Testimony

Robert Kolasky
Assistant Director
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

Public-Private Initiatives to Secure the Supply Chain

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

October 16, 2019

Washington, DC

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) ongoing 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* (P.L. 115-278) nearly one 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 U.S.'s 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 cyberspace." 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 Worldwide 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 US 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 towards improving our nation's overall defensive posture against malicious cyber activity. In May of 2018, the Department published the *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five 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 cyberspace. 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 United States Government.

The first year of the Task Force focused on four 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 four 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 nine 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 US 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 six 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 five 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 U.S. 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 3rd 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 nationwide US 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.