure. Visit *https://www.it-scc.org* to learn more.

[3] See ITI membership list at *https://www.itic.org/about/membership/iti-members.*

in principles of risk management and public-private partnerships; (3) the progress of the task force to date, including the recently-released Interim Report and the task force's work to help the Department of Homeland Security (DHS) implement the supply chain Executive Order (EO); and (4) recommendations on a collaborative path forward, including discussing how the Federal Acquisition Security Council (the "FASC") and other Federal Government stakeholders can synergistically work with the task force to help advance our collective supply chain security policy interests.

1. THE EVOLVING SUPPLY CHAIN THREAT

While supply chain security is not a new topic, particularly for large technology companies managing sophisticated global supply chains, the heightened policy maker focus on the issue over the past 2 years is unprecedented. The increased focus on supply chain security, by governments, policy makers, and private-sector actors, is prompted by a few key developments.

A Multifaceted and Growing Threat.—Supply chain risk management (SCRM) has always been a multifaceted challenge. On the one hand, SCRM is one element of an organization's overall cybersecurity risk management program (indeed, the visionary Cybersecurity Framework developed in the U.S. integrated SCRM into Version 1.1 in 2018). On the other hand, a SCRM program must address much more than just cybersecurity threats to IP, systems and networks, but also threats that are physical (e.g. building security), personnel-based (e.g. insider threats), economic (e.g. cost-volatility), legal (e.g. weak IP laws), development or manufacturing-related (e.g. compromises in system, hardware, or software development life-cycle processes or tools), or external threats such as those related to environmental, geopolitical, or workforce-related factors.

When we consider our increasingly connected global ICT digital infrastructure and economy, and acknowledge the reality that ICT products, hardware, software, and services are powering every segment of the economy as we move toward surpassing 20 billion connected devices in 2020,[4] one can better appreciate the vast scope of risks to the global ICT supply chain "attack surface" that we need to secure. Nation-state threats, too, are a greater part of the conversation than before, implicating not only National security but also economic security and U.S. competitiveness.

Putting both of those pieces together—the large and growing number of all-hazards threats and the vast and increasing number of products and services generated by the global ICT supply chain—we can better appreciate the scope of the risks that must be managed, and the scope of the policy challenge.

The Rise of 5G and Data.—The build-out of 5G networks has magnified the spotlight on supply chain security challenges, where the focus has largely been on anticipated risks. While securing the 5G infrastructure, including both networks and component ICT parts, is of course critical, it bears noting that 5G networks and equipment will also contain security enhancements that can help make 5G networks more secure than previous generations. Rather, it is the increased speed and volume of data that will soon flow through 5G networks, helping to enable the next generation of data-enabled innovations such as the internet of things (IoT) and artificial intelligence (AI), that has driven the United States and other governments to more intensely focus on global supply chain security threats.

As the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) documents in its 5G Risk Assessment,[5] 5G networks will enable increased speeds and amounts of data that are staggering. The data flowing through 5G networks, or throughput, will be multiplied by a factor of up to 200. The speed at which data travels, or latency, will be up to 20 times faster than in 4G networks. The implications of these numbers are significant—not only because 5G will power the next wave of data-driven innovations such as IoT and AI, but also because the question of who potentially has access to or controls that data raises a panoply of questions, including implications for individual privacy, National security, technological leadership, and economic competitiveness. The centrality of data to our present and future lives and to the supply chain debate underscores that SCRM must focus on managing potential vulnerabilities and other malicious activity targeted at ICT supply chains as well as the potential for governments

[4] "Leading the IoT, Gartner Insights on How to Lead in a Connected World", Mark Hung, 2017, available at: *https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.*

[5] "Overview of Risks Introduced by 5G Adoption in the United States", Cybersecurity and Infrastructure Security Agency (CISA), July 31, 2019, available at: *https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.*

or others perceived as adversaries to access that data through their domestic legal regimes.

While it will be important to continue to focus on ICT SCRM, and creating high assurance, trusted ICT products, we must realize that managing the full range of data access risks implicated by the current SCRM debate moves us into somewhat uncharted territory.

Increase in Supply Chain Policy Making.—We appreciate the focus of governments and policy makers globally on the urgency of addressing supply chain risk, for all the reasons stated above. However, the sheer volume of policy making activity has, in some instances, overwhelmed the ability of private-sector entities, particularly small and medium-sized businesses (SMBs), to effectively monitor, make sense of, and implement important supply chain policy or legal developments. While well-intended, some policies may have unintended consequences on security, innovation, and competitiveness—which is why public-private sector cooperation is imperative. To ensure these measures can be properly addressed and implemented, is critical that this activity is coordinated and targeted at identified legal or policy gaps.

Global government activity regarding supply chain security is rising across the European Union, and in countries including Japan, Australia, and elsewhere. In the United States there continues to be significant and not always visible activity across multiple Federal agencies, and the last few years have brought multiple legislative efforts from Congress, including numerous stand-alone bills and National Defense Authorization Act (NDAA) amendments, as well as President Trump's recent supply chain EO, and the launch of the FASC following last year's SECURE Technology Act. The task force helps drive a more holistic, coordinated approach through a better understanding of supply chain policy making activity in the United States and holds the promise to help streamline efforts to address potential risks.

2. THE CREATION OF THE TASK FORCE GROUNDED IN ON PRINCIPLES OF RISK MANAGEMENT AND PUBLIC-PRIVATE PARTNERSHIPS

While formation of the Supply Chain Task Force was motivated out of a heightened concern regarding supply chain threats, its formation, structure, and mandate are grounded in cyber and supply chain security principles long advocated by the ICT industry. Those principles are based on the importance of taking risk-management based approaches to complex threats such as global ICT supply chain security threats and the promise of public and private stakeholders working together through partnerships to forge durable solutions to those threats.

Approaches to Risk Management: No One Size Fits All.—The ICT industry has long maintained that efforts to improve cybersecurity, including supply chain security, must be based on effective risk management of a dynamic and ever-evolving set of threats.

Cybersecurity is not an end-state, but rather a continuous process of protecting the global digital infrastructure and its users.—No sector of the economy is without some inherent risk, whether that is the result of a natural disaster, a malicious automated attack, or simple human error. As cyber and supply chain attacks become increasingly more sophisticated, the adoption of comprehensive risk management strategies is critical for organizations of all sizes and across all sectors, particularly those managing complex global supply chains. By integrating technologies, people, and processes into an overall risk management framework, limited resources can be most efficiently focused on where the need is greatest.

Effective risk management allows individuals and entities to properly identify, assess, prioritize, and manage threats to their data, systems, and operations, including supply chains. There is no one-size-fits all approach. Eliminating one potential threat may unintentionally create other vulnerabilities. For example, using the same supplier (even a "trusted" supplier) throughout a network or supply chain could make it easier to exploit a vulnerability; thus, a diversity of suppliers is crucial to risk management. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, informed by a collaborative effort involving public and private-sector stakeholders, provides a familiar example of a flexible risk management tool that can help a diversity of entities—critical infrastructure owners and operators, government agencies, and other stakeholders—understand how to approach cybersecurity risk management. Notably, Version 1.1 of the Framework, published in 2018, incorporates SCRM standards, guidelines, and best practices.

Global ICT companies build risk management into their daily operations and long-term planning, including efforts to secure their supply chains, through mechanisms like legal and contractual agreements, cybersecurity operational controls, adherence to global risk management standards, and a host of other practices. As the primary owners and operators of critical cyber infrastructure, the private sector has devoted significant resources, including expertise, initiative, and investment in cybersecurity and risk management efforts to create a more secure and resilient internet ecosystem. However, the ICT industry understands it cannot tackle current and future cybersecurity challenges on its own.

Public-Private Partnerships Are Essential.—Public-private partnerships and other multi-stakeholder approaches are essential to addressing supply chain security. Government and industry often have access to unique information sets—only when this information is shared can all relevant stakeholders see the complete picture. These partnerships are essential to: (1) Identify potential threats; (2) understand how and whether the risk can be managed; and (3) determine what actions should be taken to address risks without yielding unintended consequences. The private-sector ICT community has been foundational in developing the infrastructure of cyber space and, for well over a decade, has provided leadership, innovation, and stewardship in all aspects of cybersecurity, including helping to develop and participating in numerous public-private partnership structures and efforts.

Sector Coordinating Councils. Global ICT companies participate in sector-coordinating councils (SCCs), which are self-organized, self-governed councils that allow owners and operators of critical infrastructure to engage on a range of sector-specific strategies, policies, and activities. SCCs also enable participants to coordinate with their sector-specific agencies and related Government Coordinating Councils (GCCs) to facilitate Government collaboration on a range of critical infrastructure security policy and strategy issues, including on supply chain security. I am pleased to chair the ITSCC and to work closely with my counterparts in the Communications SCC, as well as DHS as our sector-specific agency and other U.S. Government partners, on the task force.

Formation of the Task Force.—The task force embodies these critical dual principles of risk management and public-private partnership. The task force aims to better secure global ICT supply chains, gathering stakeholders from key communities—including from the communications and IT sectors, as well as across multiple Federal agencies, including Departments of Homeland Security, Commerce, Defense, Treasury, Justice, and Energy; Office of the Director of National Intelligence (ODNI), National Security Agency (NSA), General Services Administration (GSA), Social Security Administration (SSA), National Telecommunications and Information Administration (NTIA), Federal Communications Commission (FCC), NIST, NASA, and others. These entities should work together to enable targeted resource investment, share technical and policy expertise, and identify actionable policy solutions aimed at helping public and private stakeholders better manage ICT supply chain risks.

From the perspective of the IT sector—both ITI and the ITSCC—there was no hesitation regarding the merits of task force participation. Supply chain security had been identified as the top cybersecurity priority of both organizations, and many experts across the sector who had been working on this issue for a long time shared the view that this was a moment in time where real progress could be made.

There was also wide-spread agreement that the challenges quite clearly are shared by Government and the private sector—and thus adequately addressing them requires a collaborative, holistic approach involving the IT and Communications sectors working together with U.S. Government partners from key Federal agencies.

3. PROGRESS OF THE TASK FORCE TO DATE

The task force was chartered in late 2018 by DHS and CISA working with the IT and Communications SCCs, with the express purpose of providing guidance and recommendations to Government and private-sector critical infrastructure owners and operators to help them better assess and manage risks associated with the global ICT supply chain.

Comprised of 60 voting members—20 IT companies and associations, 20 communications-sector stakeholders, and 20 representatives from across the U.S. Government—the task force acts as a forum for private-sector and Government collaboration on methods and practices to effectively identify, prioritize, and mitigate ICT supply chain risks, with the goal of providing realistic, actionable, timely, economically feasible, scalable, and risk-based recommendations for addressing those risks. Beyond its voting membership, scores of other entities have additionally participated in the Task Force at the working level.

Once we were up and running, the task force members surveyed the vast supply chain threat and risk management landscape, identifying 4 initial working groups focused on both longer-term, foundational efforts that could have global ICT ecosystem-wide impact and shorter-term tactical efforts geared toward shoring up the

Federal Government's supply chain: (1) Development of a common framework for the bi-directional sharing of supply chain risk information between Government and industry; (2) identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services; (3) identification of market segments and evaluation criteria for Qualified Bidder and Qualified Manufacturer lists to address considerations of vendor and product inclusion and exclusion; and (4) policy recommendations to incentivize purchase of ICT from original equipment manufacturers (OEM) and authorized resellers.

