17 February 2022

Dr. Neil E. Jenkins
Chief Analytic Officer
Cyber Threat Alliance

Testimony Before the US-China Economic and Security Review Commission on U.S. Private Industry Responses to the China Cyber Challenge

Introduction

Thank you for the opportunity to provide testimony United States government and private sector responses to cyber threats from China. In the testimony below, you will note that the fundamentals of cybersecurity for the Federal government and the private sector are – for the most part – independent of the specific cyber threat from China. Organizations must manage the risk from the full spectrum of malicious cyber actors of all types, including nation state actors, cyber criminals, and hacktivists.

Malicious cyber actors leverage various tactics, techniques, and procedures, or TTPs, to achieve their end goals. At times, the TTPs that actors use to gain access to systems, such as spearphishing or password guessing, will be very similar. But what they do with that access can be very different. Through intelligence gathering, information sharing, and operational collaboration, organizations can begin to understand their specific risk profiles and adapt their defenses appropriately.

This testimony first describes the roles and responsibilities of Federal government agencies in cybersecurity, how the Federal government organizes for cybersecurity efforts, and how it shares information and collaborates with the private sector. I then describe private sector cybersecurity risk management and how collaboration between the public and private sectors fosters resilience. Next, I highlight the cyber threat from China, emphasizing how it is more of a long-term strategic threat in comparison to other nation state adversaries such as Russia, Iran, and North Korea. I conclude with a discussion of critical infrastructure cybersecurity efforts and recommendations for further improvements.

Roles and Responsibilities of U.S. Government Agencies in Cybersecurity

The roles and responsibilities of U.S. government agencies in cybersecurity are quite complex, reflecting the nature of cyberspace itself. Information technology (IT) is used to enhance our abilities to communicate, conduct business, store our information, and make processes more efficient. However, malicious actors can use those same IT systems to undermine trust in that same information, conduct disruptive ransomware attacks, steal intellectual property, and lead to destructive attacks against critical infrastructure. A discipline that covers this much territory cannot be managed effectively by a single government agency. The government must bring various agencies together to work toward a common goal and use their various authorities and capabilities in a coordinated and collaborative way, providing guidance and information to the private sector so they may manage their own cyber risk.

National cyber strategy and policy is guided by the White House by the National Security Council (NSC) and the newly established Office of the National Cyber Director (ONCD). The National Security Advisor develops national security strategy and policy for the President, of which cyber is and will continue to be an important factor, and connects cyber to the broader geopolitical strategic approach to China and other nation states. The development of a National Cyber Strategy will be conducted by the NSC, in coordination with the ONCD and other government agencies.[1] The NSC also has a role in coordinating military and intelligence cyber operations with the operational activities of other government agencies.

The ONCD intends to guide cooperation and collaboration between government agencies to improve public-private collaboration, align resources across the government, and increase present and future resilience.[2] The ONCD and the NSC must work together closely to model the cooperation and collaboration needed across federal agencies. The Office of Management and Budget (OMB) also has a role in setting cybersecurity policy for Federal departments and agencies through the Federal Chief Information Officer and the Federal Chief Information Security Officer.

The bulk of the federal government's cybersecurity efforts are conducted by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Justice's Federal Bureau of Investigation (FBI). CISA leads "the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure"[3] and acts as the Nation's risk advisor. CISA is the operational lead for Federal cybersecurity (the .gov) and acts as the National Coordinator for critical infrastructure security and resilience. CISA provides technical assistance, incident response, tools, information, and training that organizations across the public and private sectors can use to manage their risk. To differentiate the responsibilities of CISA and the NCD, CISA Director Jen Easterly noted in recent Congressional testimony that CISA is "the quarterback" and NCD is the "coach of the team" that brings a "sense of coherence and unity of effort," reflecting their respective operational and strategic roles.[4]

Whereas CISA focuses their cybersecurity efforts on information technology assets, organizations, and sectors, the FBI focuses on the threat actors at the source of cyber intrusions. The FBI's cyber strategy is to "impose risk and consequences on cyber adversaries" through their role as the lead federal agency for investigating cyber attacks and intrusions.[5] The FBI conducts law enforcement investigations related to cyber activity, attributes malicious

