AMERICA THE VULNERABLE: THE NATION STATE HACKING THREAT TO OUR ECONOMY, OUR PRIVACY, AND OUR WELFARE

By: Laura Clark Fey[*] *& Sarah D. Wiese*[**]

I. INTRODUCTION

Two thousand twenty, arguably one of the most challenging years in American history, went out with a bang as news developed of our "Cyber Pearl Harbor."[1] On December 13, 2020, while investigating a hack of its systems, cybersecurity firm FireEye discovered a single line of malicious code in a software update received from software vendor, SolarWinds, for its widely used Orion software.[2] Cybersecurity experts attributed the SolarWinds cyberattack to Russia's Foreign Intelligence Service (SVR).[3] The attack provided the suspected

* Laura Clark Fey, one of the first twenty-seven U.S. attorneys recognized as Privacy Law Specialists through the International Association of Privacy Professionals (IAPP), leads Fey LLC, a global data privacy and information governance law firm. She and her team help multinational and U.S. organizations develop and implement practical solutions to their unique data privacy and information governance challenges. Ms. Fey is a member of the inaugural class of IAPP Fellows of Information Privacy (FIP), a Certified U.S. and European Information Privacy Professional (CIPP/US/E), and a Certified Information Privacy Manager (CIPM). The U.S. Department of Commerce and the European Commission selected her as an arbitrator in connection with the former EU-U.S. Privacy Shield Framework Binding Arbitration Program. Ms. Fey teaches Global Data Protection Law at the University of Kansas School of Law and International Issues at Baylor Law School.

** Sarah D. Wiese is Counsel at Fey LLC. The authors would like to thank Eleazar Rundus, Keith Geekie, and Maeve McKinney for their valuable assistance and insights in developing this article.

[1] *See* Steven J. Vaughan-Nichols, *SolarWinds: "IT's Pearl Harbor."*, INSIDER PRO (Mar. 5, 2021), https://www.idginsiderpro.com/article/3609889/solarwinds-its-pearl-harbor.html [https://perma.cc/8AKR-FCL3].

[2] Michael Hess, *The SolarWinds Hack: What Happens Now*, CBT NUGGETS (Dec. 23, 2020), https://www.cbtnuggets.com/blog/certifications/security/the-solarwinds-hack-what-happens-now [https://perma.cc/PKG3-A96H]; *see generally* Brian Krebs, *Malicious Domain in SolarWinds Hack Turned into 'Killswitch'*, KREBS ON SEC. (Dec. 16, 2020), https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/ [https://perma.cc/7K6A-4JCA].

[3] Isabella Jibilian & Katie Canales, *Here's a Simple Explanation of How the Massive SolarWinds Hack Happened and Why It's Such a Big Deal*, BUS. INSIDER (Feb. 25, 2021, 10:03 AM), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-

Russian hackers with privileged access to servers of 18,000 global entities. The hackers targeted specific entities, including U.S. departments and agencies focused on national security, and information technology and cybersecurity corporations. Cybersecurity expert Bruce Schneier summed up the SVR's cyberattack as follows: "[I]t was massive, and it is dangerous."[4] Schneier ominously warned, "Russia is almost certainly laying the groundwork for future attack."[5]

Nation state cyberattacks, like the SolarWinds attack, will continue to escalate, and so will the corresponding risks to our economy and to the privacy and welfare of individual Americans. This article highlights those risks and provides recommendations on potential offensive and defensive responses for the Biden Administration to consider.

The second section of the article provides additional information highlighting the significance of the SolarWinds attack. In the third section, the authors explain why they agree with FBI Director Christopher Wray that the United States requires "a whole-of-society response" to address this very serious threat to our life, liberty, and prosperity. The fourth section provides recommendations for the Biden Administration to consider in three categories: (1) overhauling cybersecurity; (2) improving information governance; and (3) improving America's cybersecurity leadership.

II. SOLARWINDS: A MASSIVE CYBERATTACK

The Biden Administration has only been in power for a short time, but it inherited a massive cybersecurity problem that will continue pose a grave security risk to our nation long after the Biden Administration ends.