Interim Report.—The Interim Report,[6] published in September 2019 at CISA's 2d Annual Cybersecurity Summit, provides a fuller summary of the task force's origins, membership, and workstreams, and also details progress to date on each of those workstreams. Rather than restating all that information in my testimony, I thought the committee would find it more helpful if I highlighted a few key takeaways:

Information sharing remains a key priority. Working Group One made excellent progress exploring the types of information that would be most valuable in mitigating supply chain risk; whether that information exists in a standardized or easily accessible form or from sources that can be easily identified, accessed, and leveraged for risk management purposes; and what barriers might exist that are impeding the collection and or dissemination of such information. While Working Group One determined that many types of risk information are indeed available, the sources were not always easily known and did not typically exist in a standardized format (unlike cyber threat indicators in the cybersecurity threat information sharing context). Additionally, due to the wide array of supply chain threats, such information was not easily centralized nor accessible.

Working Group One significantly determined that the highest-value supply chain threat information relates to suspected, known, or proven bad actors in the supplier context, but that legal and policy issues often prevent the sharing of such information. The Working Group concluded that further legal analysis and guidance are thus prerequisite to fully developing the envisioned bi-directional supply chain information sharing framework. This foundational work will likely be carried forward into year 2 of the task force and may well presage the need for future legislative action to remove legal barriers to effective sharing of SCRM threats.

The supply chain threat landscape is vast. The efforts of Working Group Two help illustrate the vast threat space in play when we consider scope of global ICT supply chain challenges. Working Group Two was established to identify processes and criteria for threat-based evaluation of ICT suppliers, products, and services. The working group concentrated on threat evaluation related to suppliers as an initial matter, rather than risk assessment, to ensure it was looking more broadly at the breadth of the SCRM ecosystem, rather than at risks associated with specific ICT products and services.[7] The working group methodically identified and inventoried the global supply chain threat landscape, compiling nearly 200 supplier-related threats and categorizing those threats into 9 categories to provide a helpful taxonomy. The threat categories included counterfeit parts, cybersecurity, internal security operations and controls, compromise of system development life cycle and tools, insider threats, inherited risks (extended supply chain), economic, legal, and external end-to-end threats ranging from natural disasters to workforce and labor issues.

The Working Group then developed several threat scenarios, ranging from ransomware attacks to natural disasters, and reviewed and documented those scenarios to provide additional context regarding the threat, its importance and potential impact on the supply chain, as well as information related to threat sources, vulnerabilities, and potential mitigations. Next steps for the Working Group could include creating a similar inventory and taxonomy of threats related to ICT products and services (as per the group's mandate and providing a similar assessment of various threat scenarios related to those products. In any event, the foundational work around threat evaluation has already informed the work of other task force working groups, and as the work product matures can prove invaluable for informing future Government and private-sector SCRM activities.

[6] "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report: Status Update on Activities and Objectives of the Task Force," CISA, September 2019, available at: *https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20-Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29__-508.pdf*.

[7] Working Group 2 determined that "risk" is the intersection of assets, threats, and vulnerabilities. A vulnerability is a shortcoming or hole in the "security" of an asset. Risk represents the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

We need to continue to explore the extent to which we can leverage public-sector SCRM solutions in the private sector and vice versa. Working Groups 3 and 4 tackled tactical issues more immediately relevant to Federal Government SCRM and procurement, including identification of market segments and evaluation criteria for Qualified Bidder (QBL) and Manufacturer (QML) lists (Working Group 3) and policy recommendations to incentivize the purchase of ICT from OEMs, authorized channels, or other trusted suppliers (Working Group 4). Whether and how to use QBLs and QMLs is a topic with different implications in the public procurement and private-sector contexts. For instance, many global companies currently manage trusted supplier programs and there are lessons that could be leveraged in Federal procurement. However, the process of qualifying suppliers in the public-sector procurement context could have a disproportionate impact on SMBs if not managed carefully. These are the types of issues Working Group 3 will continue to explore. In the case of Working Group 4, the primary tasking of the group was completed with the delivery of its policy recommendation, Procurement of ICT from OEMs, their Authorized Channels, or other Trusted Suppliers, and is primarily geared toward addressing risks associated with the procurement of potentially counterfeit products from the gray market or other unauthorized channels. The efforts of Working Group 4 illustrate the task force's capability to rapidly conclude targeted projects and make recommendations that can translate into policy solutions in the short term.

Urgent Supply Chain Inventory Work.—As the Interim Report indicates, good progress was made on compiling a private-sector inventory of SCRM standards, guidance, and best practices. This inventory work product will provide invaluable guidance that companies and Federal Government agencies can use to better inform their supply chain risk management activities. A parallel effort to compile supply chain risk management efforts across the Federal Government is still in flight. When completed and shared, the Government inventory will assist the task force members as they consider future workstreams and can serve as a resource for policy makers in Congress and elsewhere as they consider which aspects of the multi-faceted supply chain issue to address via legislation. Further, the Government inventory will bring clarity to the supply chain risk management landscape for those stakeholders who have expressed concern that that the volume of supply chain risk management activity is difficult to effectively monitor.

Collaboration with FASC.—The task force is also coordinating efforts with the Federal Acquisition Supply Chain (FASC) to help ensure the effectiveness of the implementation of the Federal Acquisition Supply Chain Security Act (FASCSA) (passed late last year as part of the SECURE Technology Act). Having established the connective tissue between the task force and the FASC over the past several months, the task force is poised to help inform the interim implementing rules for FASCSA due at the end of 2019 and the final rules due in 2020, as well as to advance a number of other interagency supply chain risk management priorities.

Collaboration on the Supply Chain EO.—In addition to its regular workstreams, the task force also stepped in to assist DHS as it fulfilled its duties pursuant to Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain (Supply Chain EO), which tasked DHS with producing a report assessing the criticality of ICT products and systems. Task force members provided required private-sector input to CISA's National Risk Management Center (NRMC), which was delegated the responsibility of conducting the ICT criticality assessment required by the Supply Chain EO. This input resulted in a deconstruction of the ICT supply chain into 5 roles, 11 sub-roles, and 61 elements (ICT hardware software and services). DHS has stated that it hopes this elemental deconstruction will provide a helpful and standardized taxonomy for discussing ICT criticality within the task force and elsewhere.

The initial assessment focused on ICT products and services comprising the "connect" theme of the National Critical Functions list (primarily covering the backbone of national connectivity enabling cross-country and global core telecommunications networks and services), and future assessments will address other themes identified by the NRMC in the National Critical Functions (NCFs).[8] As we understand it, the assessment will inform the Commerce Department's promulgation of rules to implement the Supply Chain EO, and the assessment may help inform any future work taken on by the task force to assess threats associated with ICT products and services. The deployment of the task force to assist in producing the ICT assessment helps illustrate the value of the partnership as a durable resource to assist Government policy makers implement SCRM policies.

[8] "National Critical Functions Set (NCFs)", CISA, April 2019, available at: *https://www.dhs.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf.*

4. RECOMMENDATIONS ON A COLLABORATIVE PATH FORWARD

My testimony thus far illustrates the substantial amount of progress that has been made by the task force, but also recognizes that there is much work still to be done. While the task force intends to continue to advance the ball on multiple SCRM projects during year 2 of its mandate, below are concrete recommendations for U.S. Government actions on how to maximize the impact and effectiveness of the task force's work to aid in other Federal supply chain efforts, as well as recommendations for broader strategic U.S. Government action to address global SCRM challenges.

Build Out the Established Connective Tissue Between the Task Force and the FASC.—Structurally, the established connective tissue between the task force and the FASC creates real opportunities for the FASC to leverage the private-sector expertise assembled in the task force to help build out the rules to implement the FASCSA. Involving the task force in its efforts with more regularity can help the FASC achieve the bill's objectives for better securing the Federal Government's supply chain, while minimizing unintended impacts to continued technology innovation and the technological leadership of U.S. companies.

Prioritize Communicating the Task Force Inventory Results to Key Stakeholders and Integrate the Inventory Results into SCRM Policy Planning.—Soon after the task force's inception, we reached consensus that conducting an inventory of public-sector supply chain activities would be useful to help bring order to the scores of disconnected on-going SCRM efforts across the Federal Government. Taking a strategic approach, the task force's goal in recommending the Government conduct such an inventory was that by taking stock of the various existing and on-going supply chain efforts we could prevent duplicative efforts, and identify what work needed to be done. After completion and review of existing efforts (which will essentially provide a gap analysis), both the task force and other stakeholders will be better situated to: (1) Identify what tasks aren't being done and prioritize those that are most important and needed; (2) identify tasks that are most well-suited to be completed by the task force; and (3) identify what tasks are important, but should be completed by others (such as by Congress in instances where changes to legal authorities are needed to implement SCRM improvements).

Embrace the Task Force as the center of gravity for public-private collaboration on SCRM.—The task force could also help increase visibility of the on-going efforts and construct a narrative to articulate how everything fits together. If we take this type of strategic 360-degree approach to the problem, we can essentially position the task force as the central hub for all the many on-going and disconnected supply chain efforts across the U.S. Government and industry more broadly. Other stakeholders, including Congress, will at least indirectly benefit from cementing the task force as an SCRM resource.

Further streamline USG supply chain efforts.—To help mitigate current and on-going SCRM risks, we recommend that Congress work with the administration in streamlining existing and new tools on supply chain issues (including the FASC, FASCSA implementation, and Supply Chain EO) to better align resources and avoid duplicating efforts and support long-term, coordinated solutions to address global supply chain challenges. The Government inventory can play a key role here.

Target Future Supply Chain Measures to Identified Gaps.—The task force learned quickly through our initial scoping activities that attempting to "boil the ocean" to "solve" supply chain security challenges would be a fruitless task. Instead, we worked to target both foundational and tactical workstreams that could tackle discrete elements of the issue, while also laying the groundwork for future success. Laws, regulations, and other measures to address supply chain security risks should take a fact-based, narrowly-tailored approach to combat concrete and identifiable risks, rather than apply broadly to entire categories of technology or business activity.

Deepen Engagement with International Partners and Pursue a Coordinated Approach.—Global ICT SCRM challenges ultimately call for globally scalable solutions, and we encourage cross-border collaboration on this issue. The United States and other open economies should take common approaches to technology-related National security risks—including through promotion of global, consensus-based, industry-led standards—to avoid harmful fragmentation of markets. The Prague Principles on 5G Security[9] provide a good blueprint for this sort of activity.

[9] "The Prague Proposals: The Chairman Statement on Cybersecurity of Communication Networks in a Globally Digitalized World." May 3, 2019, available at: *https://www.vlada.cz/assets/mediacentrum/aktualne/PRG_proposals_SP_1.pdf*.

CONCLUSION

Members of the committee, ITI and our member companies are pleased you are examining how public-private partnerships play a key role in addressing evolving and increasingly sophisticated supply chain threats.

Historically, the United States has maintained a leadership position in cyber space—from the companies who have led the way in building the global digital economy and internet-based services that have fueled its growth, to visionary cyber policy developments such as the Cybersecurity Framework, to pioneering the use of cybersecurity public-private partnerships. The U.S. Government should aspire to maintain a similar leadership position going forward on SCRM policy, and to do so it must work collectively, via public-private collaboration and across sectors, both domestically and on the global stage.

ITI stands ready to provide you any additional input and assistance in our collaborative efforts to develop policy approaches to supply chain security that continue to leverage risk management-based solutions and public-private partnerships as the most promising way forward for addressing complex and evolving global ICT supply chain threats.