[1] https://www.lawfareblog.com/how-national-cyber-director-position-going-work-frequently-asked-questions

[2] https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf

[3] https://www.cisa.gov/about-cisa

[4] https://twitter.com/ericgeller/status/1403002705702916096?s=20

[5] https://www.fbi.gov/investigate/cyber

activity to specific actors, and responds to incidents to provide technical assistance and collect evidence. Federal agencies such as the U.S. Secret Service and Immigration and Customs Enforcement also have cyber law enforcement authorities, and these various investigations are coordinated through the FBI's National Cyber Investigative Joint Task Force (NCIJTF).

Other government agencies with significant cybersecurity responsibilities include:

- Sector Risk Management Agencies (SRMAs) such as the Department of Energy and the Treasury, work with the 16 critical infrastructure sectors to understand their risks and build trusted partnerships with the U.S. government.[6]
- Members of the Intelligence Community provide strategic indications and warnings, situational awareness of threat actors, and technical indicators of threat activity.
- Within the Department of Defense (DoD), the National Security Agency provides cyber related intelligence and protects National Security Systems, while the U.S. Cyber Command provides options for military cyber operations, defends the DoD networks, and supports the defense of national interests in cyberspace.[7]
- The State Department conducts diplomacy with other countries on cybersecurity issues.
- The Department of Justice uses tools such as criminal indictments or asset seizures against malicious cyber actors.
- The Department of Treasury imposes sanctions on malicious adversaries at the direction of the President.
- The Department of Commerce can place an organization on its Entity List, which restricts the US organizations from trading with specific entities, including Chinese companies like Huawei and ZTE.
- The Federal Communications Commission regulates access to U.S. telecom markets.
- The Federal Trade Commission and the Securities and Exchange Commission provide regulatory oversight roles for cybersecurity in the private sector.

When government agencies collaborate, they can synthesize information from various sources inside and outside of government to help the private and public sectors manage their risk and find the best ways to punish malicious cyber actors. The level of collaboration within the government has improved greatly over the last decade. Ten years ago, agencies would often release different information to different stakeholders, confusing the private sector and reducing the strategic impact of the releases. Now, agencies are much more likely to coordinate the release of technical indicators and risk management advice in a joint report. I will return to this in a later section of this testimony.

Private Sector Cybersecurity and Resilience – Improving, but still room for growth

The cybersecurity of an individual organization is the responsibility of that organization and not of the federal government. The information technology and systems that organizations use to conduct business, operate critical infrastructure, and communicate internally and externally are

[6] https://www.cisa.gov/sector-risk-management-agencies

[7] https://www.cybercom.mil/About/Mission-and-Vision/

deeply embedded in business practices. Organizations must constantly make risk-based decisions on how best to secure themselves while maintaining their ability to operate. Cybersecurity decisions are often resource-intensive and patching a new vulnerability or setting up multi-factor authentication can slow business operations. Organizations are in the best position to understand how to best implement cybersecurity practices and mitigate their risks.

An organization's overall level of cybersecurity is dependent on the resources and budget available. Cybersecurity is complex, requires a well-trained workforce, and is often costly to implement at scale. Over time, managing cybersecurity risk has gotten easier as cybersecurity providers have improved their products and services and many organizations that provide IT solutions have improved the security of their products. But the complex nature of systems that operate on code and are connected to the internet require constant monitoring and updating to address new vulnerabilities and threats.

What steps do organizations take to build a cybersecurity program? Most organizations, especially those that own and operate critical infrastructure, will leverage a layered, defense-in-depth strategy to cybersecurity. They will do their best to follow general cybersecurity best practices, like the NIST Cybersecurity Framework[8] and the Center for Internet Security's Critical Security Controls,[9] and practice good cyber hygiene, like scanning their environment for known vulnerabilities and patching them. They will train their workforce to improve their ability to identify and avoid phishing emails. They will develop and exercise cyber incident response plans.