A. The Victims

According to news reports, victims of the SolarWinds attack include numerous U.S. Government departments and agencies, including the Department of Homeland Security, Department of Commerce, Department of Energy, the State Department, the Justice Department, the U.S. Treasury, the National Nuclear Security Administration, the National Institutes of Health,

---

security-2020-12 [https://perma.cc/9TWV-NJR7]. On January 5, 2021, the FBI, CISA, the Office of the Director of National Intelligence and the NSA released a joint statement indicating that "an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks," but stopped short of specifically implicating the SVR. *Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure [https://perma.cc/TK23-VHKA].

[4] Bruce Schneier, *Russia's SolarWinds Attack*, SCHNEIER ON SEC. (Dec. 28, 2020), https://www.schneier.com/blog/archives/2020/12/russias-solarwinds-attack.html [https://perma.cc/A7JV-AK68].

[5] *Id.*

NASA, the Federal Aviation Administration, and parts of the Pentagon.[6] The SolarWinds attack also compromised the federal judiciary's electronic case management and filing system.[7] The attack hit at least one unnamed think tank and several U.S. public research universities.[8] In addition, the hackers infiltrated many U.S. corporations, including, among others, technology and cybersecurity

---

[6] *E.g.*, David E. Sanger, Nicole Perlroth & Julian E. Barnes, *As Understanding of Russian Hacking Grows, So Does Alarm*, N.Y. TIMES (Jan. 2, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html [https://perma.cc/QZN8-WXLJ]; Ellen Nakashima & Craig Timberg, *DHS, State and NIH Join List of Federal Agencies—Now Five—Hacked in Major Russian Cyberespionage Campaign*, WASH. POST (Dec. 14, 2020, 10:20 PM), https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html [https://perma.cc/TSK4-MFGY]; Ellen Nakashima & Craig Timberg, *Russian Government Hackers are Behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce*, WASH. POST (Dec. 14, 2020, 10:30 AM), https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html [https://perma.cc/WD22-BJSP]; Natasha Bertrand & Eric Wolff, *Nuclear Weapons Agency Breached Amid Massive Cyber Onslaught*, POLITICO (Dec. 17, 2020, 3:29 PM), https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855 [https://perma.cc/4362-2JK6]; Dustin Volz, *U.S. Agencies Hacked in Foreign Cyber Espionage Campaign Linked to Russia*, WALL ST. J. (Dec. 13, 2020), https://www.wsj.com/articles/agencies-hacked-in-foreign-cyber-espionage-campaign-11607897866 [https://perma.cc/3C8J-CVGZ]; Lily Hay Newman, *Security News This Week: The SolarWinds Body Count Now Includes NASA and the FAA*, WIRED (Feb. 27, 2021, 10:19 AM), https://www.wired.com/story/solarwinds-nasa-faa-robot-dog-fight-security-news/ [https://perma.cc/3CFE-VK9W].

[7] Tim Starks, *Federal courts are latest apparent victim of SolarWinds hack*, CYBERSCOOP (Jan. 7, 2021), https://www.cyberscoop.com/solarwinds-hack-us-courts/ [https://perma.cc/VH4Z-2CN9]; Eric Tucker & Frank Bajak, Justice Department, Federal Court System Hit by Russian Hack, U.S. NEWS (Jan. 6, 2021, 6:52 PM), https://www.usnews.com/news/business/articles/2021-01-06/justice-department-says-its-been-affected-by-russian-hack.

[8] *E.g.*, Betsy Foresman, *After SolarWinds Attack, Universities Double-Check for Compromise*, EDSCOOP (Dec. 29, 2020), https://edscoop.com/after-solarwinds-attack-universities-double-check-for-compromise/ [https://perma.cc/3GJK-GX8L] (listing the University of Texas at San Antonio, Iowa State University, and Kent State University); Lauren Fruen, *Biden is 'considering cyber attacks' on Russian Infrastructure in Retaliation for 'Pearl Harbor of hacks' That Breached 200 US Federal Agencies and Firms – as Fired DHS Cybersecurity Chief Chris Krebs Admits His 'failure' to Stop It*, DAILY MAIL (Dec. 20, 2020), https://www.dailymail.co.uk/news/article-9074231/Joe-Biden-considering-cyber-attacks-Russian-infrastructure-retaliation-hack.html [https://perma.cc/B86W-DRBJ].

companies;[9] telecommunications companies;[10] accounting firms;[11] hospitals;[12] and aerospace and defense companies.[13] Another victim is the California Department of State Hospitals (DSH).[14]