I thank the Chairman, Ranking Member, and Members of the committee for inviting me to testify today and for their interest in and examination of this important issue. I look forward to your questions.

Thank you.

Chairman THOMPSON. Thank you very much. I remind all witnesses for their testimony, and I really appreciate you for your sharing that.

I guess the concern that I heard from all the witnesses is you might learn who a bad actor might be, but there might be some liabilities in saying who that bad actor might be. Can you burrow down a little bit and help the committee with—we have identified them, but now, because of liability concerns, we can't share who they are. How do we—is it liability protections, as somebody talked about?

But I guess the task force's work is good. But I think at this point you have given us additional problems, and not enough solutions. I guess I am waiting on the next report.

So Mr. Mayer, you brought it up, so I will start with you.

Mr. MAYER. So the Congress has made some progress with—important progress with information sharing. So the 2015 Cybersecurity Information Sharing Act created liability protections for sharing indicators of compromise.

So indicators of compromise would be some indication that there is a cybersecurity threat, and it is very specific, and that can be shared. What we don't have is a situation where an organization, for example, has a piece of equipment where they discover, you know, some software, malware, or some—or a pattern of activities that allow—makes them feel very suspicious about a particular company that would be very beneficial to share with—it could be upstream providers, it could be downstream providers, and it could be anybody else in the ecosystem that could benefit from that information.

The lawyers are going to be very reluctant to allow that person, that company, to make those kinds of remarks or evidence without liability protections, because there are laws in place, and private causes of action that could result in litigation. So in the absence of a similar liability protection that was created in 2015 for this particular instance, the members of the working group said we need to think about how we can encourage that type of information sharing.

Chairman THOMPSON. Well, Mr. Miller, since you included that as one of your recommendations, share some more enlightenment, if you would, with the committee.

Mr. MILLER. Thank you, Chairman Thompson. Well, I mean, I think Robert covered well what—the way that the task force has looked at it. You know, I don't want to prejudge the next phase of the task force's work in this regard, because we do believe that significant legal analysis is needed to, you know, examine these barriers and how they can be adequately removed.

I mean, I think a couple of things that are important to note, you know, again, clearly, as I think all the witnesses have already indicated, it is actually a much more complex set of threat information that needs to be shared in some ways, or at least more diverse than in the cybersecurity threat indicator sharing context from the 2015 CISA that was passed by Congress.

Then I think the other thing that is important is that, you know, if we look at—I think some of these issues will be answered through implementation of some of the current policy initiatives that I think you mentioned in your opening statement. For instance, the Secure Technology Act does provide Federal Government entities with the authorities to remove or exclude certain suppliers. You know, that is one of the things the FASC is working on now. Importantly, in that piece of legislation, there were important due process and other types of provisions that were built into that process to kind-of guard against some of these potential legal challenges.

Chairman THOMPSON. Mr. Kolasky.

Mr. KOLASKY. Sure. On top of the FASC, let me make 2 points.

No. 1, you know, we want something in place to encourage private-sector firms to share information about things they might not have trust in, based on due diligence work they do. I think that is an area where, to Robert and John's point, we need to expand the ability to do that.

Within the Federal Government itself, a lot of time we will derive this information through intelligence or other analysis that we are doing. We will—when we derive it through intelligence, we will do—we do a pretty good job when we—there is intelligence out there to get that information in the hands of owners and operators who make a decision. We want to expand our ability within the Federal Government to get it in the hands of the procurement officials within the Federal Government, and that is what we are working on within the FASC, to stand up a better information repository so that we know about threats that could be in the supply chain.

Then, to the point John just made, when we are ready to take action, we want to make sure there is due process and we are respecting fairness in everything. We lived through this through the Kaspersky Labs software and the operation directive that DHS issued. That withstood a court test. We built the case of evidence, and we indicated to the private sector and State local governments that we had taken these steps as a Federal Government, that we didn't trust this stuff on our systems. We couldn't tell them not to buy it in their systems, but I think our indicator was very important.

I think some of the FASC authorities will allow us to do that in a more streamlined process, and make sure that that information gets out there. If we are making a trust judgment for our own systems, we want others to know in case they want to make the same trust judgment.

Chairman THOMPSON. Thank you very much. I yield to the Ranking Member for 5 minutes.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. Kolasky, how do you think the supply—your task force's efforts are lining up with similar efforts across the rest of the Federal Government?

Mr. KOLASKY. Sure. We—as Rob and John mentioned, we have an inventory of other activities going on across the Federal Government.

In the critical infrastructure sectors there are 3 sectors that are really taking some steps on supply chain risk management that we are integrating with: The energy sector, particularly the electricity sector; the health and public health sector; and the defense industrial base sector that DoD is working on.

I co-chaired the Government coordinating councils with other sector-specific agencies, and so it is a good opportunity for me to make linkages for other critical infrastructure work. A lot of that is less about ICT systems and more about component pieces to actually deliver the mechanisms of the functioning infrastructure. Call it the operational technology for that. But we are coordinating cross efforts and looking for synergies there.

Then, you know, there are other efforts across the Federal Government that are important that we are integrating, particularly that the Department of Commerce is taking through the Executive Order. We are the decision support to help the Secretary of Commerce make decisions on potential actions taken through IEPA on that. So, again, the task force is providing key input to the Secretary of Commerce that he will then ultimately implement through the regulatory process. So that is a linkage.

Then there is some software bill of assurance work that Congress is working on that——

Mr. ROGERS. You made reference to the DoD's efforts. The DoD is requiring that supply chain risk management certification be required for many of its contracts—to participate. Would something like that be recommended for the DHS?

Mr. KOLASKY. So yes. So what DoD is doing there particularly is, you know, the big prime contractor is driving down deeper into supply chains, in that—the CMMC tool and some of the work they are doing is to drive down deeper into supply chains.

I think it is fair to say that the task force is interested in learning more about that effort, and is still at the point of evaluating, and, in DHS's opinion, will be informed by some of the task force evaluation. We actually have—the team is working on CMMC. Katie Arrington and her team are coming to brief the task force, and are meeting next week on the 25th, to hear more about the CMMC process so that the task force can learn more, ask them questions, and ultimately will deliberate on, you know, the value, and is there any application in the broader civilian ICT space.

But I do—I don't want to prejudge, you know, task force members' evaluation and opinion.

Mr. ROGERS. Mr. Miller, you made reference in your—at the end of your remarks about recommendations that we try to incentivize other countries to be as vigorous on this subject as we are hoping to be. How do we do that? How do we—we can't make another country do anything. How would you recommend, or—do you all plan to explore ways to recommend to us that we incentivize other countries to be vigorous in their policing of this topic?

Mr. MILLER. Thank you for the question. I don't think it is necessarily just about incentivizing other countries. But, you know, I made reference to the Prague principles on 5G security, for instance.

I think, you know, Step No. 1 is making sure that countries—that the United States is talking with other countries, particularly, you know, its other partners in the case of the Prague principles, as well as having most of the European nations—you know, you had countries like Australia, Israel, Japan, other—you know, Canada and other like-minded nations.

You know, and I think, just as is the case, for instance, as we were talking about with respect to information sharing between private and public-sector actors in the United States, countries like the United States and other allies sharing information can help inform kind of a coordinated policy-making approach.

I think it is—so I think it is about getting people on the same page. You know, that said, there will always be a need for contextual fact-based analyses when we are talking about risk management. It is possible that other countries don't necessarily always see eye to eye with the United States. But, you know, we should continue to do what we are doing, which is talking, and trying to share our intelligence and insights in this matter.

Mr. ROGERS. For any one of you, just give us a very simple example of how a bad actor—because all of you made reference to 5G. We hear a lot about it, and how it is going to change things, how we have to be very careful about it. Give us an example of how a bad actor could penetrate and exploit 5G to our detriment, commercially or governmentally, either way.

Mr. MAYER. So when you think about 5G, it is an evolution beyond the existing 4G in some very substantial ways. The architecture of the networks changes fundamentally. You have much more computing power, intelligence at the edge. You have a much broader variety of participants in the ecosystem, even more than you have right now. Software is going to be a big factor, because these are going to be software-defined networks that are going to constantly be upgraded.

So what you have is, essentially, more vectors where attacks can take place.

Now they are—we are building into the architecture security by design. This is the first generation of wireless where security by design is being embedded from the very beginning, and there are bodies working on that. Having said that, there are capabilities that will help us defend, but we can also expect, I think, more attacks.

So what makes it very important here is that the nature of the 5G environment is going to touch on all critical infrastructures. It is going to touch on, you know, key things like medical supplies, logistics vehicles, things that we can't even imagine yet. You know, a determined and persistent bad actor is going to look for every vulnerability.

If they don't find a vulnerability today, they will look for it again tomorrow, and they will use automated technologies to do that. You know, just like we use artificial intelligence and machine learning into our defensive capabilities, the bad guys are going to use the same technology. So we are now in a very dynamic kind of battle between those two opposing forces.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for being here today, your testimony.

Director Kolasky, I am glad you mentioned that you are following and tracking the work that DoD is doing on supply chain vulnerability identification and risk management.

I serve as the chair of the Subcommittee on Intelligence, Emerging Threats, and Capabilities on Armed Services. Of course, we track the Department's efforts to address supply chain security risks. The forthcoming cybersecurity maturity model certification, I believe, is one way that the Pentagon hopes to mitigate some of the data security risks that they face in the defense industrial base.

So one of the essential steps, of course, in supply chain risk management is actually understanding the dependencies underlying a function. My understanding from the CMMC is that a good deal of the value will come from helping to illuminate supply chain. So what approach is the NRMC taking to illuminate supply chains that support the National critical function set?

Mr. KOLASKY. Sure. Thanks, Congressman, I appreciate the question.

So you referenced at the end the National critical function set. So one of the things, the first things we did as a National risk management center, was identify 55 National critical functions that are things that critical infrastructure produces that are absolutely essential to National security, economic security, and community health and safety. Those National critical functions include things like conducting elections, and the provision of position and navigation timing services, and the provision of wholesale payment services, and the communications core network, and communicating wirelessly.

So that is our overall risk architecture that we were designed as part of our assessment that we did per the EO that the President signed in May of this year. We looked at the critical functions associated most prominently with the communications in the connect function, the things that allow us to be connected as a country. We started to map out.

You know, what are the elements and sub-elements of the supply chains?

What enables those critical functions to work?

What are the elements and sub-elements of the supply chains?

Should any of those sub-elements fail, what is the criticality at a National security, National economic security perspective?

So we did that kind-of initial analysis to prioritize areas where we think that most likely—most critical in a communications supply chain, because they support essential functions that we need as a country.

Mr. LANGEVIN. But you are not just confining your work to ICT. You are looking across the broad spectrum of critical infrastructure, correct?

Mr. KOLASKY. Across the work we are doing at the Natural Risk Management Center. Yes, there are things—you know, operational technology type things, there is work—again, position navigation, timing, finance, election security. Those are key functions. Ultimately, there could potentially be key supply chain vulnerabilities within all of those functions.

Our analysis structure is going to allow us to build that out, understand the sources of criticality. Then, ultimately, when you get to the critical elements, that is when you start to look at what actually is going into those supply chains. How diverse is the market? Who are the key providers? How interconnected is the market; how could it——

Mr. LANGEVIN. Yes——

Mr. KOLASKY. So we are taking that approach, so that we can then start to study particular use cases to help make decisions of the importance of trust there.