They will use a cybersecurity provider to operate a detection and response capability on their endpoints and networks. They will manage a Security Operations Center or use a Managed Security Services Provider to comb through alerts from their systems to look for signs of malicious activity and subscribe to commercial threat intelligence feeds to get access to indicators of compromise or strategic warning on cyber attacks. Some organizations will staff their own threat intelligence teams to focus on specific threats to their organizations and use that intelligence to adapt their defenses against the threats most likely to target them.

Organizations may also employ threat hunters who look for signs of adversary TTPs being used on their networks that their sensors missed. They could hire external services to act as penetration testers that act like hackers and try and break into an organization, testing and probing their cyber defenses.

They can also join an Information Sharing and Analysis Center (ISAC) with companies in the same critical infrastructure sector to learn about threats and vulnerabilities their competitors face and apply those lessons. For any risks they can't mitigate with technology, outside contractors, training, or information sharing, they may purchase cyber insurance and transfer their risk.

[8] https://www.nist.gov/cyberframework
[9] https://www.cisecurity.org/controls/

The bottom line is that each of these layers of defense represent a cost for an organization. C-suites must make decisions on whether to spend their budget on additional cybersecurity protections, on other security provisions, or on a new manufacturing line. The larger the organization, in general, the more of these steps they can take. Unfortunately, most organizations are not able to take all these actions and must make choices, eventually accepting a level of cyber risk. This includes organizations in the supply chain of critical infrastructure owners and operators who provide important services and embedded technology.

All organizations need good, actionable information to understand the threats they face and the vulnerabilities inherent in their systems and help them make their risk management decisions. This information comes from multiple sources, such as their product and security vendors and their ISACs. It can also come from the Federal government.

Cooperation Between the U.S. Government and Private Industry on Cybersecurity Issues

Historically, cooperation between the U.S. government and private industry has been focused on information sharing between the private and public sectors to ensure that threats and mitigations are widely known and actioned accordingly. Information sharing should be bidirectional to be most effective, from the government to the private sector and vice versa. The government should strive to get the right information to the right recipients in time to make a difference. This section focuses on the cooperation between the government and the private sector in general. We will discuss how the government conducts enhanced collaboration with critical infrastructure in a later section.

Over time, information sharing from the government has improved and expanded in scope and scale. 15 years ago, cybersecurity information may have only been shared to organizations in classified environments where the government would give a Chief Executive Officer a one-day security clearance. The company may not have been able to do much with the information to make themselves more secure. Now, CISA and FBI work together and with their partners in the intelligence community to declassify information, combine that with reporting from the cybersecurity industry, and produce a single alert with strategic warning and technical indicators that can be used to secure systems and look for signs of malicious cyber activity. CISA posts that alert on their public website[10] and will tweet links to it, imploring organizations to take action.

CISA provides dedicated websites to highlight the threat from nation state actors such as China,[11] Russia,[12] Iran,[13] and North Korea.[14] Each website provides an overview of the cyber

[10] https://www.cisa.gov/uscert/ncas/alerts
[11] https://www.cisa.gov/uscert/china
[12] https://www.cisa.gov/uscert/russia
[13] https://www.cisa.gov/uscert/iran
[14] https://www.cisa.gov/uscert/northkorea

threat from these nation states and the latest advisories related to that activity. CISA has released more advisories on China over time, providing one China-specific alert each in 2017, 2018, and 2019, and then 4 alerts in 2020 and 5 in 2021. These alerts provide details on how to mitigate and detect this activity and report any incidents to the government.

Despite these advances, information sharing is far from perfect. The Federal government has tried to implement automated sharing of technical information with limited success and its most current efforts in this realm have little utility.[15] Federal agencies have greatly improved their timeliness when releasing alerts and technical information, but indicators shared in these reports can still be months old – a lifetime in cybersecurity. Organizations are relatively unwilling to share information to the government because of concerns with information becoming public and negatively impacting their reputation, increasing regulations on them or their sector, or exposing the organization to legal liability.

