Statement for the Record
of
Jamil N. Jaffer[1]
on
Safeguarding the Federal Software Supply Chain
before the
Subcommittee on Cybersecurity, Information Technology, and Government Innovation
of the
Committee on Oversight and Accountability

November 29, 2023

I. Introduction

Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee: thank you for inviting me to discuss the threat facing our nation from potential vulnerabilities in the federal software supply chain.

I want to thank Chairwoman Mace and Ranking Member Connolly for holding today's hearing on these important issues and, in particular want to thank both of you for your leadership in highlighting the threat posed to the United States by software supply chain vulnerabilities. As you both well know, such vulnerabilities can enable significant attacks and hacks by nation-state and other threat actors. I also want to thank both of you for your leadership in advocating for action by key players in both the public and private sector to close the gaps in this area. I hope this hearing will offer us the opportunity to have a candid and frank discussion on these important matters.

II. The Threat of Supply Chain Attacks is Real, Current, and Significant

At a recent hearing before the House Homeland Security Committee, the Secretary of Homeland Security testified that "cyber threats from foreign governments and transnational criminals remain among the most prominent threats facing our nation" and noted that "[h]ostile regimes like Russia, the PRC, Iran, and North Korea…continually grow more sophisticated, steal our data and intellectual property, extort ransoms, and threaten our cyber systems."[2] At the same hearing, the

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and as an Assistant Professor of Law and Director of the National Security Law & Policy Program at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports and invests in innovative companies that develop promising, early-stage technologies to address the critical cyber and advanced technological needs of both commercial and government customers. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer is testifying before the Committee in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or former employer.

[2] *See* Secretary Alejandro N. Mayorkas, *Testimony: Worldwide Threats to the Homeland*, Committee on Homeland Security, at 5, U.S. House of Representatives (Nov. 15, 2023), *available online at* <https://homeland.house.gov/wp-content/uploads/2023/11/2023-11-15-HRG-Testimony.pdf>.

Director of the Federal Bureau of Investigation (FBI) argued that “criminals and nation-states believe that they can compromise our networks, steal our property, extort us, and hold our critical infrastructure at risk without incurring any risk themselves,” and noted these actors “continue to innovate, using unique techniques to compromise our networks and maximize the reach and impact of their operations…includ[ing] selling malware as a service or targeting vendors to access scores of victims by hacking just one provider.”[3] It is this latter methodology—the targeting of one provider to access a broad range of victims—that is at the heart of software supply chain attacks.

The Cybersecurity and Infrastructure Security Agency (CISA), in a joint publication with the National Institute of Standards and Technology (NIST), defines a software supply chain attack as taking place “when a cyber threat actor infiltrates a software vendor’s network and employs malicious code to compromise the software before the vendor sends it to their customers” which then allows the threat actor to further “compromise[] the customer’s data or system.”[4] According to CISA, “[n]ewly acquired software may be compromised from the outset, or [may be] compromise[d]…through other means like a patch or hotfix” and, because such software is already trusted, can ultimately “have widespread consequences for government, critical infrastructure, and private sector software customers.”[5]

According to CISA, such software supply chain attacks can take place at anywhere in the information and communications technology (ICT) lifecycle, from the design, development and production, and distribution phases, all the way through the acquisition and deployment, maintenance, and disposal phases.[6] Indeed, CISA cites examples of software supply chain attacks across the ICT lifecycle going back well over a decade, including attacks that allowed a foreign company to exfiltrate call data from U.S. cell phones, malware preinstalled on 20% of the devices tested by a major U.S. software manufacturer, the compromise by a foreign intelligence service of a popular antivirus software tool used by a number of U.S. government agencies, and backdoors embedded in routine software maintenance updates, just to name a few.[7]

Some of the most well-known examples of software supply chain attacks involve nation-state attackers going after other nation-states. According to CISA, “[s]oftware supply chain attacks typically require strong technical aptitude and long-term commitment,” and, as a result, advanced persistent threat (APT) actors, like nation-states, “are more likely to have both the intent and capability to conduct the types of highly technical and prolonged software supply chain attack campaigns that may harm national security.”[8] These actors use a variety of techniques to conduct

[3] *See* FBI Director Christopher A. Wray, *Testimony: Worldwide Threats to the Homeland*, Committee on Homeland Security, at 5, U.S. House of Representatives (Nov. 15, 2023), *available online at* <https://homeland.house.gov/wp-content/uploads/2023/11/2023-11-15-HRG-Testimony.pdf>.

