Testimony

Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"5G: The Impact on National Security, Intellectual Property, and Competition"

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

May 14, 2019

Washington, DC

Chairman Graham, Ranking Member Feinstein, 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 our telecommunications infrastructure. Thanks to Congress's leadership and passage of the *Cybersecurity and Infrastructure Security Agency Act of 2018* (P.L. 115-278), we are now even better poised to further the maturation of the organization to best reflect our essential mission and role in safeguarding and securing infrastructure from cyber threats.

My testimony today will focus on the deployment of 5th Generation (5G) wireless telecommunications networks. Advances in 5G technology, the Internet of Things, and other emerging technologies are driving significant transformation in how we communicate, operate our critical infrastructure, and conduct economic activity. 5G is the next generation of networks that will enhance the bandwidth, capacity, and reliability of mobile communications. 5G was launched on a limited-basis in the United States and South Korea at the end of 2018, and more countries are rolling it out this year. According to the Global System for Mobile Alliance (GSMA), 5.1 billion people, or 67 percent of the global populations, is subscribed to mobile services. It is expected that 5G networks will cover 2.7 billion people, or 40 percent of the global population, by 2025.

The first generation of wireless telecommunications networks in the United States was deployed in 1982, and its capabilities were limited to basic voice communications. Later generations added capabilities like text, picture, and multimedia messaging; Global Positioning System (GPS) location, video conferencing, and multi-media streaming. 5G networks will support greater bandwidth, capacity for tens of billions of sensor and smart devices that make up the Internet of Things (IoT), and ultra-low latency necessary for highly-reliable, critical communications. According to GSMA, between 2018 and 2025, the number of global IoT connections will triple to 25 billion. Autonomous vehicles, critical manufacturing, medical doctors practicing remote surgery, and a smart electric grid represent a small fraction of the technologies and economic activity that 5G will support. Separately, multiple studies have indicated that 5G networks will enable applications to drive significant technological advances and add $1.2 trillion and three million jobs to the U.S. economy. With advancing technologies, comes increased risk to the Nation's infrastructure.

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.

The concern regarding the growing presence of Chinese telecom equipment is particularly acute in the Radio Access Network (RAN) portion of the network where there are a limited number of RAN equipment suppliers. There are four main purveyors of 5G RAN technology globally, none of which are considered United States-based, and the largest of which is Chinese-based. If Chinese manufacturers, who receive significant state support, 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.

Risks to mobile communications generally include such activities as call interception and monitoring, user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data. Integrating 5G into current wireless networks may convey existing vulnerabilities and impact 5G network security. Data on 5G networks will flow through interconnected cellular towers, small cells, and mobile devices that may provide malicious actors additional vectors to intercept, manipulate, or destroy critical data. Malicious actors could also introduce device vulnerabilities into the 5G supply chain to compromise unsecured wireless systems and exfiltrate critical infrastructure data.

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 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.

Supply Chain Risks

Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232) generally prohibits federal agencies from procuring or extending a contract to obtain any equipment, system, or services, or enter into a contract with an entity that uses any equipment, system, or service, that uses telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation; video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company; or telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the FBI, reasonably believes to beowned or controlled by, or otherwise connected to, the government of the People's Republic of China. The interagency is working to implement the requirements of the act.

The Federal Acquisition Regulations (FAR) Council is developing acquisition regulations. Once those regulations are published, all executive agencies will be required to follow them. With the passage of the Federal Acquisition Supply Chain Security Act of 2018 (P.L. 115-390), the Federal Acquisition Security Council provides a dedicated interagency body to take action on information and communications technology (ICT) supply chain matters for federal acquisitions, inclusive of 5G technologies. CISA is an active participant on the Council, and is working through this and other mechanisms to assist with implementation of the upcoming statutory requirements. The Council will be able to recommend that the Secretaries of Homeland Security and Defense, and the Director of National Intelligence, issue government-wide "removal orders" and "exclusion orders" to address supply chain risks, when necessary.

Additionally, CISA, through the National Risk Management Center, 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, to include the challenges 5G technology presents. One of the lines of effort of the Task Force is the identification of processes and criteria for risk-based evaluation of ICT suppliers, products, and services.

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.

In 1991, at the direction of the NSTAC, the Network Security Information Exchanges (NSIE) were established. Industry and government coordinate through the NSIEs to voluntarily share sensitive information on threats to operations, administration, maintenance, and provisioning of systems supporting telecommunications infrastructure. Government NSIE

members include Federal agencies that useNS/EP communications services, represent law enforcement, or have information related to network security threats and vulnerabilities. Industry representatives include subject-matter experts engaged in prevention, detection, and/or investigation of communications software penetrations. In January 2018, the NSIE facilitated a discussion on 5G technology.

International Engagement

CISA regularly engages with international partners on a range of cyber and communications risks including the Usual 5, or the cyber centers from the United Kingdom, Canada, Australia, and New Zealand; the International Watch and Warning Network, which includes 15 countries; and many other bilateral relationships. The NSIE holds biennial multilateral NSIE (MNSIE) meetings with its members. The MNSIE is a global partnership between NSIEs from Australia, Canada, New Zealand, the United Kingdom, and the United States. In September 2018, the MNSIE was hosted by the United Kingdom's National Cyber Security Center, and a number of pressing topics were discussed, including 5G technology.

Over the last year, 5G security and associated supply chain risk management topics have come up frequently with international partners during both senior and working level engagements. With Five Eye partners, these discussions include both information sharing, strategic alignment on policy approaches where appropriate, and identification of opportunities for collaboration.

Many international partners share concerns broadly on 5G security. Some have effectively banned the use of Huawei equipment in their 5G networks. Others continue internal efforts to formally review the security impact of 5G technology, to include the potential risks of using hardware or software in 5G networks built by companies from certain countries.

National security must be a primary consideration in technological and infrastructure development of 5G technologies. As certain firms of concern, such as Huawei and ZTE, have a significant share of the market for 5G products and associated network devices, efforts to build 5G infrastructure potentially introduces major risks to national security. Security concerns must be considered in any policy action that would promote infrastructure development underpinning telecommunications or cyber ecosystem.

One consistent critical challenge is the lack of comparably priced alternative products from domestic and trusted partner nations, due in large part to the heavy state support that Chinese firms receive. Market incentives are needed to stimulate market growth for trusted suppliers, both to compete internationally and provide viable, cost-competitive alternatives domestically. A fundamental shift in market dynamics is needed to incentivize and cultivate suppliers from trusted sources, otherwise U.S. technological and infrastructure development efforts in 5G will be impeded by lack of viable, trusted alternatives.

Our efforts to cultivate 'trusted foundries' for 5G technologies must proceed in partnership with 'like-minded' countries. Risk could be mitigated in a more effective manner if coordinated in an international effort of like-minded countries to drive the dynamics that could

move the market. This avails 'trusted foundries' with more flexibility and counters the narrative that the U.S. seeks to mimic China's predatory industrial policy approach that seeks to tilt global markets towards domestically manufactured ICT devices.

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 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 specification development initiatives. CISA currently works with industry, including nationwide U.S. wireless carriers, in preparing technical specification to ensure NS/EP personnel will have priority communications services on 5G networks.

DHS's Study on Mobile Device Security, which was required by the Cybersecurity Act of 2015 (P.L. 114-113), identified risks to mobile devices and communications and identified opportunities to make progress on security. The study also called for government-funded research and development and for cooperative agreements with private-sector entities such as mobile network operators and associations, and enhanced U.S. government participation in development of consensus-based voluntary mobile security standards and best practices.

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.

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.