Mr. LANGEVIN. What about the private companies themselves? How are you dealing with them? They may not know their supply chains and their supply chain vulnerability risks.

Mr. KOLASKY. I mean, I think that is part of what we are trying to do in this general awareness as part of the task force. I think John and Robert, for the most part, represent companies who recognize the importance of knowing their supply chain have to drive toward knowing that. I think—and they can talk a little more to how advanced the discipline is getting.

There will be private companies who haven't done that work. You know, a lot of what we are trying to do in CISA is to support—develop tools and offer technical assistance to help make sure that there are easy ways to understand your supply chain——

Mr. LANGEVIN. All right. So before my time expires, you are turning to threat assessment. Can you expound on the cyber intrusion techniques that are most worrisome to you?

You know, the supply chain, cybersecurity vulnerabilities take many forms. In the Target breach, for instance, it was connections to the HVAC contractor's network. Petya leveraged a hijacked software update from a Ukrainian tax company. Some of their—of the vulnerabilities we have talked about today are rooted in hardware.

So these vulnerabilities all have different mitigations. So what metrics does NMRC use to evaluate vulnerabilities, both specific examples or classes of vulnerabilities?

How do you prioritize mitigation efforts based on these metrics, if at all?

Mr. KOLASKY. Sure. So I think the metrics associated in vulnerabilities, turning vulnerability metrics into risk metrics, which means understanding the consequences of how the vulnerability could be exploited. So if you look at the question from sort-of a philosophical approach, it is really turning vulnerability metrics into risk metrics.

To your question of which ones concern me the most, you know, it is a dynamic environment, so it is hard to answer that quickly. But what I would say is the things that people don't have any reason to look for. Right? The places where there is already trust inherent in the—inherent in what is going on, that something has not thought twice that there might be a vulnerability, that it was bought by a company they trust, or it is been serviced by an insider.

If those—if we allow people into supply chains and things that are inherently—we think are inherently trustworthy, it is going to be harder to find those vulnerabilities. That is what we are worried that the adversaries are going—some of this is through foreign investment. Some of this is through other sort-of counter-intelligence means. Those are the ones that keep me up at night.

Mr. LANGEVIN. I know my time has expired, but I know Mr. Mayer has something.

Mr. MAYER. Just real quickly. There were almost 200 threats that were identified and put into categories. They ranged from everything from interdiction of the supply chain to human activity that could be both malicious or non-malicious.

One of the things that I think is interesting is that you have to look at the supply chain in terms of different stages. So it goes from design, development, production. Then it gets, you know, acquired, it gets distributed, gets deployed, then it has to be operated and maintained, and it has to be disposed of. So all of these ICT products and services have this life cycle to them, and you can have the threat at any particular point in that process.

What we want to do, I believe—and hopefully in Year 2, and we are discussing it now—is provide a framework that gives some guidance to companies so that they can understand, look, I can't deal with 200 threats and track that every day. How do I prioritize this? How do I—where do I get the information that is going to be valuable here? Who can I coordinate with in terms of mitigating the risk?

Ultimately, where we want the task force to go is to provide real, concrete, practical risk mitigation, you know, practices and information, so that it can—we can start affecting the—buying down risk, basically.

Mr. LANGEVIN. OK. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from New York, Mr. Katko, for 5 minutes.

Mr. KATKO. Thank you, Mr. Chairman. Thank you all, gentlemen, for being here today.

I was a 20-year Federal organized crime prosecutor, and I never made a case of any significance without a task force. A task force for Federal, State, local, and sometimes private components. I recognize the value of it. Sometimes they work better together, sometimes they don't. But it is clear to me from your testimony that it is working, and I am really glad to see that. Public-private partnerships are really a wonderful thing to hear. It is good that you are exchanging information.

I appreciate some of the barriers that you are experiencing, but your goal, as part of your task force, I hope, is to identify how to get past some of those barriers, especially with respect to exchange of information. Because exchange of information is everything in a task force, and the success of a task force. So I appreciate that.

That is one of reasons why a bill that was passed out of committee recently I hope gets passed out of the House to form a CISA advisory committee overall, because I think it is going to be very important.

I want to talk to you about best practices in supply chain management. There is clearly an incentive, from a legal standpoint, to do it because, as best practices become more apparent, there is also liability or exposure for companies who don't utilize best practices. But instead of trying to solve a problem in a courtroom, I would like to see if we could solve the problem by incentivizing companies.

So I wonder if any of you can talk to me about anything you have discussed within the task force about incentives that may be—that you might be recommending with respect to supply chain management practices.

We could start with Mr. Mayer, since you are nodding your head.

Mr. MAYER. So I would say that, you know, we have a very interesting group of participants. So you have some companies who are global leaders in brand management and have very sophisticated activities around protecting the value chain. They have every incentive based on market activities to make sure that their supply chain—the integrity of their supply chain.

One of the conversations that we have had in the task force—and in some—it relates in part to what DoD is doing with respect to their CMMC and their efforts to create, you know, higher levels of assurance in the smaller companies. But we have also talked more generally about the group of companies. The small and medium business organizations clearly do not have the kind of resources that these global communications and IT companies have, yet they can be very impactful from a supply chain, especially as they provide products upstream.

I think we are going to have to grapple with this—it came up in yesterday's meeting of the co-chair leaders—to make sure that, as we think about how we move forward with information sharing, threat evaluations, the development of qualified bidder lists, and things like that, that we keep in mind that there are certain companies that are going to be very successful in this space and have very sophisticated capabilities, and there are other companies that don't have the financial resources, the human resources to implement these capabilities.

I think DoD is going to discover some of that as they implement the CMMC. That is just a societal problem we have to deal with, and we have to think very carefully about the kinds of incentives—cybersecurity generally, but supply chain, in particular.

Mr. KATKO. Have you come up with any incentives yet that you have you have talked about or bantered about?

Mr. MAYER. We have bandied about many ideas. I mean, this goes back to the Executive Orders in President Obama's administration, where he wanted departments to look at incentives.

My view is that nothing ever really came out of that effort. I think we have to revisit that. Incentives take—require money, and there is a great deal of complexity in administrating it. Some companies don't want incentives. If you give incentives to some company, are you tilting the market dynamic in some way? So it is a complicated question.

I think it is something that industry and Government should work closely with Congress on and think through. I think we are getting to the point in time where we need to think——

Mr. KATKO. I would ask you to do that. I think it is very important. I had a roundtable discussion back in my district, and it is clear to me that the smaller businesses just don't have the financial capacity, and they make value judgments every day and—of where to spend their money, and they are just not prioritizing this the way they should. That is a big concern to me.

So, Mr. Kolasky, part of the Secure Technology Act's requirement in their strategic plan was that DHS come up with some sort of incentives, some ideas of some incentives. Have they done that yet?

Mr. KOLASKY. So I would frame it this way, that the way the procurements have been done in the Federal Government for a while, incentives have been around evaluating contracts from a current cost performance schedule incentive. What we need to do is reframe cost, performance schedule, and security have to be—and there is a Deliver Uncompromised report that MITRE put together that—they have to be the pillars of a procurement strategy.

It is amazing, as you know, once you put that into a Federal acquisitions process rule, that you have to evaluate security, just like you are validating cost and past performance. That very quickly becomes real incentives. You start to build tools for procurement officials to know how to do that. The companies who are trying to get into the space then have to demonstrate it. It sets up an auditing potential, you know, free-market auditing regime to evaluate things like that, and all that. You see that contract incentives can drive a lot of change in performance doing that in a way and, you know, talking—as we put that in our own contracts, can we share that with other big buyers who are procuring things even at the private sector to use similar language?

I think that is a real—that is going to be a real driver in change of behavior down supply chains.

Mr. KATKO. Yes, I appreciate it. Just keep working on that, because we are looking forward to hearing from you.

Mr. Miller, I know I am almost—I am out of time, but anything you want to add?

Mr. MILLER. I mean I, first of all, agree with everything my fellow panelists said on this. Really, just to highlight the point about the small and medium-sized businesses, you know, I think both panelists have talked about how that is one of the things that I think DoD is trying to get at with their CMMC program.

When we start talking about things—when we say things like 3 or 4 levels down in the supply chain, we are talking about small and medium-sized businesses usually, right?

I mean, I think just the numbers themselves, just to kind-of put a fine point on how important this issue is, I am not sure what the latest statistic is from the, you know, Small Business Association, but it is something like 90 to 95 percent of companies in the United States for small and medium-sized businesses. I think DoD has something like 90,000 contractors and 300,000 subcontractors. Most of those companies are small and medium-sized businesses.

So, as Robert said, one of things we talked about yesterday was the importance of kind-of integrating the, you know, this notion of incentivizing, you know, SMB practices, or just at least trying to consider the SMB dimension of everything we are doing, because we have a lot of large companies in the task force that are doing really good work. Again, they are not perfect, either. But, you know, figuring out how to get down deeper into their supply chains, into the Government supply chains, is really the key.

Mr. KATKO. Yes, I think it is critically important to examine this issue, and I ask that you do that and report back to us in a timely manner.

With that I yield back. Thank you, Mr.——

Chairman THOMPSON. Thank you. The Chair recognizes the gentleman from California for 5 minutes, Mr. Correa.

Mr. CORREA. Thank you, Chairman Thompson, for holding this most important hearing. As we all know, technology is rapidly evolving, and that is why cyber threats is a major challenge to all of us.

You know, as I listen to this conversation, this discussion, I am reminded of a story I read back a couple of decades ago. The Iraq War. I read the story where it talked about how the United States made Xerox machines that were being used in Iraq. We essentially put chips in those Xerox machines that were—at the right time we were able to activate them, and they caused all kinds of headaches for the Iraqis and their defense system, which helped us have a competitive edge when it came to winning that war.

I guess you look back at that chapter and lessons learned, and now we are talking about 5Gs, you know, infinitely more complex, a whole lot more players. In your words, the number of vector threats growing exponentially. Trying to figure it all out.

I would ask—supply chain trustworthiness.

You, Mr. Miller, just talked about the small businesses. I agree, gentlemen, that we have to go with those that we trust. At the same time, we are looking at the lowest-cost producer of a chip, lowest-cost producer of something out there.

So where do we start, or where do we keep going in terms of making sure that, you know, first of all, if—try to make sure most of those chips, most those products, are made in the United States. But even if they are made in the United States, God knows, how do we prevent a lot of those chips and a lot of those things from being put in our systems that can come back to haunt us? Open question to all of you.

Mr. MILLER. Sure. I mean I think—I think that's a really good question. You know, I mean 2 things I would say on that.

You know, No. 1, as we have mentioned a few different times, we did have a threat assessment group looking at this issue. It was nearly 200 threats. I think 188 different threats were cataloged and divided into 9 different categories.

I think it bears noting that only one of those categories was—you know, really involved cybersecurity threats. I mean, again, there is a whole bunch of other different types of threats, as if it wasn't complex enough that we have to deal with—when we are talking about global supply chains.

Country of origin was also—is also just one of 188 threats. So I think it highlights the importance of really basic risk management principles, and always thinking about, you know, how do we conduct a fact-based, context-based analysis of these various different multiple threat vectors?

You know, it includes the entity and the supplier, of course. But also, what is the——

Mr. CORREA. Let me flip that around.

Mr. MILLER. How is it used?