[4] *See* Cybersecurity and Infrastructure Security Agency, *Defending Against Software Supply Chain Attacks* (Apr. 2021), Department of Homeland Security, at 2, *available online at* <https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf>.

[5] *Id*.

[6] *Id*. at 3.

[7] *Id*.

[8] *Id*. at 5.

their supply chain attacks, including by hijacking software updates, illicitly signing code to make it look legitimate, and compromising open source code that may be used by other developers.[9]

For example, in 2017, Russian military hackers associated with the Russian Main Intelligence Directorate (GRU),[10] exploited a vulnerability in the update cycle of M.E.Doc, a Ukrainian accounting program, using its access to a wide range of entities across various sectors to deliver a highly capable piece of malware that successfully bricked hundreds of computers within Ukraine.[11] The tool also spread worldwide, hitting a number of major Western companies and taking down critical servers, including the global shipper Maersk's entire system of network domain controllers worldwide, causing it to suffer significant limitations on its port and shipping operations for weeks, and causing an estimated $10 billion in damage globally to Maersk and other companies.[12]

Likewise, in the 2019 SolarWinds attack, hackers operating on behalf of the Russian Foreign Intelligence Service (SVR), utilized a vulnerability in the update process of a security software platform (as well as other access methods, including compromising legitimate accounts)[13] to gain authorized access to tens of thousands of the security company's customers (and others), including a broad swath of U.S. government agencies, defense contractors, and think tanks.[14] Once inside, the Russian hackers then took aim at a specific subset of these customers, focused primarily on government and national security targets, and further exploited gaps in the Microsoft Azure and Active Directory infrastructure of those organizations to obtain more persistent and defensible access, making it nearly impossible to fully identify and remove the threat actors from those organizations' cyber infrastructure.[15]

[9] *Id.*

[10] *See* Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (Oct. 19, 2020), *available online at* <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and> (noting that "GRU hackers and their co-conspirators engaged in computer intrusions and attacks…us[ing] some of the world's most destructive malware to date, including…NotPetya, which caused nearly $1 billion in losses to the three victims identified in the indictment alone.")

[11] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 22, 2018), *available online at* <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

[12] *Id.*

[13] *See* CISA, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Apr. 15, 2021), *available online at* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a> ("CISA has evidence that there are initial access vectors other than the SolarWinds Orion platform and has identified legitimate account abuse as one of these vectors (for details refer to Initial Access Vectors section). Specifically, we are investigating incidents in which activity indicating abuse of Security Assertion Markup Language (SAML) tokens consistent with this adversary's behavior is present, yet where impacted SolarWinds instances have not been identified.")

[14] *See* Kim Zetter, *The Untold Story of the Boldest Supply-Chain Hack Ever*, Wired (May 2, 2023), *available online at* <https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/>.

