Testimony

Bryan Ware
Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

Dangerous Partners: Big Tech and Beijing

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND TERRORISM

Wednesday, March 4, 2020

Washington, DC

Chairman Hawley, Ranking Member Whitehouse, and members of the Subcommittee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) ongoing efforts to support the private sector's efforts to increase the cybersecurity of their networks. CISA works every day to support the private sector and the American people's efforts and responsibilities to secure their corporate and personal data, the focus of today's hearing. Safeguarding and securing cyberspace is a core mission of DHS.

At CISA, our mission is to defend against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow – "Defend Today, Secure Tomorrow."

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 continue to see malicious 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. 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 and strategic competitors are 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.

Increasingly, most discussions around cybersecurity threats include some risk calculation related to supply chain, third party, or vendor assurance risk. In 2018, cybersecurity firm Symantec reported 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 information and communications technologies (ICT) and their related supply chains for purposes of espionage, sabotage, foreign interference, and criminal activity. Vulnerabilities in supply chains – either developed intentionally for malicious intent or unintentionally, including 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. More often, our adversaries are looking at these vulnerabilities as a principal attack vector, and we are greatly concerned with aggressive actions by potential foreign adversaries and strategic competitors 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 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 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, and we do this with attention to protecting privacy, civil liberties and confidentiality. 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 incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

CISA provides entities with 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 sharing 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, without eroding privacy protections or civil liberties.

CISA provides a broad range of capabilities to assist private sector entities across all 16 sectors of critical infrastructure. In addition to information sharing and incident response, these capabilities include assessments and technical services as well as recommended remediation and mitigation techniques that improve the cybersecurity posture of the Nation. Among other services, these include vulnerability scanning and testing, penetration testing, phishing assessments, and red teaming on operational technology that includes the industrial control systems which operate our nation's critical infrastructure.

Supply Chain Risks

There are also steps we can take to secure the hardware agencies and entities use to build their networks and the software that runs those networks. ICT is critical to every business's ability to carry out its mission efficiently and effectively. Vulnerabilities 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 supply chain could

be a fundamental degradation of its confidentiality, integrity, or availability and potentially create adverse impacts to essential government or critical infrastructure systems.

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 Information Technology (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.

In its first year, 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 2019, 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, including 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 information sharing about supply chain risks with a particular focus on potential adversaries. 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 regarding 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 from 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.

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 and its people. ”DHS, specifically CISA, plays a key role in the EO, which requires the Secretary of Homeland Security to “assess and identify entities, hardware, software, and services that present vulnerabilities that pose the greatest potential consequences to the national security of the United States.” CISA coordinated with federal and private partners to assess what ICT hardware, software, and services (referred to individually in this report as elements) present the greatest vulnerabilities in U.S. infrastructure and pose the greatest consequences, this assessment was completed in August 2019.

Mitigating the Risks

CISA works with our private sector partners every day to help them protect their networks and their data from bad actors, using some of the previously-mentioned tools and coordination activities. However, as we work with the private sector to help them secure their information, CISA has published the Cyber Essentials guide for leaders of small business and small and local government to show basic steps that can be taken on their own to improve their cybersecurity posture:

- Employ a backup solution that automatically and continuously backs up critical data and system configurations;
- Enable automatic updates whenever possible;
- Replace unsupported operating systems, applications, and hardware; and
- Test and deploy patches quickly.

Along with these steps, companies must develop a culture, at all levels, that reinforces cybersecurity essentials. Corporate leaders should drive cybersecurity strategy, investment, and culture by learning how much of their organization’s operations are dependent on IT and by leading the development of cybersecurity policies. Promoting security awareness and vigilance through training and maintaining awareness of cyber risks among all employees is vital. Critical assets and applications must be protected through implementing secure hardware and software configurations and leveraging email and web browser security settings to protect against spoofed or modified emails and unsecured webpages. Companies must manage their operational footprint, access, and identities to ensure that only those that require access to the corporate network receive permissions. Knowing who is on your network, using multi-factor authentication for administrative privileges and remote access, and issuing unique passwords for all user accounts is important in this area. Finally, information should always be backed up and protected by instituting rules such as establishing regular automated backups and redundancies of key systems and deploying malware protection capabilities, with an organization’s most critical data encrypted, including Personally Identifiable Information, or PII, particularly when it is “at rest,” in storage.

Even if an organization implements these steps, it must be ready and prepared to respond and recover from a potential cyber incident and breach of personal data. Companies should

develop incident response and disaster recovery plans, as well as a personal data breach response plan. Business impact assessments should be leveraged to prioritize resources and identify which systems must be recovered first. Internal reporting structures must be built to detect, communicate and contain an attack. IT security officials should have already determined who to call for help when an incident takes place, whether it is outside partners, vendors, government/industry responders such as CISA, technical advisors or law enforcement. Planning should occur before a potential cyber incident to determine which in-house containment measures can be applied to limit the impact of the cyber incident when it occurs.

Administrative Subpoena Authorities

Finally, CISA supports Congress's efforts to address a significant gap in the protection of critical infrastructure through the introduction of legislation, such as the Cybersecurity and Vulnerability Disclosure Act (S. 3045). Today, our Nation's adversaries can use publicly available, easily accessible tools to detect vulnerable systems operating our Nation's critical infrastructure that are connected to the public internet. While CISA is aware of these vulnerable online systems operating critical infrastructure, the Agency is unable to identify the vulnerable system's owners or operators.

The Internet service providers (ISPs), who can identify and provide contact information for these operators, are generally prohibited by law from disclosing this information to the federal government. If Congress provides CISA with a legal mechanism to obtain very limited information regarding the contact details for the affected entity, the Internet service providers could legally provide it.

The authority CISA seeks is limited in scope and would provide the Agency with a necessary tool to help secure our Nation's critical infrastructure from cyber-attacks. CISA does not seek to change the voluntary nature of our cybersecurity support to industry. Ultimately, our goal is to enable that broader collective defense against cybersecurity threats, where government and industry understand the risks we face and are prepared to defend against them. We look forward to working with Congress on this legislation.

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 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 responses in order to effectively secure the Nation. CISA contributes unique expertise and capabilities to mitigate cyber-physical risk.

I recognize and appreciate the Subcommittee's strong support and diligence as it works to understand this evolving 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 Subcommittee today, and I look forward to your questions.