Mr. CORREA. Let me flip it around. I am almost out of time here. But Mr. Katko talked about incentivizing. How do you keep the—continue to work with small businesses that may not have the resources to have so many guards up, so to speak, security-wise, and at the same time we value their entrepreneurship. They are incentivizing, coming up with new technologies. How do you work with those folks? How do you make sure that they are part of this system, they are secure, and they keep us moving to 6G?

Mr. MILLER. Well, I mean, really quickly, one way, for instance, is that, you know, larger companies can—you know, they often have trusted supplier programs or something, and they can—or they can flow down requirements, you know, even to, for instance, do something as simple as—or maybe not as simple, but something like using the cybersecurity framework into their contracts as a way of trying to incentivize those companies to do that.

But there is a host of other incentives that could be explored, as well.

Mr. CORREA. Gentlemen, any other comments?

Mr. MAYER. So I know how we are not going to make progress. I always think of, like, regulation, technology, and markets. This is evolving too quickly. It is too dispersed for——

Mr. CORREA. It is not regulation.

Mr. MAYER. It is not regulation.

Mr. CORREA. Not legal, but it is—what is it?

Mr. MAYER. Oh, so it is a combination of one—as technologies advance, hopefully they become more functional in this respect, and cheaper, as it is more broadly adopted, so you have capabilities to address supply chain risk.

But the most important aspect, I think, are how can we make markets drive some of this.

So for a large company that has a supply chain, a diverse supply chain that has to guarantee their brand, they can do that through contractual arrangements. They can do that by requiring audits, attestations. There are all kinds of mechanisms. They have to provide some discipline to the people who provide markets there.

I think that this issue is going to get continued visibility in society writ large, and it is going to get to the point where there is going to be a standard of care around protecting the supply chain. It is just going to emerge naturally as part of business. There are going to be players who are going to take serious consideration of how to manage their supply chain risk. Those that don't, they are going to find themselves vulnerable to either reputational harm, or potentially other kinds of, you know, legal or regulatory considerations.

So I am hopeful that the markets and technology and the work that we are doing in the task force, by thinking about how to make it possible for some of these companies to be more effective, is the way we can have some success here.

Mr. CORREA. Mr. Kolasky.

Mr. KOLASKY. Sure. The question brings to mind a couple things, right? There is processes to subsidize small businesses for a lot of reasons, and there is some responsibility, I would say, on the vendor side, if they are buying chips and there is only a couple of sources of chips, to perhaps use some of the resources to make sure that there is security at that level. So, you know, I would hope that the market would see some incentive to helping small businesses.

But then there are ways that we have, as a Federal Government, have subsidized small enterprises for a lot of different reasons, partially because they are a key source of innovation here. I do think, you know, if this—you know, depending on—if this gets too unbalanced, thinking about ways that the Government can subsidize some security practices, we certainly are building tools to help small businesses who want to take this seriously so that they don't necessarily have to go buy those tools from the market to get better at cybersecurity. We will help the assistance. But, you know, there may be a point where it gets out of alignment and some version of subsidization is necessary.

Mr. CORREA. Thank you, Mr. Chairman. I yield.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from Texas, Mr. Crenshaw, for 5 minutes.

Mr. CRENSHAW. Thank you, Mr. Chairman. Thank you, everyone, for being here.

Earlier this year my staff met with Intero Solutions. It is a company that uses artificial intelligence to evaluate supply chain vulnerabilities. Their program found some interesting issues.

For instance, with—the F–35 at tier 2 and tier 3 components have 22 percent and 72 percent Chinese-manufactured parts, for instance.

Closer to what you might deal with in DHS they also found that, within our voting systems—I think there is only 3 companies that actually—3 vendors that actually make our voting systems here in America, and 19 percent of those components in the tiers 1 through 3 had supply chains that came from China-based companies.

Almost 60 percent of companies studied have supply chains and locations in China, Russia, or China and Russia. Even worse, some of these companies included awards from the NRTA, which is China's State-run censorship organization.

I just want to get a sense from you, Mr. Kolasky, on how CISA deals with this.

Mr. KOLASKY. Sure. I can take this question from a number of angles. I will try to take them from 3 different ones.

No. 1, Intero does participate in the task force, and is a member of the task force, within that.

We have looked at Intero's tools. That kind offering, whether from them or someone else, does a good job of scraping together publicly available data that is just hard to aggregate without taking advantage of machine learning and technology, and providing areas that you might want to do a deeper dive.

I don't think—and I think if Jennifer was here—wouldn't tell you that they are absolutely right in those statistics, but those statistics start to narrow it down in cause for areas of—for deeper exploration. So we look at tools like that as a good way to get closer to evaluating risk.

I am familiar a little bit with the election work, and—familiar greatly with election work. We are doing a little bit of what Intero studies. The three companies you reference—Dominion, ES&S, and Hart, you know, are all companies we do business—we work with as part of our election security efforts.

I can tell you that this has been a subject that we have had conversation with in the Election Subsector Security Council. I know that the companies are increasingly aware that there may be supply chain threats, and are looking deeply at their own supply chains to start studying, including some of the companies have actually gone out and inspected the factories that are providing key components of that to try to have a better sense of the provenance of the component pieces that they put in.

I won't say for any certainty, you know, the exactness of this, but it is an area where the combination of a technology like that to help illuminate a supply chain, and then good supply chain risk management, and actually going out looking and seeing is there any reason to be concerned, the businesses are doing that. We at DHS stand ready to work with them if you are finding areas of concern and, you know, maybe push certain things out of election supply chains.

Mr. CRENSHAW. Yes. I mean they—well, let's say the technology is half right. You know, it is still a pretty big concern. Like you said, it points you in the right direction.

How much are we just relying on those companies to actually investigate their own supply chains? What is the relationship between them and you all to make sure that they do, and that our election machines are safe for the 2020 election?

Mr. KOLASKY. Sure. Again, we have a good information-sharing relationship. You know, a couple of those companies, at least, we tested some of their equipment, the key equipment within a supply chain. So we have done some testing at our Idaho National Lab.

So, you know, you are, in theory, worried about supply chains. But then, ultimately, it manifests itself—is there actually a vulnerability? If you get to sort-of a lab testing, you can actually test do any of those vulnerabilities manifest itself.

I don't want to say, you know—we can't be in a position where say, oh, you bought something from this country, and therefore, inherently, somehow the whole system is going to collapse. That is not realistic.

Mr. CRENSHAW. Right.

Mr. KOLASKY. You have to understand where the sources of that material influence——

Mr. CRENSHAW. In my limited time—that actually gets to another question on the DJI drones. Are you familiar with that entire situation? What is DHS's take on DJI, and whether those drones are safe to use?

Mr. KOLASKY. We have provided a couple guidance of concerns that we have with drones manufactured in China. We put out 2 public products. We think there is potential, if mitigation has not been put in place, that there could be information leakage through the drone process. We have some recommendations that we think can effectively mitigate the actual information leakage from the drone.

So we are not at a point where we are saying don't use drones from——

Mr. CRENSHAW. Does DHS use any of those drones?

Mr. KOLASKY. I don't know, off-hand——

Mr. CRENSHAW. Border security or anything?

Mr. KOLASKY. I don't—yes, we don't—CISA doesn't operate drones. So I don't know off-hand. We can get back to you on that one.

Mr. CRENSHAW. All right. I yield back my time. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentlelady from Florida, Mrs. Demings, for 5 minutes.

Mrs. DEMINGS. Thank you so much, Mr. Chairman. Thank you to all of you for being here with us today.

Mr. Kolasky, once again, the committee is holding a hearing against the backdrop of major departures and leadership shakeups in DHS. How are you working to make sure that the NRMC and this task force, in particular, is staying above the fray?

Does the NRMC have the support it needs to carry out its mission during this very critical time?

Mr. KOLASKY. I would cite a quote Mr. Mayer gave to Inside Cybersecurity yesterday about our ability to stay above the fray, and I will let him paraphrase the phrase, but it is a serious question.

We have had support consistently through the Secretaries and Acting Secretaries that have served this administration, including Acting Secretary McAleenan. CISA has been—I think this is paraphrasing Robert's quote, to some extent—we have had—sorry, we have had really good consistency at the political leadership level, starting with Chris Krebs and down there.

So we have been—I can say, as somebody who has been a part of, you know, 3—now 3 Presidential administrations in the Department, you know, the consistency has allowed us not to have to change any direction based on any change of leadership at the more senior level, at a strategic level.

You know, we will see what happens with the successor to Acting Secretary McAleenan. But at this point we expect it is full speed ahead with the work of the task force.

Mrs. DEMINGS. So with the consistent support that you talk about, that does not necessarily include the more senior level.

What concerns you the most, though, about the changes in leadership, and how it affects your—could affect your operation? What are you preparing for as you await the next——

Mr. KOLASKY. Yes, I am—I mean I am human. Any change of leadership, you know, you want to be responsive to that.

I am not expecting that a change of leadership at the DHS Secretary level is going to drive a change in how we approach supply chain risk management or risk management for critical infrastructure. Obviously, we serve our leadership to some extent. But, you know, I can say that we have had consistency, and we expect consistency going forward. We are not planning to adjust our plans based on having a new Acting Secretary.

Mrs. DEMINGS. Then you don't need one? You know, that is not really a serious question.

Mr. Mayer, since he interjected you into his answer, would you like to speak for yourself on——

Mr. MAYER. Oh, thank you.

Mrs. DEMINGS [continuing]. Staying above the fray?

Mr. MAYER. Yes. So I appreciate that. So I think what I said was that the system was operating on all cylinders, and that the public-private partnership with DHS has never been stronger. I really believe that.

I have had 10 years of working with DHS, and I have seen it evolve over these many years to the point where we are now having a level of engagement, bringing subject-matter experts to the table, DHS is listening. We are listening. We are developing products that reflect a great deal of collaboration.

Most recently, for example, the 80-day criticality assessment that had to go into the efforts on the—we are having those discussions on 5G, we are having those conversations on National critical functions.

Going back all the way, I think, to Secretary Kelly and some of the changes that have existed at the top levels, I have not observed anything that suggested that it is either a distraction or disruption.

Mrs. DEMINGS. Perfect. Thank you. To you or to Mr. Miller, it appears the task force has focused on the issues of hardware to our ICT supply chain. Can you describe the work—either one of you or both—that has been done to secure cloud-based storage and applications in the process?

Mr. MILLER. Excuse me. Just to clarify the question, are you asking about cloud in the context of the task force?

Mrs. DEMINGS. Yes.

Mr. MILLER. I don't believe that the task force has worked on cloud, specifically, other than in the context of the broader, you know, threat assessment work.

But, you know, more broadly speaking, I think it—you know, talking about cloud does highlight one of the points that I made earlier, and that is about, you know, data access and managed service providers and other cloud providers are, you know, a really important part of the conversation right now. So, you know, it is definitely a focus area, and I think a future focus area of our work.

Mrs. DEMINGS. Mr. Mayer, anything to add?

Mr. MAYER. The only thing I would add is I don't think how you can think of the supply chain in the context of ICT and not give a lot of consideration to cloud, because a lot of the services are moving there.

The other point that I would make is there must be—you know, I would go through the list of the 40 companies. I would imagine a good number of those companies either rely intensely on cloud capabilities, or provide those services themselves. So I think it is kind of being built into the thinking, as it should be, because you cannot talk about this ICT ecosystem without thinking about how much of the—how big a role the cloud is having.

I would also say that, from a security perspective, I think the cloud has been very instructive in terms of how well we have been able to defend it. I think the lessons we learn from cloud security are going to be easily applied to the 5G environment, which is going to be very helpful.