[15] *See, e.g.*, CISA, *SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures* (Mar. 17, 2021), *available online at* <https://www.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf> ("The advanced persistent threat (APT) actor associated with the SolarWinds Orion supply chain

And lest one think that these type of supply chain attacks by Russia don't present a current threat to the United States, it's worth noting that the Director of National Intelligence (DNI), in her annual worldwide threat assessment released earlier this year, indicted that "Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities[,]" because it "views cyber disruptions as a foreign policy lever to shape other countries' decisions."[16] This is particularly important in the context of the ongoing war in Ukraine and U.S. support for our partners in the region, especially given the fact that the DNI highlighted that "Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."[17]

The Secretary of Homeland Security underlined this point earlier this month, when he noted that "[m]alicious cyber activity targeting the United States has increased since Russia's full invasion of Ukraine, a trend we expect to continue throughout the duration of the conflict" and also flagged that Russia and others have, in the past three years, undertaken activities "impacting organizations of all sizes and disrupting critical services, from the Russian government's compromise of the SolarWinds supply chain to the widespread vulnerabilities generated by open-source software like Log4j."[18] Likewise, he noted that DHS assesses that ransomware attacks—which are often deployed through the exploitation of software supply chain vulnerabilities—targeting the United States, including federal, state, and local governments, as well as our critical infrastructure entities, "will increase in the near- and long-terms."[19]

Moreover, it is important to note that such supply chain attacks are hardly isolated to Russian threat actors. Indeed, China has long been active in the software supply chain exploitation space as well, including being suspected of involvement in the recently identified CarderBee attacks that targeted key systems across Asia, including in Hong Kong.[20] These attacks, which hijacked the software update process of a piece of Chinese-developed security software knows as Cobra DocGuard, also exploited compromised digital signatures from Microsoft, allowing the malware to masquerade as legitimate code from a major American software company and making it that much harder to detect.[21] CISA has also noted that Chinese-government linked hackers, like those involved in

compromise moved laterally to multiple systems—including Microsoft cloud environments—and established difficult-to-detect persistence mechanisms.").

[16] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023), at 15, *available online at* <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf> (emphasis added).

[17] *Id*.

[18] *See* Mayorkas, Worldwide Threats, *supra* n. 2 at 4.

[19] *Id*. at 4-5.

[20] *See* Andy Greenberg, *A New Supply Chain Attack Hit Close to 100 Victims—and Clues Point to China*, Wired (Aug 22, 2023), *available online at* <https://www.wired.com/story/carderbee-china-hong-kong-supply-chain-attack/>.

[21] *Id*.

APT41 (also known as Barium, Wicked Panda, and Wicked Spider), have conducted similar supply chain attacks exploiting code-signing vulnerabilities and third-party provider software to target more than "100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks, and foreign governments[.]"[22]

China, for its part, has also been implicated in other similar attacks as well, having been outed—in a joint cybersecurity advisory put out just two months ago by the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), CISA, and two Japanese national law enforcement and cyber organizations—for hacking the firmware of certain Cisco routers in order to target U.S. and Japanese corporations. The hack was designed to allow the Chinese hackers to infiltrate these companies "without detection and [by] exploiting routers' domain-trust relationships [to] pivot[] from international subsidiaries to headquarters in Japan and the U.S."[23] This attack, while arguably not a classic supply chain attack like the others mentioned herein, nonetheless exploits similar tactics and bears a close resemblance to software supply chain attacks in that it clandestinely modifies trusted software, enabling a "deep level of unauthorized access,"[24] that, in the case of such routers, could be used to "manipulate traffic within the network…and [to] surreptitiously route [], capture [], and exfiltrate traffic out of the network to [threat] actor-controlled infrastructure."[25]

And perhaps most concerningly, the DNI earlier this year made clear that China certainly has the access and capability—through a combination of supply chain exploits and other access methods—to "launch[] cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems."[26] Indeed, the DNI warned that China "probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks," noting that "[i]f Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide" in an effort to "deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces."[27] This, of course, is important to consider in the context of China's provocative activities towards Taiwan, including

[22] *See* DOJ, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally* (Sept. 16, 2020), available online at <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>; *see also* CISA, *Software Supply Chain Attacks*, *supra* n. 4 at 4 ("For example, APT 41, a China-based threat actor, routinely undermines codesigning while conducting sophisticated software supply chain compromises against the United States and other countries.").