Legislation such as the Cybersecurity Information Sharing Act of 2015[16] helped clarify how the private sector can report incidents to the Federal government and provides liability protection to entities that share appropriately. Unfortunately, this legislation has not had the impact that many had hoped as the information sharing environment has proven to be complex. Additional steps may be required correct issues. It's likely that the entire community needs to completely reset expectations for what will be shared to the government and to the private sector. We must continue to address issues with information sharing and improve them whenever possible, but, in parallel, we must realize that information sharing alone is not enough and we must focus on actual operational collaboration between the Federal government and the private sector.

Operational collaboration is the act of bringing organizations together to share information, but then working together to act on that information to plan, prioritize, and synchronize activity to protect networks, disrupt malicious cyber activity, and respond to cyber incidents. Operational collaboration happens today in various pockets and sectors, such as the Cyber Threat Alliance,[17] the Analysis and Resilience Center,[18] and any number of trust communities within the cybersecurity ecosystem. These groups actively work together to have a broader impact on the cybersecurity of the whole ecosystem and organizations they represent. At its heart, operational collaboration builds trust between people and organizations, expanding the possibility of what can be shared and what actions can be taken together.

CISA has recently taken steps towards operational collaboration with the private sector, establishing the Joint Cyber Defense Collaborative (JCDC) to bring together public and private sector actors to "unify defensive actions and drive down risk in advance of cyber incidents occurring" and "strengthen the nation's cyber defenses through planning, preparation, and

[15] https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf
[16] https://www.congress.gov/bill/114th-congress/senate-bill/754/text
[17] https://www.cyberthreatalliance.org/
[18] https://systemicrisk.org/

information sharing."[19] JCDC partners currently include platform and cloud providers, like Microsoft, Google Cloud, and Amazon Web Services, as well as cybersecurity providers, such as CrowdStrike, Mandiant, Palo Alto Networks, Cisco, and Symantec. CISA is rightly focusing their initial collaborative efforts on the organizations that can have the most impact on the broader cyber ecosystem. They plan to include more critical infrastructure and state, local, tribal, and territorial (SLTT) partners over time.

While operational collaboration is clearly the correct next step and CISA should be applauded for moving in this direction, we must acknowledge that there are two key factors that shape the extent and limits of cooperation between private sector and the Federal government. First, the fundamental interests of the parties are not always the same. Private sector companies seek a profit while governments protect the national interest. One goal is not necessarily better or more important than the other, but these interests shape the relationship in steady state. The area of interest for the private sector is also not the same for the government. Many companies are multinational and must work with non-U.S. government entities (sometimes including China) while the U.S. government is solely focused on the United States. Partners in operational collaboration must understand that everyone's interests will not always be the same and focus efforts on common goals and objectives.

Malicious Cyber Activity from Chinese Actors

Before I describe how the U.S. government collaborates specifically with U.S. critical infrastructure, let's first discuss recent trends and malicious cyber activity from emanating specifically from China. Chinese nation-state activity in cyberspace has been different than the activity we see from the other nation-state actors we typically focus on. Russia, Iran, and North Korea see it in their national interests to be disruptive, attempting to upend the international system. China, on the other hand, seeks to remake the international system in its favor, without entirely upsetting the current economic and geopolitical order. They want to compete and win within the current system. Rob Joyce, the Director of the NSA's Cybersecurity Division, makes a useful analogy: "I kind of look at Russia as the hurricane. It comes in fast and hard. China … is climate change: long, slow, pervasive."[20,21] When asked by the Washington Post which nation is the United States' most dangerous cyber adversary, Katie Nickels, the director of intelligence for cybersecurity firm Red Canary said, "When dangerous is defined as having the greatest potential to threaten the strategic role of the U.S. as an enduring great power, the answer is China."[22]

This strategic competition in cyberspace from Chinese actors has manifested in espionage and the theft of intellectual property targeting various sectors and technology that the Chinese

