Statement for the Record

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

FOR A HEARING ON

China's Non-Traditional Espionage Against the United States:
The Threat and Potential Policy Responses

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

Wednesday, December 12, 2018

Washington, D.C.

Chairman Grassley, Ranking Member Feinstein, and members of the Committee, thank you for the opportunity to testify regarding current economic and cyber threats from China. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission. The Cybersecurity and Infrastructure Security Agency (CISA) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical 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 securing cyberspace.

DHS is responsible for assisting civilian Federal Government agencies to protect their networks and collaborating with Federal agencies; state, local, tribal, and territorial (SLTT) governments; and the private sector to defend against cyber threats to our Nation's critical infrastructure. 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 all levels of government, the private sector, international partners, and the public, we are enabling collective defense to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing of best practices and cyber threats, and strengthen resilience.

Cyber Threats from China

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. The past several years have marked a turning point in the cyber domain, at least in the public consciousness. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states increase the frequency and sophistication of these attacks. 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 democracy.

The distinction between criminal and nation-state activity is likely to become increasingly blurred as some countries view cyber criminal tools as a relatively inexpensive and deniable means to support their goals. Transnational organized cyber criminals pose substantial risks to financial and payment systems and develop capabilities that are often coopted by various state actors. Nation-state threat actors such as China, Russia, Iran, and North Korea have used cyber intrusions to steal private sector proprietary information and sabotage military and critical infrastructure.

China will continue to use cyber espionage and bolster cyber attack capabilities to support its national security priorities. The intelligence community and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral U.S.-China cyber commitments of September 2015. Most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or information technology and communications firms whose products and services support government and private sector networks worldwide. Since 2015, China has been

advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015.

China continues to target U.S. Government and private sector entities. These activities are evidenced by the recent indictment of a Chinese operative on charges of economic espionage and attempts to steal trade secrets from U.S. aviation and aerospace companies. There have also been indictments against a state-owned enterprise in China, a Taiwanese company, and three individuals on crimes relating to a conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company. China has been responsible for the theft of intellectual property, including trade secrets and other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. This is of special concern to us from a supply chain risk management perspective for information and communications technology (ICT).

Cybersecurity Priorities

DHS, our government partners, and the private sector are engaging in a more strategic and unified approach as we work to improve our Nation's overall defensive posture against malicious cyber activity. In May of this year, DHS published a Department-wide Cybersecurity Strategy, which outlines a strategic framework to execute our cybersecurity responsibilities during the next five years. Both the Strategy and Presidential Policy Directive 21- Critical Infrastructure Security and Resilience, emphasize that we must all maintain an integrated approach to managing risk.

The National Cyber Strategy, released in September, reiterates the criticality of collaboration and strengthens 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 DHS's efforts to secure federal networks and strengthen critical infrastructure. For example, the Department uses its authorities to ensure agencies are updating and patching systems, strengthening their email security, and removing problematic technology from their systems. DHS also works across government and industry critical infrastructure partnerships to share timely and actionable information as well as provide training and technical assistance.

DHS's CISA, which includes the National Cybersecurity and Communications Integration Center (NCCIC), 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. The NCCIC operates at the intersection of the private sector, state and local governments, federal departments and agencies, 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 automated sharing of cyber threat indicators and defensive measures. The automated indicator sharing (AIS) capability allows the Federal Government and the private sector network defenders to share technical information at machine speed.

National Risk Management

Our adversaries' capabilities online are outpacing our stove-piped defenses. Specifically, there has been a critical gap in cross-sector, cross-government coordination on critical infrastructure security and resilience. Working together with the private sector and other government partners, we are taking collective action to strengthen cross-sector, cross-government coordination against malicious cyber actors.

With the renaming and refocusing of the Office of Cyber and Infrastructure Analysis as the National Risk Management Center (NRMC), housed within CISA, we have stepped up our efforts to provide a comprehensive risk management approach to cyber and physical security. The NRMC is a core component of DHS's efforts to take a holistic cross-sector approach to managing risks to the critical functions that drive our economy and are necessary to our national security. Through the NRMC, government and industry are coming together to create a more complete understanding of the complex perils that threaten the nation's critical infrastructure.