[23] *See* CISA, *People's Republic of China-Linked Cyber Actors Hide in Router Firmware* (Sept. 27, 2023), *available online at* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a>.

[24] *Id.*

[25] CISA, *People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices* (June 10, 2022), *available online at* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a>.

[26] See DNI, Annual Threat Assessment, supra n. 16 at 10.

[27] *Id.*

the incursion of 43 Chinese warplanes and 7 military vessels into Taiwan's air identification zone and close to the island in just the last month[28]—mimicking activity that it has undertaken numerous times over the past couple of years—as well as China's other threats to U.S. and allied ships in the region in recent days.[29] It is also particularly concerning when one accounts for China as a potential rising superpower and the likely pacing threat for the United States into the next decade.

Likewise, other threat actors, like Iran and North Korea, that are potentially even less deterrable—and almost certainly even more volatile than China or Russia—have also engaged in recent significant efforts to target American and allied software supply chains for exploitation. For example, just last week North Korean threat actors were identified as exploiting a Taiwanese software supplier earlier this Fall in order to install malware on "more than 100 devices in multiple countries, including Japan, Taiwan, Canada and the United States."[30] Iranian activity is particularly important given the ongoing war between Israel and Hamas (an Iranian-backed foreign terrorist organization), the potential for a second front with Hizballah (an Iranian proxy terrorist group) in the north, and expanded Iranian proxy attacks on American forces in Iraq and Syria (and potential American responses). It is even more concerning given that the DNI noted earlier this year that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data" including making "critical infrastructure owners in the United States susceptible to being targeted by Tehran, particularly when Tehran believes that it must demonstrate it can push back against the United States in other domains."[31] Likewise, when it comes to North Korea, the DNI has noted that its "cyber forces have matured and are fully capable of achieving a range of strategic objectives against diverse targets, including a wider target set in the United States" and that "Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States."[32] Each one of these threat actors standing alone would be concerning enough, but taken together, they represent a clear and present danger to the United States, our government, our critical infrastructure, and our people.

Finally, when it comes to the threat scenarios, it is worth noting that the exploitation or compromise of our software supply chain not only has national security implications because of its use for potential espionage or the delivery of destructive malware, but also because of it continued use to

[28] *See* Christopher Bodeen, *China Sends 43 Planes and 7 Ships Near Taiwan in Ongoing Military Pressure Campaign*, Associated Press (Nov. 1, 2023), *available online at* <https://www.pbs.org/newshour/world/china-sends-43-planes-and-7-ships-near-taiwan-in-ongoing-military-pressure-campaign>.

[29] *See, e.g.*, Reuters Staff, *China, US Exchange Accusations over US Vessel in South China Sea* (Nov. 25, 2023), *available online at* <https://www.reuters.com/world/china/china-says-us-destroyer-entered-its-territorial-waters-without-permission-2023-11-25/>.

[30] *See, e.g.*, Carly Page, *North Korea-Backed Hackers Target CyberLink Users in Supply-Chain Attack*, Wired (Nov. 22, 2023), *available online at* <https://techcrunch.com/2023/11/22/north-korea-backed-hackers-target-cyberlink-users-in-supply-chain-attack/> (); Ionut Arghire, *Iranian Hackers Deliver New 'Fantasy' Wiper to Diamond Industry via Supply Chain Attack*, SecurityWeek (Dec. 8, 2022), *available online at* <https://www.securityweek.com/iranian-hackers-deliver-new-fantasy-wiper-diamond-industry-supply-chain-attack/> (describing Iran's targeting of an Israeli software developer in late 2022 to access entities in South Africa, Israel and Hong Kong and to deploy a wiper virus and ransomware capability).

[31] *See* ODNI, *Annual Threat Assessment*, *supra* n. 16 at 19.