[19] https://www.cisa.gov/jcdc
[20] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/06/the-cybersecurity-202-u-s-officials-it-s-china-hacking-that-keeps-us-up-at-night/5c7ec07f1b326b2d177d5fd3/
[21] https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/
[22] https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/

government has prioritized. In recent years, this activity has focused on the sectors identified in their “Made in China 2025” plan.[23] FBI Director Christopher Wray recently highlighted the threat to intellectual property and U.S. economic security from Chinese activity, noting that “it’s reached a new level – more brazen, more damaging than ever before, and it’s vital – vital – that all of us focus on that threat together.”[24]

China’s ”Made in China 2025” plan provides a useful guide to the industries that Chinese state actors have targeted for intellectual property theft, including information technology, robotics, aerospace, biopharmaceuticals, medical, electrical, farming, rail, new energy vehicles and green technologies. As Director Wray notes, “Whatever makes an industry tick, they target: source code from software companies, testing data and chemical designs from pharma firms, engineering designs from manufacturers, personal data from hospitals, credit bureaus, and banks.”[25]

Chinese targets have also obtained personal data of cleared civilian U.S. government employees and contractors through the 2015 Office of Personnel Management (OPM) incident. Experts speculate that combining data gained through the OPM hack with stolen data from other entities such as hotels and credit bureaus could lead to identification of U.S. intelligence agents and assets.[26]

Chinese nation-state actor TTPs have become more sophisticated over time. Prior to the 2015 Obama-Xi agreement, Chinese activity was relatively “loud” from a cybersecurity perspective. They leveraged spearphishing emails to target entities across nearly every critical infrastructure sector, and multiple threat actors from various Chinese government agencies would be found targeting the same data. Of late, Chinese actors “now concentrate on lower-volume but more-sophisticated, stealthier operations collecting strategic intelligence to support Chinese strategic political, military, and economic goals.”[27] They have transitioned away from spearphishing and often use harder-to-detect TTPs such as software vulnerabilities, living-off-the-land binaries, dual-use tools like Cobalt Strike, and exploitation of network devices and web facing applications. They also have been seen leveraging supply chain vulnerabilities and targeting third party providers, such as Managed Security Providers, to gain access to their eventual end targets.[28,29]

While intellectual property theft and espionage are the primary ways Chinese actors have impacted U.S. entities, we have seen signs of other cyber activity that trends towards more

[23] https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
[24] https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122
[25] https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122
[26] https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/
[27] https://www.mandiant.com/resources/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices
[28] https://www.mandiant.com/resources/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices
[29] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

brazen and disruptive actions. In February and March of 2021, Chinese state-sponsored actors that Microsoft calls HAFNIUM began targeting zero-day vulnerabilities in on-premises Microsoft Exchange Servers through automated attacks, installing malicious webshells on any vulnerable server they could access.[30] Cybersecurity firm ESET noted that multiple Chinese groups beyond HAFNIUM were using this vulnerability to compromise email servers around the world.[31] This indiscriminate activity from multiple Chinese threat actors was out of character compared to their activity in recent years for and required many organizations to interrupt their normal business activities to patch and remediate this activity.

Additionally, CISA and FBI provided evidence of a Chinese campaign targeting U.S. oil and national gas pipeline companies from 2011 to 2013 "for the purpose of holding U.S. pipeline infrastructure at risk."[32] The report noted that the activity "was ultimately intended to help China develop cyberattack capabilities against U.S. pipelines to physically damage pipeline or disrupt pipeline operations." U.S. government officials have also accused actors working for Chinese intelligence of using ransomware to extort U.S. businesses,[33] but it is unclear if this ransomware activity was directed by the Chinese government. These insights into potentially disruptive cyber activity from China are few and far between, but they provide a glimpse into what could be possible in the event of an escalation in global tensions.

U.S. Critical Infrastructure Cybersecurity, Regulatory Frameworks, and Recommendations

Critical infrastructure in the United States is defined in the Patriot Act of 2001 (42 U.S. Code § 5195c) as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[34] Presidential Policy Directive 21 (PPD-21) makes it the policy of the United States to "strengthen the security and resilience of its critical infrastructure against both physical and cyber threats"[35] and provides guidance to Federal government agencies to work with critical infrastructure owners and operators to take proactive steps together to manage their risk.