Mrs. DEMINGS. OK, thank you.

Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much. The Chair recognizes Mr. Taylor for 5 minutes.

Mr. TAYLOR. Thank you, Mr. Chairman.

Chairman THOMPSON. Or less.

[Laughter.]

Mr. TAYLOR. Thank you, Mr. Chairman. I will be brief. Just looking forward to the next—to the future of the task force, what are some of the primary areas that you think you will focus on in the future, Mr. Kolasky?

Mr. KOLASKY. Sure. I mean we will start by continuing the work of the working groups, some of the information-sharing threat evaluation work that we have talked about, and particularly pushing further on guidance around QBL, qualified bidder lists, and qualified manufacturer lists.

So we want to come back with, I think, on information sharing, some tangible recommendations, the changes that need to be made to facilitate information sharing on threat evaluation. We want to come back and work on what I call sort-of a reference guide on risk mitigation. How do you mitigate risk against threats that are of particular concern to your supply chains? So that is going to be the principle area that we start with.

We have talked about some other ideas, and we are in the deliberating process. I think there is an opportunity to bring some of the work going on in other critical infrastructure sectors and connect that. There is an opportunity to make additional connections across the Federal Government. Part of that will then be to influence the implementation of the FASC strategic plan, the Federal Acquisition Security Council strategic plan.

So Year 2 we are going to have a tighter linkage, now that the Federal Acquisition Security Council has worked through the sort-of forming—storming and forming stage, tighter linkage around that.

Mr. TAYLOR. So nothing I heard there would indicate a need for statutory changes or statutory assistance that—you would come to the committee and say, "Hey, we need the law changed here, here, and here," or did you just not mention it?

Mr. KOLASKY. No, I mean, I think you have heard here information sharing and incentives are 2 areas where I think, ultimately, we may come back with some recommendations of current statutory gaps that allow us to push in those areas.

We don't think we need codification to operate as a task force, or to get people to the table, things like that. The critical infrastructure partnership authorities that already exist have enabled us to do that.

So I think we are in a good place, as a standing with the task force, but there may be recommendations that—around incentives and information sharing.

Mr. TAYLOR. Looking forward to those recommendations.

Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much. Let me thank the witnesses for your absolute expert testimony. Your interest and participation in this subject matter is clear.

We are waiting for the next report to kind-of see how far down the road we can get.

Taken from Mr. Taylor, I think there will be some legislative fixes on liability and some other things we will have to look at down the road. I am a little concerned that there is a reluctance to call out a bad actor for fear of being sued, and that might create a vulnerability that should not be. So there is no reluctance on the Chairman's part, and I don't think any other Member of the committee's part that, if we need to do that to secure our systems, that is fine.

The other thing I would like the next time you gentlemen come is to kind-of talk about some of those nation-state bad actors, and what they are doing, and what we are doing to counter them. We get a lot of companies who come to us and say, "Well, we can't really compete in a competitive market, because this company that is winning the bids is owned by X Government." I am trying to figure out if those entities are some of the entities who—the bad actors also in this scheme of things.

So I want you to think a little bit about that, because some of those small businesses Mr. Correa and some of the other people talked about are saying, you know, when companies don't have a bottom line, they can just about compete at zero and win. But I am not—that is not what we want. So I want you to kind-of think about some of that.

I thank you also for your valuable testimony. The Members of the committee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions. Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 11:17 a.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR ROBERT KOLASKY

Question 1a. The ICT Supply Chain Task Force has taken on very complicated issues with respect to supply chain risk management, and its work is on-going. What is the future of the task force?

Question 1b. Does the Cybersecurity and Infrastructure Security Agency (CISA) plan to make the task force permanent?

Answer. The first year of the task force focused on 4 priority areas for supply chain risk management, including Information Sharing, Threat Evaluation, Qualified Bidder Lists, and Qualified Manufacturer Lists, and Policy Recommendations to Incentive Purchase of Information and Communications Technology (ICT) from Original Equipment Manufacturers and Authorized Resellers. In September 2019, the task force released an Interim Report, providing an update on activities and objectives. The ICT Supply Chain Risk Management Task Force also serves as a private-sector engagement point for the Federal Acquisition Security Council.

For year 2, the task force will continue 3 of the 4 work groups with a focus on Information Sharing, Threat Evaluation, Qualified Bidder Lists, and Qualified Manufacturer Lists. It is also likely that the task force will initiate a new working group related to attestation of suppliers and vendor vetting. The task force will continue to allow for industry engagement with the Federal Government on a myriad of supply chain risk management efforts, including the Federal Acquisition Security Council.

The task force is currently operating under a 2-year charter. While no decision has yet been made about future work, there is strong interest across the membership in re-chartering its work beyond that date.

Question 2a. This committee has always supported CISA's work, and has worked to ensure it has the authorities it needs to carry out its mission to defend Federal networks and critical infrastructure. Does CISA currently have all the authorities it needs to carry out its supply chain risk management efforts? Moving forward, do you anticipate that the work of the task force may result in CISA seeking additional authorities?

Answer. We currently have the authorities we need to carry out our supply chain risk management initiatives. The task force is helping us analyze this question and we will let the committee know if we identify additional authorities that are needed.

Question 3a. In the Interim Report it stated that the task force is working closely with OMB and the Federal Supply Chain Acquisition Council to compile a Federal version of your "Inventory of Supply Chain-related Standards & Best Practices." When do you expect that to be complete? How will that information inform the future work of the task force?

Question 3b. Although the work of the task force is targeted at Federal information and communications technology, do you expect the inventory will benefit the private-sector supply chain risk management efforts as well?

Answer. Information for the initial inventory has been gathered from Government sources and is being analyzed for completeness and utility. With a complete inventory, this will ensure an understanding of the range of Federal efforts and help identify where additional Federal work may be needed.

We believe there is benefit to compiling this information, both to help focus the task force on not creating redundant work and also to give a more holistic view of applicable Federal Government processes and programs to help support private-sector supply chain risk management efforts.

Question 4a. It is imperative we secure the supply chain for 5G technology, and I understand there are 5G Network Security and Resilience initiatives under way at CISA's National Risk Management Center (NRMC). Can you speak to what CISA is doing to help secure the 5G supply chain?

Question 4b. How has CISA engaged other agencies, and in particular the FCC, in addressing 5G supply chain security concerns?

Question 4c. What more should we be doing as the country moves toward 5G?

Answer. Cybersecurity and Infrastructure Security Agency's (CISA) 5G work is grouped into 4 areas of effort:

1. Encourage the design and deployment of 5G networks with security and resilience;
2. Promote 5G use cases that are secure and trustworthy;
3. Identify and communicate risks—including supply chain risks—to 5G infrastructure; and
4. Promote development and deployment of trusted 5G components.

As part of those efforts, we have worked with the Information Technology and Communications Sectors to conduct a broad review of the risks and opportunities posed by 5G technology and have publicly posted this risk characterization on our website.

We are maturing our testing capabilities of 5G infrastructure, starting with 5G handset testing with one of our National laboratory partners.

We have partnered with the U.S. Chamber of Commerce and the Competitive Carriers Association on a Rural Engagement Initiative to support the rollout of 5G networks in rural environments. We also are engaging with the U.S. State Department and international partners to a take risk-based approach to trusted 5G deployment around the globe.

Specific to the Federal Communications Commission (FCC), the FCC is an active participant in the task force. We have offered review on the FCC rulemaking related to use of Universal Service Fund for 5G and we stand ready to support the FCC with any analysis that might help with their exercise of their authorities. Finally, CISA participates in Communications Security, Reliability, and Interoperability Council VII, specifically on working groups 2 and 3, which intend to specifically address matters related to 5G and 5G security. We are actively working to enhance the capability of this group.

Question 5a. Part of what has enabled foreign ICT components to become so ubiquitous throughout the Federal supply chain is the desire for less expensive products. Moving forward, how will integrating supply chain security requirements into Federal purchasing requirements affect cost?

Question 5b. Should we anticipate spending significantly more on products with strong supply chain assurances?

Answer. There is a growing consensus that security is now the so-called 4th pillar of Federal acquisition to complement the existing pillars of cost, performance, and schedule. CISA's participation in the Federal Acquisition Security Council and other Federal procurement activities will help streamline and mature the inclusion of security requirements in Federal acquisition of ICT. It is true that there may be additional upfront costs associated with procuring more secure elements of the ICT supply chain, but often much of the up-front costs can be offset by the benefits of having more secure systems, thus limiting the risk of future costs associated with security incidents.

Question 6a. There has been more momentum behind supply chain risk management efforts over the past 2½ years—from the establishment of the Task Force and the Federal Acquisition Security Council to the Executive Order. From your perspective, to what degree have the activities led by the Federal Government stimulated better supply chain risk management practices within the ICT sector?

Question 6b. What more should the Federal Government be doing?

Answer. The activities of the Federal Government are making a difference. Increasingly, many or most discussions around cybersecurity and critical infrastructure protection include some risk calculation around supply chain, third-party, or vendor assurance. Vulnerabilities in supply chains—either developed intentionally for malicious intent or unintentionally through poor security practices—can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system and network failure. Managing risk to the ICT supply chain is a top priority for CISA.

We live in a system of systems world where ICT components—these foundational building blocks of hardware, software, and services—underpin a broad range of critical infrastructure and governmental functions the American people depend upon. We must have trust in these components. They must be secure by design. And their manufacturers should operate without risk of subversion or manipulation by adversarial regimes.

Our engagements with ICT stakeholders largely reinforce a growing recognition that effective ICT Supply Chain Risk Management (SCRM) is not only important for product security, but is also necessary for business and organization resilience, as well as economic and National security. The participation in our ICT SCRM Task Force by 40 of the largest ICT stakeholders is testament to the intentions of those on the front end of developing and producing the connected infrastructure underpinning our digital world are committed to leading in and prioritizing security and resilience in their business decisions. The combination of this work and the utilization of a range of Federal authorities is driving companies to a position of taking less supply chain risk.

Question 7. While it is encouraging to see the membership of the task force include the leaders in each of the Communications and Information Technology Sectors, I am concerned that the voices of small businesses are not part of the task force membership. How are you ensuring that small business concerns are taken into consideration through the task force and its component Working Groups?

Answer. The task force and the respective Working Groups recognize the unique circumstances and needs of small and medium-sized businesses. In fact, CEOs of two small business that produces cybersecurity tools and services sit on the task force and participate actively in the Working Groups. Their perspective has been valuable, and their input has been considered.

The task force is including small business concerns into each of the working efforts and some of the recommendations will be designed specifically to make available more information and capability for small businesses to help them secure their ICT components.

Questions From Honorable James Langevin for Robert Kolasky

Question 1. What responsibility does the National Risk Management Center have for helping to illuminate private-sector supply chains?

Answer. While we cannot compel private-sector action by illuminating our understanding of risk to the Nation's critical infrastructure, we are confident that owners and operators of critical infrastructure can make more informed decisions that make infrastructure more resilient.

In particular, the National Risk Management Center (NRMC) is looking at improving analytics to help illuminate supply chains around three general questions:

1. How big is the risk exposure of particular supply chain elements?
2. Should we demand higher level of assurance in supply chains given the risk exposure?
3. Does the proposed solution give us enough assurance that critical functions to National security are not at risk?

