Testimony

Jeanette Manfra
Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"Role of the United States Government in Securing the Nation's Internet Architecture"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES

Committee on Armed Services, Subcommittee on Intelligence and Emerging Threats and Capabilities
Committee on Oversight and Reform, Subcommittee on National Security

September 10, 2019

Washington, DC

Chairman Langevin, Chairman Lynch, Ranking Member Stefanik, Ranking Member Hice and members of the Subcommittees, 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 and collaborative efforts to secure the Nation's internet architecture. Safeguarding cyberspace is a core homeland security mission, and CISA leads the Nation's efforts to advance the security and resilience of our cyber infrastructure.

CISA is responsible for assisting agencies with protecting civilian Federal Government networks and coordinating with other federal agencies, as well as state, local, tribal, and territorial governments, and the private sector to defend our Nation's critical infrastructure. We work to enhance information sharing across the globe in order to help critical infrastructure entities and government agencies protect their infrastructure, and we do this in a way that protects privacy and civil liberties. By bringing together all levels of government, the private sector, international partners, and the public, CISA strengthens the resilience of our Nation's critical infrastructure.

Risk Characterization

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.

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. According to the U.S. Department of Commerce's Bureau of Economic Analysis, the digital economy supported 5.1 million jobs and accounted for $1.4 trillion of gross domestic product (GDP) in 2017, or about 7 percent of the U.S. economy. Virtually every element of modern life is now dependent on cyber infrastructure. The sector recognizes that other sectors consider its services to be critical, and its practices reflect this understanding.

The nature of communication networks involve both physical infrastructure (buildings, switches, towers, antennas, etc.) and cyber infrastructure (routing and switching software, operational support systems, user applications, etc.), representing a holistic challenge to address the entire physical-cyber infrastructure. The result has been the establishment of a robust, resilient network infrastructure that successfully provides services globally. Over the last several decades, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry, using terrestrial, satellite, and wireless transmission systems.

CISA Roles and Responsibilities

CISA, along with the Department of Defense (DOD), Department of Commerce, and other government and private sector partners, engage in a strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity. In May of 2018, the DHS 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.

The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting sector infrastructure and assets. Working with the Federal Government, the private sector is able to predict, anticipate, and respond to sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other sectors, and affect response and recovery efforts.

A core component of the CISA mission is advancing reliable and secure communications for public safety, critical infrastructure owners and operators, and the general public. CISA supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. We assist with preparedness by ensuring federal, state, local, tribal and territorial public safety organizations have the necessary plans, resources, and training needed to support operable and advanced interoperable emergency communications. Additionally, CISA works across government and industry to ensure the national security and emergency preparedness community has access to priority telecommunications and restoration services to communicate under all circumstances.

CISA serves as the Sector-Specific Agency (SSA) for the Communications and Information Technology Sectors, and it operates the Communications Sector Information Sharing and Analysis Center. We lead communications response and recovery efforts under Emergency Support Function 2 of the National Response Framework. Through our operations center, we monitor national and international incidents and events that may impact communications infrastructure. Today, 11 Federal Government agencies and more than 60 private sector communications and information technology companies routinely share critical communications information and advice in a trusted environment to support CISA's national security and emergency preparedness communications mission. As the SSA for these sectors, DHS works closely with DOD, Department of Justice, Department of Commerce, Federal Communications Commission, General Services Administration, the Intelligence Community, and the private sector to address both short-term and longer-term challenges regarding risks to telecommunications networks.

CISA shares timely and actionable classified and unclassified information, focusing on sharing cyber threat information in a manner that protects privacy and civil liberties, and the confidentiality of those who share sensitive information with us. CISA also provides 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, DOD, 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.

CISA provides entities with information, technical assistance, and guidance they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. CISA operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The *Cybersecurity Information Sharing Act of 2015* (P.L. 114-113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. CISA's automated indicator sharing capability allows the Federal Government and private sector network defenders to share technical information at machine speed.

Joint DOD and DHS Cybersecurity Efforts

The challenge of effectively coordinating homeland security and homeland defense missions is not new, but it is amplified and complicated by the global, borderless, interconnected nature of cyberspace where strategic threats can manifest in the homeland without advanced warning. Almost a year ago, DHS and DOD finalized an agreement, which reflects the commitment of both Departments in collaborating to improve the protection and defense of the U.S. homeland from strategic cyber threats. This agreement clarifies roles and responsibilities between DOD and DHS to enhance U.S. government readiness to respond to cyber threats and establish coordinated lines of efforts to secure, protect, and defend the homeland.