[32] *Id*. at 21.

expand the massive economic impact of nation-state-enabled IP theft. As the Committee all too well knows, China has, for many years, engaged in unambiguous economic warfare against the United States and our allies,[33] including through the large-scale, national-level theft of intellectual property from the United States private sector by Chinese state intelligence agencies, providing an economic base for China to build massive state-owned and state-influenced enterprises that now seek to expand across the globe.[34] This nation-state-enabled theft—transferring innovative technology from the United States private sector to the Chinese government and its state-owned and operate companies—is so massive that it has often been described as the "greatest transfer of wealth in modern human history."[35] The cost of this IP theft alone is estimated to total over $600 billion annually,[36] and key elements of this IP theft are increasingly enabled through software supply chain exploitation. Even beyond the physical threat posed by software supply chain exploitation, the risk to the American economy itself constitutes a significant national security threat.

[33] *See* Keith B. Alexander & Jamil N. Jaffer, *China Is Waging Economic War on America. The Pandemic Is an Opportunity to Turn the Fight Around*, Barron's (Aug. 4, 2020), *available online at* <https://www.barrons.com/articles/china-is-waging-cyber-enabled-economic-war-on-the-u-s-how-to-fight-back-51596587400>.

[34] *See* Jamil N. Jaffer, *Updated Statement for the Record: Examining China's Coercive Economic Tactics*, House Committee on Rules (May 10, 2023), *available online at* <https://nationalsecurity.gmu.edu/wp-content/uploads/2023/05/Jaffer-House-Rules-Testimony-on-China-Economic-Coercion-Updated-for-the-Record-5.10.23.pdf>.

[35] *See* Christopher Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, The Hudson Institute (July 7, 2020), *available online at* <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states> ("It's the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history."); Gen. (Ret.) Keith B. Alexander, *Prepared Statement on Digital Acts of War: Evolving the Cybersecurity Conversation*, Subcommittees on Information Technology and National Security of the Committee on Oversight and Government Reform (July 13, 2016), *available online at* <http://nationalsecurity.gmu.edu/wp-content/uploads/2018/05/Gen-Alexander-Statement-Digital-Acts-of-War-7-13.pdf> ("[T]he rampant theft of intellectual property from American private sector companies by nation-states and their proxies[] constitut[es] what I have previously described as the greatest transfer of wealth in human history..."); *see also* Jamil N. Jaffer, *Waking up to the Threat of the Chinese Communist Party: A Call to Action from Congress*, The Hill (Feb. 28, 2023) (op-ed), *available online at* <https://thehill.com/opinion/national-security/3877095-waking-up-to-the-threat-of-the-chinese-communist-party-a-call-to-action-from-congress/>. ("We've known for many years that China has robbed the U.S. of trillions of dollars by pilfering American know-how and technology through theft, extensive hacking, and extortion of American companies operating in China.")

[36] *See, e.g.*, Chairman Mike Gallagher, et al., *Letter to Attorney General Merrick B. Garland from Members of the House Select Committee on the Chinese Communist Party and the House Small Business Committee*, at 1 (June 15, 2023), *available online at* <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/6.15.2023-letter-to-doj-china-select-cmte.-on-small-business.pdf> (*citing The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, The IP Commission (2017) available online at <www.nbr.org/wpcontent/uploads/pdfs/publications/IP_Commission_Report_Update.pdf>).

III. Challenges Facing the Federal Government on Addressing Software Supply Chain Threats and Potential Actions to Address Them

While the federal government has taken significant steps to address software supply chain threats, including removing exploited software from its infrastructure as in the case of the Russian Kaspersky "security" software,[37] and Congress has played a key role in prohibiting the federal government from contracting with entities using certain telecommunications equipment and video surveillance products by key Chinese state-owned or influenced companies, like Huawei,[38] and the Executive Branch in recent years has also sought to partner more closely with the private sector to better share information about cyber threats,[39] much more remains to be done.