Question 2. If a private-sector entity supporting a National Critical Function does not have a good understanding of its supply chain—or its supply chain risk—are their actions the NRMC can take to get a better understanding of that supply chain risk?

Question 3. What responsibility do sector-specific agencies have to illuminate, or help private-sector organizations, illuminate supply chain risk within their sectors?

Question 4. Does the NRMC have any agreements with sector-specific agencies specific to supply chain risk and efforts to illuminate it within their sectors?

Answer. The NRMC works in a voluntary manner with the private sector to better understand and assess supply chain risk. Our partnership with most of the industry that contributes to the delivery of National Critical Functions helps us understand their supply chain risks, but we are exploring ways to increase information sharing and better understand vulnerabilities and risks. This could lead to new industry-Government partnerships in the future.

Sector-Specific Agencies (SSAs) contribute to this effort. CISA is the SSA for 8 of the 16 sectors and responsible for coordinating the security of critical infrastructure across all sectors. We are driving this imperative across all sectors. We have partnered with the U.S. Departments of Energy, Defense, and Health and Human Services on targeted sector-specific supply chain efforts. The cross-sector collaboration on supply chain risk management remains a priority in 2020.

Question 5. Does the NRMC have any plans to scan, request information of, or otherwise directly illuminate supply chains of entities supporting National Critical Functions, whether using NRMC resources, other intra-governmental resources, or contracts with non-Government entities?

Answer. From an ICT supply chain perspective, we did this as part of our responsibilities under Executive Order 13873. The NRMC utilized a repeatable, qualitative approach, developed in collaboration with the National Laboratories, Government, and private-sector entities, to decompose 7 NCFs into their respective ICT elements (hardware, software, and services). These ICT element classes can then be analyzed for criticality. The NRMC continues to refine its analytical process for supply chain risk management to help build a lasting analytical engine.

In Year 2 of the assessment, the NRMC plans to conduct both deeper and broader analysis across ICT supply chains to better illuminate any risks of concern.

Question 6. How does the NRMC model supply chain risk across the National Critical Function Set? Is the risk modeling quantitative or qualitative?

Question 7. Does the modeling capability support the dynamic introduction of new intelligence? For instance, if a new zero-day vulnerability is disclosed and is actively being exploited in the wild, can risk metrics rapidly be recalculated across National Critical Functions?

Answer. The NRMC uses a repeatable, qualitative approach, developed in collaboration with the National Laboratories, Government, and private-sector entities, to decompose each of the NCFs into their respective ICT elements. These ICT element classes are then analyzed in terms of National security or regional-level impacts, based on assumed compromise of the element. For National-level analysis, the risk assessment accounts for likely compromises, so the overall strategic level assessment wouldn't necessarily need adjustment regarding a zero-day vulnerability. It's the tactical-level operational protocols that would likely need adjustments.

As new intelligence is introduced into the model, our assessment of criticality and threat can change which could cause different risk judgments and priorities in terms of mitigation.

Question 8. What steps is the NRMC and DHS more broadly taking to "promote market dynamism and support existing trusted-vendors in the space while investing in innovation and research and development that will help the trusted community win the quality battle in the RAN, innovate to a future 5G, and compete on a level playing field in the market?" How is CISA working with the interagency to achieve these ends?

Answer. During the current early stage of 5G, CISA is focused on cross-collaboration and awareness until more mature use cases emerge in real-world deployments. We are coordinating with the DHS Office of Science and Technology and other areas of research and development across the inter-agency to ensure technology that will support 5G deployment has proper incubation and innovation stimulated around it. We work with partners to support a consortium of industry vendors to promote interoperability between vendors supporting 5G infrastructure. We also participate in international standards bodies like 3GPP to support a level playing field for American innovation.

Further, we are in close collaboration with the U.S. Department of Defense, as well as several of the National Laboratories, to ensure we are coordinated in the area of research and development. Finally, we are persistently engaged with our European partners through forums such as the Prague 5G Security Conference.

Question 9. What other technologies, besides 5G, are of particular concern to the NRMC?

Answer. Most technologies present strategic opportunities, as well as risk management challenges. For instance, artificial intelligence (AI) enables adversaries to be more automated in their attacks; however, it also empowers network defenders like CISA to be more strategic in the way we defend against cyber threats.

The NRMC also has dedicated resources to the topic of space and terrestrial-based Position, Navigation and Timing (PNT), and the associated technologies that ensure those capabilities. As we assess the National Critical Functions and work to determine the elements in those functions, technologies such as PNT and 5G stand out as areas we want to get ahead of.

Other technologies of interest are quantum computing, smart cities, and associated automation, and advances in the bio-economy.

Question 10. What barriers does NRMC believe exist to effective threat information sharing with the private sector? How do these barriers fall outside protections enacted in the Cybersecurity Act of 2015?

Answer. Potential barriers to effective information sharing with the private sector include those that are legal, process or operational, financial, and reputational. Through the ICT SCRM Task Force, we plan to convene key Government agency and private-sector representatives with specific subject-matter expertise on the legal issues relating to supply chain information sharing barriers and discuss throughout this year. Many of the key issues are related to having more assurance that suppliers can be trusted to deliver secure hardware and software.

Questions From Honorable Dina Titus for Robert Kolasky

Question 1. If, as you say in your testimony, a particular focus for CISA " . . . needs to be on ensuring that State-influenced entities do not dominate a market . . . to potentially do the work of adversary action," how should the United States convince other countries of the risks and vulnerability of adopting Chinese technology? How should the United States work with countries that have already adopted Chinese networks out of economic necessity?

Answer. In our efforts, we are also encouraging all countries to adopt a risk-based security framework for the rollout of 5G networks. We urge nations to conduct a careful evaluation of potential hardware and software equipment, vendors, and the supply chain. It is imperative that the international community renews its efforts to incentivize security in the marketplace and ensure it is a primary consideration, alongside cost, in product development, manufacture, acquisition, and procurement. Earlier this year, the global community made great strides at the Prague 5G Security Conference where officials from nearly 40 countries met to discuss a set of principles on how best to design, construct, and administer secure 5G infrastructure, known as the Prague Proposal. Additionally, the European Commission and member states released their coordinated E.U. risk assessment of 5G security. The assessment clearly identified the vulnerability of 5G vendors or suppliers that could be subject to pressure or control by a third country, especially countries without legislative or democratic checks and balances. The assessment also highlighted the corporate ownership structure of 5G suppliers as a potential risk factor, which aligns with the U.S. assessment and the Prague Proposals' call for transparency. Establishing international cybersecurity norms, like we did in Prague, must continue with our international partners, we must continue to encourage responsible behavior and oppose those who would seek to disrupt networks and systems.

Question 2. How can non-Chinese companies compete with Huawei given that its telecom networks typical cost 20 to 30 percent less than competing products?

Question 3. Huawei is trying to build 5G networks around the world. Why doesn't the United States have any competitors with similar 5G infrastructure?

Answer. American companies can continue to compete in the development of emerging technologies by participating in interoperability efforts, which will allow American companies to more easily incorporate new technologies within existing networks. The Federal Government can continue to support American companies, by limiting the adoption of Chinese 5G equipment that may contain vulnerabilities. Section 889 of the 2019 National Defense Authorization Act prohibits Federal agencies from procuring or obtaining, or extending or renewing a contract to procure certain Huawei and ZTE equipment and services, and the recently-enacted Federal Acquisition Supply Chain Security Act provides the Government with important new authorities to address risks presented by the purchase of technologies developed or supplied by entities whose manufacturing and development processes, obligations to foreign governments, and other factors raise supply chain risks.

Furthermore, Chinese companies, such as Huawei, appear to have benefited from subsidized financing for their equipment sales. Countries should adopt the best practices in procurement, investment, and contracting, and require that financing be commercially reasonable, conducted openly and transparently, and based on free market competition, while taking into account trade obligations.

Within the United States, there are a multitude of companies that will be well-positioned to provide aspects of the 5G network, while there are trusted international vendors that have ample U.S. presence. We believe that a move to a more open 5G architecture will only advance the opportunity for U.S. companies in 5G.

Question 4. How should the United States work with countries that have already adopted Chinese networks out of economic necessity?

Answer. Response was not received at the time of publication.

Questions From Chairman Bennie G. Thompson for Robert Mayer

Question 1. The Business Software Alliance, last week, wrote to Commerce Secretary Wilbur Ross of their disappointment in a lack of public comment before the Interim Public Rule is issued, pursuant to the ICT Executive Order.

How does a lack of input into this Rule impact the Communications and IT Sectors?

Question 2. What is the capacity of the ICT industry to be able to implement recommendations without restricting competition and imposing burdensome costs?

Answer. The rules that will be issued pursuant to Executive Order 13873 will be an extraordinarily significant step in the Government's assertion of authority to intervene in the private-sector supply chain. Unlike other Government supply chain activities (such as various Federal procurement rules and the FCC's proposed restrictions on Universal Service Fund support for purchases from certain suspect suppliers), this Executive Order asserts broad authority to prohibit purely private commercial transactions.

USTelecom and other stakeholders have engaged on these issues with relevant Commerce personnel—namely senior officials and staff from the Bureau of Industry

(BIS), the National Telecommunications and Information Administration (NTIA), the Office of General Counsel (OGC) and the Secretary's office—and we are satisfied that the Department understands the significance of the step they are taking. It is our understanding that the rules will not themselves take substantive prohibitive action against specific transactions, but will instead establish the procedural, jurisdictional, and definitional framework under which such future prohibitions would take place. We expect, per multiple public statements from senior Department officials, that there will be an opportunity for robust public comment on these rules when they are issued.

For the long-term success of this policy, including to ensure positive effects on global competition and to avoid imposition of unnecessary burdens and costs, it is important that the Department receive additional formal on-the-record input from a wide variety of stakeholders in the Communications and IT sectors.

Question 3. Part of what has enabled foreign ICT components to become so ubiquitous throughout the Federal supply chain is the desire for less expensive products.

Moving forward, how will integrating supply chain security requirements into Federal purchasing requirements affect cost?

Question 4. Should we anticipate spending significantly more on products with strong supply chain assurances?

Answer. Integrating supply chain security requirements and acquiring products with supply chain assurances may in some cases increase the costs of some acquisitions, but the Government should endeavor to leverage private-sector expertise in supply chain security processes to advance cutting-edge supplier vetting and security risk management processes that can ultimately create efficiencies—and cost savings—in Federal procurement that may not exist today. While it is the case that some foreign-origin ICT components are less expensive because they have been subsidized by foreign state actors such as the Chinese government to sell at below-market prices, many private-sector buyers are aware of the longer-term security and performance costs that such purchases entail.

USTelecom believes that deep engagement with private-sector expertise on Federal supply chain risk management activities is the primary method for creating efficiencies that will control costs while mitigating risks in the supply chain.

Question 5. There has been more momentum behind supply chain risk management efforts over the past 2½ years—from the establishment of the task force and the Federal Acquisition Security Council to the Executive Order.

From your perspective, to what degree have the activities led by the Federal Government stimulated better supply chain risk management practices within the ICT sector?

Question 6. What more should the Federal Government be doing?

Answer. Further to my answers to the previous set of questions, we commend the Government for its approach to supply chain security risk management—namely in partnering with private-sector experts in developing solutions. This has been mutually beneficial to the Government and to industry. So far as we are aware, the ICT Supply Chain Risk Management Task Force is the only formally chartered industry-Government partnership whose leadership and membership are composed of a 2–1 industry-to-Government ratio. This is how these processes should proceed, because while all stakeholders have a strong interest in the security of the supply chain, it is the communications and IT sectors that have the pertinent real-world expertise regarding how to make a secure supply chain a reality.