The roles and responsibilities of DOD and DHS are complementary, but different. DOD must maintain the U.S. military's ability to fight and win wars and project power in a contested environment or while under attack in any domain, including cyberspace. As the government lead for national risk management, DHS is responsible for leading overall government efforts to protect critical infrastructure and civilian federal government informational system. As a part of these missions, DHS is working with a range of partners to identify national critical functions and ensure their integrity and resilience by leading government efforts to integrate and coordinate cybersecurity risk management and assistance with state, local, tribal, and territorial, and private sector critical infrastructure partners. DHS is a focal point for sharing cyber threat indicators and information and is responsible for providing tools, services, and programs to reduce and mitigate the risk of catastrophic consequences stemming from cyber-attacks.

DHS and DOD are both committed to improving the protection and defense of the homeland from strategic cyber threats. Specifically, DHS and DOD are working to improve intelligence, indications, and warning of malicious cyber activity; strengthen the resilience of the highest priority

national critical infrastructure; improve joint operations planning and coordination; improve joint incident response to significant cyber incidents; expand cooperation with State, local, tribal and territorial authorities; and improve joint defense of Federal networks.

DHS and DOD will achieve these objectives through three primary lines of effort. First, DOD and DHS are adopting a threat-informed, risk-based approach that ensures the resilient delivery of national critical functions and services, and denies strategic adversaries the ability to prevent delivery of such functions and services. DOD and DHS will jointly prioritize a set of high priority national critical functions and non-DOD owned mission critical infrastructure that is most critical to the military's ability to fight and win wars and project power. Second, DOD and DHS, in coordination with the FBI and the intelligence community, are collaborating to build a common understanding of strategic cyber threats that can empower private sector network defenders, critical infrastructure owners and operators, and government actors to improve resilience and integrity of national critical functions. Timely access to threat information related to adversary capabilities and intent is critical to understand and counter the risk facing our nation's critical infrastructure effectively. Third, DOD and DHS are coordinating to inform and mutually support respective planning and operational activities as appropriate for each Department's unique authorities. DHS's knowledge of the domestic risk landscape, its work with the private sector, can inform DOD's efforts to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure. And, DOD's "defend forward" operations can inform and guide DHS efforts to anticipate adversary action and understand potential risks to critical infrastructure.

5th Generation Mobile Communications

Advances in 5G technology, the Internet of Things (IoT), 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 population, are 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 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. With these dramatic advancements in telecommunications and technologies associated with them also comes increased risk to the Nation's infrastructure.

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. The capabilities 5G will allow for ensures exponentially more data will be transmitted to, from, and across networks. 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. Due to the nature of 5G network architecture, many more pieces of cellular equipment will be present in the physical world. Malicious actors could introduce device vulnerabilities into the 5G supply chain to compromise unsecured wireless systems and exfiltrate critical infrastructure data. 5G technology will enable significant advances in our society and the prosperity of the U.S. but will also usher in an age of significantly greater cyber vulnerability.

Undersea Cables

An unclassified joint paper released in 2017 by DHS and the Office of the Director of National Intelligence – in coordination with the private sector – examined the risks to undersea cables and landing stations and potential avenues to mitigate such risks. Undersea cables transmit more than 97 percent of the world's electronic communications and pose potentially devastating consequences in the event of failure. In addition to accidental physical threats, there are vulnerabilities relating to nation-state adversaries, cyberterrorists, hactivitists, and cybercriminals.

Domain Name Service

In January 2019, CISA issued Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*, directing Federal civilian agencies to take a series of immediate actions in response to a global Domain Name System (DNS) hijacking campaign. This was the first Emergency Directive issued by CISA under authorities granted by Congress in the Cybersecurity Act of 2015. The action took place after carefully considering the current and potential risk posed to Federal agencies.

The FY 2020 President's Budget also includes funds to begin development efforts to centralize the authoritative DNS resolution services for the Federal Government. The managed service will provide centralized DNS management for the Federal Government and a rich set of analytics that sit on top of traditional DNS services.

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 appreciate the Subcommittees' 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 Subcommittees today, and I look forward to your questions.