First, there is no question that the government and industry must work more closely together to ensure that all the software that the government buys and installs is built consistent with industry best practices, including applying relevant secure-by-design and resilient-by-design principles.[40] All too often, government agencies buy products from the lowest cost provider or an existing approved vendor simply because it is easier, faster, or, at times, required by law. To the extent these requirements come from law, when it comes to the safety and security of our government systems, particularly against software supply chain exploitation, which can have a major effect well beyond a single entity, it is critical that the law be modified to permit flexibility and innovation in purchasing and that the government be required to prioritize the elements of safety and security. To the extent that such purchasing decisions are the result of internal agency directives or, even more troubling, borne of a culture of risk aversion preventing government officials from buying from new providers, it is critical that Congress hold agency heads accountable for such decisions and culture.

Risk aversion can be the right instinct for government purchasers to have, for example, when it comes to buying foreign products from countries of concern, like Russia and China. However, risk aversion goes wrong when it causes government purchasing officials to buy products from the same approved vendors whose prior products have repeatedly shown to be vulnerable or where concerns have not been effectively addressed. It likewise goes wrong when it causes the

[37] *See* CISA, *BOD 17-01: Removal of Kaspersky-branded Products* (Sept. 13, 2017), *available online at* <https://www.cisa.gov/news-events/directives/bod-17-01-removal-kaspersky-branded-products>.

[38] *See John S. McCain National Defense Authorization Act for Fiscal Year 2019*, P.L. 115-232, § 889, available online at <https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf>.

[39] *See, e.g.*, CISA, *JCDC Success Stories*, *available online at* <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-success-stories>; see also NSA, *NSA Cybersecurity Collaboration Center*, *available online at* <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/>.

[40] *See, e.g.*, CISA, *Secure By Design: Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software* (Oct. 25, 2023), *available online at* <https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf>; Office of the National Cyber Director, *National Cybersecurity Strategy*, at 21-22, *available online at* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> ("Together, we can drive investment in critical products and services that are secure- and resilient-by-design, and sustain and incentivize security and resilience throughout the lifecycle of critical infrastructure. The Federal Government will also prioritize funding for cybersecurity research, development, and demonstration (RD&D) programs aimed at strengthening critical infrastructure cybersecurity and resilience. And, the Administration will work with Congress to develop other incentive mechanisms to drive better cybersecurity practices at scale.").

government to make it well-near impossible for government officials to buy the latest innovative capabilities from small American startup companies operating at the bleeding edge of cyber defense. Given that the FBI Director recently testified that as our "adversaries become more sophisticated, we are increasingly concerned about our ability to detect specific cyber operations against U.S. organizations," and noted that "[o]ne of the most worrisome facets [of adversary cyber activity] is their focus on compromising U.S. critical infrastructure, especially during a crisis,"[41] it is all the more critical that the government get its hands on the best cyber defense capabilities available, and that it incentivizes industry to build such capabilities. For far too long, the government has talked about the need to bring in the startup community and engage in more flexible purchasing, and while important steps have been taken in the right direction, the fact is that we simply haven't done nearly enough. Even today, the requirements of the Federal Acquisition Regulations (FAR), including recent updates, make it difficult for small providers to get on contract and directly provide services and products to government customers with scale and speed. Add on to this perhaps well-meaning, but often difficult to comply with rules, protocols, and procedures, officials who are incentivized to be cautious, not forward leaning, as well as a contracting and procurement system that is inherently designed to favor incremental change (if any) over rapid innovation and incumbents over new entrants, and you have a situation that is unlikely to result in good outcomes in the short- or long-run.

Fundamentally, if the government is to get out of its own way on adopting rapidly evolving, innovative technology, and truly keeping up with the scale and scope of threats it is facing, particularly in the cyber domain, it is critical that policymakers inside the executive branch—and, more importantly, the purchasing officials that support them—know that they will not be punished if they take a risk on new technology that doesn't pan out, and that they will be rewarded where such risks pay off. This doesn't mean sacrificing or cutting corners on the security of solutions being adopted by the government, but it does mean allowed procurement officials to lean forward and try new capabilities that might have leap-forward benefits. This requires not just culture change in the Executive Branch but culture change when it comes to oversight and congressional budgeting as well.