To this end, we believe the most important principle the Government can follow in this arena is to promote coordination among and between the various Government and private-sector activities on these issues in various Federal agencies and industry sectors. Additionally, these initiatives must recognize that the relevant ICT markets are global, so to the extent possible, these efforts should be coordinated among like-minded governments world-wide so as to increase the size of the market for a secure supply chain of trusted vendors.

Question 7. While it is encouraging to see the membership of the task force include the leaders in each of the Communications and Information Technology Sectors, I am concerned that the voices of smaller businesses are not part of the task force membership.

How are you ensuring that small businesses' concerns are taken into consideration through the task force and its component Working Groups?

Answer. In addition to large, global companies, USTelecom has many members who are small and medium businesses (SMB) themselves, in addition to serving the SMB community extensively as their broadband service provider. Accordingly, my role at USTelecom has given me a significant appreciation of the SMB security concerns, including overseeing the USTelecom SMB Cybersecurity subcommittee. Further, I serve as chair of the Communications Sector Coordinating Council (CSCC), which takes small/medium business concerns very seriously. One of the CSCC's formal committees is exclusively concerned with addressing the security challenges of small and medium businesses. All of this informs my work as co-chair of the ICT Supply Cain Risk Management Task Force, with guidance from other members and associations who also represent SMB segments. Furthermore, we are now in the process of identifying Year 2 projects for the task force and a proposal is before the voting members to create a new working group that will focus its attention on the unique circumstances of the SMB community and possible incentives that may be required to bring their capabilities to a higher level of maturity.

In short, small/medium business concerns are integral to our work on the CSCC, and also to our work on the ICT Supply Chain Risk Management Task Force. We must develop supply chain security approaches that work for all stakeholders in industry, small and large.

Question 8. It appears that the task force has focused on the issues to the hardware in our ICT supply chain, can you describe the work that has been done to address software concerns?

Answer. Members of the ICT Supply Chain Risk Management Task Force have been active participants in NTIA's Software Component Transparency multi-stakeholder effort. This process has yielded the development of a standard software bill of materials and proof of concept that would increase supply chain transparency across industry. The task force also recently released an Interim Report in September 2019 that provides further details on how task force members are addressing software supply chain concerns, such as providing an assessment of best practices and standards for the software supply chain.

Question 9. What protections does industry feel the task force needs to promote a deeper level of information sharing of supply chain risks?

Answer. One of the working groups on the ICT Supply Chain Risk Management Task Force looked into this issue in some depth, through the lens of the question of how industry and Government could share and/or receive derogatory, supplier-specific information—that is, "naming names" of specific suspect suppliers.

Broadly speaking, a private company's formal or informal sharing or receipt of information regarding a suspect supplier could create the prospect of facing a private cause of action, most likely brought by the supplier at issue, involving an alleged violation of a pertinent commercial agreement or of applicable Federal or State law (either statutory or common law). While certain statutory protections such as those under the Cybersecurity Information Sharing Act (CISA) and the Protected Critical Infrastructure Information Act (PCII) in some cases may be pertinent to these legal risks, these statutes may not fully accommodate the risk information sharing that is envisioned under the task force's work on this matter.

The task force continues to work on this legal challenge, and we believe there are some models in other areas of procurement and law enforcement activities that could provide legal standards and processes that would be applicable here. We would welcome the opportunity to engage with your staff in greater depth regarding these possibilities.

Question 10. As the Federal Government seeks to improve its supply chain risk management policies, how should it approach requesting information from vendors further down the supply chain without being burdensome?

Answer. Similar to my answers to other questions above, we believe the best approach to this question is to leverage private-sector expertise in supply chain security processes to advance cutting-edge supplier vetting and security risk management processes that can ultimately create and advance efficiencies in Federal procurement. Private-sector companies have been addressing these supply chain assurance challenges for years, so deep engagement with private-sector expertise on Federal supply chain risk management activities is the best method for creating supply chain security advances while avoiding unnecessary burdens.

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR JOHN MILLER

Question 1. The Business Software Alliance, last week, wrote to Commerce Secretary Wilbur Ross of their disappointment in a lack of public comment before the Interim Public Rule is issued, pursuant to the ICT Executive Order.

How does a lack of input into this Rule impact the Communications and IT Sectors?

Answer. We anticipate that we will have the opportunity to provide comments on the rules to implement the Executive Order when they are released, whether they are published as an Interim Final Rule or as an Advanced Notice of Proposed Rulemaking. We have engaged with the U.S. Department of Commerce throughout the process to share the perspectives of the ICT sector.

Question 2. What is the capacity of the ICT industry to be able to implement recommendations without restricting competition and imposing burdensome costs?

Answer. Without having seen the text of the Interim Final Rule, it is difficult to make an accurate determination as to ease of implementation or costs. Ultimately any final determination as to these and other issues will depend on what the actual rule as issued says and the process that is laid out with the rule. A flexible framework in which determinations about National security risk associated with particular ICT transactionsare grounded in a fact-based, context-based analysis should allow the ICT sector to implement recommendations without incurring significant cost or burden related to a large majority of ICT transactions.

Question 3. Part of what has enabled foreign ICT components to become so ubiquitous throughout the Federal supply chain is the desire for less expensive products.

Moving forward, how will integrating supply chain security requirements into Federal purchasing requirements affect cost?

Answer. In the absence of a clear set of requirements, it is difficult to make a clear determination. There are a number of factors which might increase the cost and that should be taken into consideration. These include: The number of different supply chain requirements that are introduced across Government, the depth within the supply chain that the industry must certify, the amount of supply chain information that is shared across procurements, the level of customization required for a certain procurement (i.e. bespoke products vs. commercial off-the-shelf products), and the willingness of Government and industry to adopt a flexible model which recognizes that risk is not equal in all procurements. Furthermore, if multiple Federal agencies promulgate supply chain requirements that are in conflict, divergent, or otherwise misaligned in significant respects, increased compliance burdens could no doubt impact overall product costs.

Question 4. Should we anticipate spending significantly more on products with strong supply chain assurances?

Answer. As noted, there are many possible cost drivers. Absent clarity on those factors, and others, it is not possible to provide a concrete response.

Question 5. There has been more momentum behind supply chain risk management efforts over the past 2½ years—from the establishment of the task force and the Federal Acquisition Security Council to the Executive Order.

From your perspective, to what degree have the activities led by the Federal Government stimulated better supply chain risk management practices within the ICT sector?

Answer. The activities led by the Federal Government have helped to shed light on the complex challenges that have emerged from an increasingly connected global ICT infrastructure and supply chain, which has in turn helped to highlight many of the supply chain security efforts already in flight across the ICT sector, as well as increasing coordination and sharing of best practices amongst IT, communications, and Federal Government stakeholders. Many of these positive attributes are highlighted by the work of the ICT SCRM Task Force, which recently issued an Interim Report detailing progress made to date on recommendations across 4 workstreams, plus an effort to inventory Federal activities and ICT best practices. The work of the task force has thus stimulated better supply chain risk management practices within the ICT sector. By bringing together parties from both the public and private sector to work on these issues in a coordinated manner, the task force has created a nexus of public-private collaboration and facilitated increased information sharing regarding supply chain threats and best practices, and this progress will be furthered once the recommendations offered by the task force are implemented.

Question 6. What more should the Federal Government be doing?

Answer. The Federal Government should continue to leverage public-private sector relationships, including the ICT SCRM Task Force, ensuring that information continues to flow openly and allowing for risk to be mitigated appropriately. The Government should look to the ICT SCRM Task Force as a resource that can be used for supply chain efforts beyond the task force itself. Please see my oral testimony for examples of how to leverage the ICT SCRM Task Force moving forward.

While the Federal Government's increased attention on supply chain security has been largely positive, some new challenges have also emerged, including a flurry of policy-making activity that has been difficult for the private sector to keep pace with. ITI recommends that the Federal Government work to streamline on-going supply chain risk management efforts, while striving to avoid duplication of efforts as new activities are undertaken. Coordinated approaches to supply chain risk management across the Federal Government will yield the best, most interoperable results, not only in the United States, but globally. In that sense, future supply chain measures and activities should be targeted to specific identified gaps, rather than duplicating existing efforts of "reinventing the wheel."

Finally, the Federal Government should work to deepen relationships with international partners and pursue a coordinated approach to supply chain security. Global supply chain challenges call for globally scalable solutions and only through continued dialog will we be able to develop such solutions and avoid harmful fragmentation.

Question 7. While it is encouraging to see the membership of the task force include the leaders in each of the Communications and Information Technology Sectors, I am concerned that the voices of smaller businesses are not part of the task force membership.

How are you ensuring that small businesses concerns are taken into consideration through the task force and its component Working Groups?

Answer. The IT sector understood from the outset the importance of small and medium-sized businesses (SMBs) to the discussion of supply chain security, and that is why we made sure that SMBs are amongst those representing the IT sector on both the task force executive committee and voting membership. For your reference, task force participants, including SMB participants, are listed in Table 1 on page v of the Interim Report. Additionally, the larger companies participating in the task force are acutely aware of the concerns of SMBs, who represent the bulk of their suppliers, business partners, and customers. As such, the task force aspires to address the concerns of SMBs throughout our work—for example, the Task Force Information-Sharing Working Group identified key challenges for SMBs to access supply chain risk information and recommended inclusion of an independent counsel to work with the SMBs. It could thus be said that the task force considers SMB concerns to be a cross-cutting priority. That said, in Year 2 of the task force, as well as considering SMBs as across-cutting priority we are considering whether to launch an SMB-specific workstream.

Question 8. It appears that the task force has focused on the issues to the hardware in our ICT supply chain; can you describe the work that has been done to address software concerns?

Answer. The task force has not focused its work exclusively on concerns related to hardware. In fact, much of the work of the task force during Year 1 has dealt with foundational topics, such as establishing a bidirectional supply chain information sharing framework, and conducting an assessment of ICT supplier-related threats, that encompass supply chain information and threats related to the full spectrum of ICT products, hardware, and services, which in the context of many ICT products and services are often implemented in integrated systems.

During Year 2 of the task force, we expect to continue the work of the ICT threat assessment group, and anticipate "phase 2" of this activity to focus specifically on evaluating threats to ICT products (including both hardware and software elements) as well as services.

Question 9. What protections does industry feel the task force needs to promote a deeper level of information sharing of supply chain risks?

Answer. The Task Force Bi-Directional Information Sharing Working Group has identified ways that the Federal Government and industry can share supply chain risk information more effectively. Some high-level conclusions offered by that working group include that supply chain risk information is often available, but that accessing and utilizing the information can often be resource-intensive and must be prioritized based on risk, and that the most relevant or actionable information may not always be generally available, particularly from non-public sources (e.g., audit firms and sensitive/business proprietary information). Further, information sensitivity is another factor, as is the form of this type of information, which is often decentralized and therefore difficult to share readily, securely, and at scale.

Question 10. As the Federal Government seeks to improve its supply chain risk management policies, how should it approach requesting information from vendors further down the supply chain without being burdensome?

Answer. Any request for detailed supply chain information adds work to the procurement process. In order to limit the impact, these requests for information should be made in a clearly-defined manner that is based on the risks for a particular procurement, makes clear how information being requested will help to mitigate the risk, and defines how that information will be evaluated and used during the procurement selection.

○