Supply Chain Risks

Earlier this year, we established the Cyber Supply Chain Risk Management (C-SCRM) program. The C-SCRM program is addressing risks to information and communications technology (ICT) supply chains by developing and deploying supply chain risk management capabilities for federal agencies, private sector critical infrastructure owners and operators, and state, local, tribal, and territorial governments. To ensure our supply chain efforts are inclusive of industry, the NRMC recently established an ICT Supply Chain Risk Management Task Force. The Task Force is the main private sector point of entry our SCRM efforts and is jointly chaired by DHS and the chairs of the Information Technology (IT) and Communications Sector Coordinating Councils.

ICT is critical to every business and government agency's ability to carry out its mission efficiently and effectively. Vulnerabilities in ICT can be exploited intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft, and insertion of malicious software or hardware. If these risks are not detected and mitigated, the impact to the ICT could be a fundamental degradation of its confidentiality, integrity, or availability and potentially adverse impacts to essential government or critical infrastructure systems.

Increasingly sophisticated adversaries seek to steal, compromise, alter, or destroy sensitive information on systems and networks, and risks associated with ICT may be used to facilitate these activities. The Office of the Director of National Intelligence (ODNI) acknowledges that "The U.S. is under systemic assault by foreign intelligence entities who target the equipment, systems, and information used every day by government, business, and individual citizens."[1] The globalization of our supply chain can result in component parts, services, and manufacturing from sources distributed around the world. ODNI further states, "Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to

[1] https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC--SCRM-Background.pdf

obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property and personally identifiable information, insert malware into critical components, and mask foreign ownership, control, and/or influence of key providers of components and services."

Risks to the ICT supply chain are no longer an emerging threat, they are a pervasive threat. However, the rules under which procurements are conducted have not kept pace with the evolution of this threat. The Federal Acquisition Regulation is designed to balance the equities of the government and the contracting parties, ensuring due process for contractors and disclosure of the government's reasons for pursuing contractual remedies in the event of performance or integrity failure. These rules, however, were designed around the procurement of commodities and services that were not anticipated to be vulnerable to, nor the target of, the sophisticated foreign intelligence activities witnessed in recent years, especially those associated with a globalized ICT supply chain. For instance, the current procurement rules and their underpinning statutes did not imagine the need to use and protect intelligence information in unclassified procurements.

New rules are needed to combat the threat to our Nation's federal information technology networks when intelligence and vulnerability information identifies risks that cannot be mitigated. As such, in the remaining days of this Congress we urge swift passage of S. 3085, the *Federal Acquisition Supply Chain Security Act of 2018*. If enacted, this legislation would establish a strategic statutory framework to protect our Federal supply chain by conducting supply chain risk assessments, creating mechanisms for sharing supply chain information, and establishing exclusion authorities—both within agencies and in a centralized manner—to be utilized when justified.

Additionally, DHS and our interagency partners are working diligently to implement Section 889 of the National Defense Authorization Act for Fiscal Year 2019. This law prohibits executive agencies from procuring certain telecommunications equipment and other technology from specific companies based in the People's Republic of China. We will continue to do what is necessary to meet this law, and leverage our other authorities to assist federal agencies with securing their information systems, including from supply chain risks.

Conclusion

In the face of increasingly sophisticated threats, DHS employees stand on the front lines of the Federal Government's efforts to defend our nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "Internet of Things" and cloud computing, and the pending development and deployment of 5G telecommunications technology offer increased access and streamlined efficiencies, while increasing the footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. Expertise around

cyber-physical risk and cross-sector critical infrastructure interdependencies is where the Cybersecurity and Infrastructure Security Agency brings unique expertise and capabilities.

As the Committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure and resilient Homeland.

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