PPD-21 defines 16 critical infrastructure sectors and assigns agencies to serve as their sector-specific agency to manage the day-to-day Federal interface with the sector and represent their risk management needs and priorities to the rest of the Federal government. The FY21 National Defense Authorization Act codified Sector-Specific Agencies as Sector Risk Management Agencies (SRMAs) to better reflect their role with the critical infrastructure sectors.[36] The

[30] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[31] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
[32] https://www.cisa.gov/uscert/ncas/alerts/aa21-201a
[33] https://www.nbcnews.com/tech/tech-news/us-accuses-china-abetting-ransomware-attack-rcna1448
[34] https://www.law.cornell.edu/uscode/text/42/5195c
[35] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[36] https://www.cisa.gov/sector-risk-management-agencies

Secretary of Homeland Security coordinates the activities of SRMAs through CISA's National Risk Management Center (NRMC)[37] which also maintains a list of National Critical Functions to help further refine the government's support of critical infrastructure.[38] Businesses and organizations within the U.S. voluntarily choose to participate in sector risk management activities with the Federal government.

The security and resilience of U.S. critical infrastructure can only be attained through partnership between the private and public sectors, which includes Federal and SLTT governments. The private sector owns and operates the vast majority of the Nation's critical infrastructure (you will commonly hear that the private sector owns as much as 85% of critical infrastructure, though this oft quoted percentage is not based on hard data[39]). The private sector operates their critical infrastructure to ensure their businesses operate effectively for the benefit of shareholders, customers, and the general public that relies on their goods and services. The Federal government has little to no directive authority over most of this infrastructure and is limited to providing information to help manage risk, such as threats and vulnerabilities that may affect critical infrastructure, and fostering analysis of cross-sector activities to highlight dependencies between sectors.

Voluntary participation in critical infrastructure activities with the Federal government confers several benefits to the participating entities. Engagement provides insights into national security priorities and a forum for the private sector to inform Federal policy security priorities and initiatives. Critical infrastructure organizations are eligible to receive security clearances and access to classified intelligence and unclassified non-public information that can be useful in managing their risk. The Protected Critical Infrastructure Information (PCII) program enhances sharing from the critical infrastructure entities to the government.[40] Sensitive and proprietary information shared with the government through PCII cannot be released to the public through Freedom of Information Act (FOIA) requests, SLTT disclosure laws, or civil litigation, and it cannot be used for regulatory actions.

Regulation related to the cybersecurity of critical infrastructure is sparse and affects a small number of sectors, such as Energy and Financial Services, where Federal regulation in general is more common. The U.S. has historically favored less cybersecurity regulation on organizations to maintain innovation and allow the market to be nimble. There is also a danger that the U.S. government could regulate poorly in cybersecurity, resulting in a compliance heavy approach that does not improve security.

However, this policy environment is shifting as recent cyber incidents like the ransomware incident targeting Colonial Pipeline have impacted critical services on a national level and there is a growing recognition that the market has not been able to keep up with the threat. Suzanne

[37] https://www.cisa.gov/national-risk-management
[38] https://www.cisa.gov/national-critical-functions
[39] https://www.lawfareblog.com/it-really-85-percent
[40] https://www.cisa.gov/pcii-program

Spaulding, the former Under Secretary for the DHS office that has become CISA and a member of the Cyberspace Solarium Commission, noted in recent House testimony that “we cannot rely upon markets alone to ensure the continuity of nationally critical functions upon which the American public relies.”[41]

Policy makers and legislators have been discussing ways to strengthen the private-public partnership through new legislative requirements. One of the most prominent legislative approaches has been a proposed requirement for critical infrastructure organizations to report cyber incidents to the Federal government. The Cyberspace Solarium Commission provides a useful legislative proposal for cyber incident reporting.[42] The latest series of discussions around this proposed legislation has framed a reporting requirement as a way to understand the scope and scale of the ransomware. Providing the Federal government with information related to all cyber incidents, including intellectual property theft and espionage like that from China, will help policy makers define the scope and scale of incidents and lead to better responses.