Second, if the government is to succeed in its effort to secure its supply chain, it needs to partner with industry and its vendors to share information about the threat landscape, the capabilities it needs to defend itself, and the technologies that can meet—and ideally go beyond—these needs. That requires more transparency from both sides on the sharing of threat information, capabilities, and solutions, and a constant conversation on how to the government can rapidly evolve to meet the rapidly morphing threat. While efforts like the JCDC at DHS and the Cybersecurity Collaboration Center at NSA are absolutely critical moves in the right direction, they need to be significantly resourced, broadened, and deepened, both in terms of what is shared, how widely information is shared, and how operational such relationships get (including how shared classified information can actually be put to work in the operational environment).

Finally, if the government is really going to effectively address the threat posed by nation-state APT actors, it cannot solely remain on the defensive. The government must rapidly expand its capabilities—and willingness—to defend forward and persistently engage the adversary in the first

[41] *See* Wray, *Worldwide Threats*, *supra* n. 3 at 5-6.

instance, an effort that is ongoing, but has proceeded largely in fits and starts as policies and personnel have changed over time. Even more important is truly implementing deterrence in an effective way in the cyber domain. For far too long, the United States has been taking cyber attacks and hacks on the chin with limited response. While, on occasion, cyber threats may rise to the level of a conversation between world leaders and may involve the imposition of some limited economic or cyber consequences (or at least the threat of such consequences), the reality is that the United States does not effectively practice deterrence in the cyber domain for a variety of reasons. First, we generally do not talk about our offensive capabilities in the cyber domain. This makes little sense—as with any other domain of conflict—there will undoubtedly be capabilities we will want to keep close hold; but talking in a limited way about cyber capabilities at all times seems like an unnecessary constraint and one that doesn't ultimately work in our favor. If we are to deter adversaries, we must talk about how we would effectuate that deterrence, whether through cyber capabilities or otherwise.

Likewise, we must be clear about what kind of activity we can tolerate and what kind of activity would cross a line and then, having established a clear line, we must be willing to enforce it and impose significant consequences on bad actors. To date, in the cyber domain as well as others, we have largely been unwilling to establish, much less enforce, effective redlines. Moreover, any such consequences that are to be imposed must be levied not in secret but in the open so that any deterrent effect works not just against the individual bad actor, but against all those who might be considering such action in the future.

While there are those that argue such a policy is too provocative or more likely to get us into a conflict, the reality is that we are already in state of sustained low-level combat in the cyber domain, and that it has gotten worse in recent years not better. The fact of the matter is that when our adversaries don't know how we might react—or worse, based on prior practices assume that we won't react all—they are more likely to push the envelope and test our boundaries. Not only is this bad for the United States because we pay the price for such adversary activity, but such a scenario is actually inherently unstable and therefore likely to lead to more conflict not less.

That's because having been tempted by a lack of American response into trying the next more aggressive thing, at some point our adversary may—whether intentionally or inadvertently—cross a line that neither they nor we understood existed but which, once crossed, requires us to respond in a significant way. Such a scenario is not hard to imagine: we've already seen cyber attacks that have, perhaps inadvertently, resulted in the loss of life, and cyber attacks that (again, perhaps inadvertently) resulted in the temporary shutdown of critical infrastructure, like the Colonial Pipeline. If we continue to maintain a policy of relative ambiguity when it comes to our redlines in the cyber domain, our capabilities to respond, what such a response would look like, and whether we would actually impose significant public costs, we can't be surprised if such half-hearted efforts at deterrence end up being fundamentally ineffective. Deterrence can work in the cyber domain. We just have to be willing to practice it for real.

IV. Conclusion

Thank you again for the opportunity to present my views to the Subcommittee. I look forward to discussing your questions on these important issues and helping find a path forward to address them, as protection of our software supply chain will be a critically important part of America's national security efforts going forward.