The Cyberspace Solarium Commission also proposed that Congress codify the concept of “systematically important critical infrastructure” (SICI) where “entities responsible for systems and assets that underpin national critical functions are ensured the full support of the U.S. government and shoulder additional security requirements consistent with their unique status and importance.”[43] SICI entities are the most critical parts of our critical infrastructure. As noted above, participation by entities in government efforts is currently voluntary, but this proposal would seek to identify the infrastructure that is most important to the public health and safety, economic security, and national security of the U.S. and require them to participate in “collaborative joint security efforts.” In exchange for special assistance and support from the U.S. government to these organizations and enhanced liability protections, they would be required to certify their security compliance on a regular basis.

This proposal would go a long way in filling the gaps in the current voluntary private-public partnership model and foster the operational collaboration necessary to better manage cybersecurity risk nationally. Focused information sharing and collaboration with SICI entities that are likely targets of Chinese intellectual property theft should be a priority.

More generally, the Federal government should continue to increase the incentives for organizations to implement better cybersecurity. Government should leverage existing regulations where possible to promote good cybersecurity behavior, support and encourage the use of best practices, and drive industries to set standards of care[44] for cybersecurity. Establishing a generally accepted level of cybersecurity for organizations within an industry would remove uncertainty and enable businesses to plan investments, as well as addressing concerns about liability and reduce barriers to collaboration and information sharing. Existing

[41] https://homeland.house.gov/activities/hearings/transportation-cybersecurity-protecting-planes-trains-and-pipelines-from-cyber-threats
[42] https://www.solarium.gov/
[43] https://www.solarium.gov/
[44] https://www.bens.org/file/publications/CyberStandardofCare-101.pdf

efforts such as the National Telecommunications and Information Administration's (NTIA) Software Bill of Materials (SBOM), which provide an inventory of the software components and dependencies in the supply chain, would go a long way in helping organizations understand their risk to newly discovered vulnerabilities.[45] Like the previous recommendations, these efforts would improve the overall cybersecurity of the U.S. private sector against all threats, including the specific threat from Chinese nation state actors.

Conclusion

Cybersecurity is a risk management issue and there are no easy fixes. It requires organizations to look holistically at their business practices and take proper precautions. It requires collaboration across government agencies to properly understand the scope and the scale of the threat and share information effectively so that organizations can properly manage their risk. Most of all, it requires a partnership between the private and public sectors to ensure that the critical infrastructure we all rely on is secure and resilient. The current approach to critical infrastructure cybersecurity is fundamentally correct and we have made great strides over the last two decades, but in practice we do need some tweaks to fully realize its potential.

Likewise, there are no easy solutions to the threat from China's nation state actors in cyberspace and no there is no reason to expect this threat will diminish. China has leveraged stolen intellectual property from Western companies to make great gains in their economic standing. Recent indications suggest they continue to innovate their tactics and target organizations or their service providers to target the information they need to meet their strategic objectives. While the cyber threat from China is not as immediately disruptive as the threat from other nation states, organizations most at risk must continue to improve their defenses.

While these problems are hard, they are not unmanageable. The Federal government must continue to improve internal collaboration among agencies to provide timely, relevant technical and strategic information to the private sector. New organizations like the Office of the National Cyber Director, CISA, and CISA's JCDC will bring a focus on operational collaboration with the private sector that will pay dividends over time. Congress should move forward with cyber incident reporting requirements for critical infrastructure to ensure we understand the scope and scale of the problem and resource it accordingly. Identifying and prioritizing systematically important critical infrastructure will be a key objective for private-public partnership efforts. Smart regulations of critical infrastructure, security certifications for these most important entities, and making it easier for organizations to know what software is included in their information technology are all steps we need to take to shore up our Nation's defenses against malicious cyber actors.

Thank you for the opportunity to discuss these topics and I look forward to your questions.

[45] https://www.ntia.gov/SBOM