B. The Impact of SolarWinds

The suspected Russian hackers had access to important, sensitive networks for up to nine months before the attack was discovered.[15] And for key targets, it

---

[9] Victims include Microsoft, Intel, Cisco, Nvidia, and FireEye. *See* Matthew Heller, *Nation-State Hackers Breach Cybersecurity Firm*, CFO.COM (Dec. 9, 2020), https://www.cfo.com/cyber-security-technology/2020/12/nation-state-hackers-breach-cybersecurity-firm/ [https://perma.cc/F5RP-XKA3]; David E. Sanger & Nicole Perlroth, *FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State*, N.Y. TIMES (Dec. 8, 2020), https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html [https://perma.cc/PNE6-TA2E] (indicating Russian hackers stole FireEye's "Red Team tools" which imitate the most sophisticated cyberattacks in the world and are designed to test FireEye clients' cybersecurity); Zachary Comeau, *Microsoft Identifies 40+ Victims of SolarWinds Hack, Including IT Companies*, TECHDECISIONS (Dec. 18, 2020), https://mytechdecisions.com/network-security/microsoft-solarwinds-victims-hack [https://perma.cc/62XU-UXEN]; Maria Korolov, *The List of Known SolarWinds Breach Victims Grows, as Do Attack Vectors*, DATA CTR. KNOWLEDGE (Dec. 23, 2020), https://www.datacenterknowledge.com/security/list-known-solarwinds-breach-victims-grows-do-attack-vectors [https://perma.cc/53G4-HU9E].

[10] One example is Cox Communications. Jack Stubbs & Ryan McNeill, *SolarWinds Hackers Broke into U.S. Cable Firm and Arizona County, Web Records Show*, REUTERS (Dec. 18, 2020, 10:27 AM), https://www.reuters.com/article/us-usa-cyber/solarwinds-hackers-broke-into-u-s-cable-firm-and-arizona-county-web-records-show-idUSKBN28S2B9 [https://perma.cc/Y2CL-EJHP].

[11] Ernst & Young is one accounting firm listed as a confirmed victim of the SolarWinds attack. Sam Ingalls, *FireEye, SolarWinds Breaches: Implications and Protections*, ESECURITY PLANET (Dec. 18, 2020), https://www.esecurityplanet.com/threats/fireeye-solarwinds-breaches-implications-protections/ [https://perma.cc/X36Q-PAYN].

[12] Victims include the South Davis Community Hospital, Mount Sinai Hospital, and California Department of State Hospitals. *E.g.*, Fabio Viggiani, *The SolarWinds Orion SUNBURST Supply-Chain Attack*, TRUESEC BLOG (Dec. 17, 2020), https://blog.truesec.com/2020/12/17/the-solarwinds-orion-sunburst-supply-chain-attack/ [https://perma.cc/8VCY-9PWX].

[13] *E.g.*, Ingalls, *supra* note 11 (listing Lockheed Martin as a victim); *see also* Sebastian Moss, *Supply Chain Attack on SolarWinds Used to Breach US Government Agencies*, DATA CTR. DYNAMICS (Dec. 14, 2020), https://www.datacenterdynamics.com/en/news/supply-chain-attack-solarwinds-used-breach-us-government-agencies/ [https://perma.cc/4GZ7-CFBR] (listing Booz Allen Hamilton as a customer of SolarWinds).

[14] Kevin Poulsen, Robert McMillan & Dustin Volz, *SolarWinds Hack Victims: From Tech Companies to a Hospital and University*, WALL ST. J. (Dec. 21, 2020), https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402 [https://perma.cc/5FVK-9VZC]; *Welcome to the Department of State Hospitals*, CAL. DEP'T OF STATE HOSP., https://www.dsh.ca.gov/About_Us/index.html [https://perma.cc/ARE8-5VP9] (describing California state hospital system, which provides mental health services to patients admitted into DSH facilities through the criminal court system who have committed or have been accused of committing crimes linked to their mental illness).

[15] Thomas P. Bossert, *I Was the Homeland Security Adviser to Trump. We're Being Hacked*, N.Y. TIMES (Dec. 16, 2020), https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html [https://perma.cc/NL72-HPQJ]; David E. Sanger, Nicole Perlroth & Julian E. Barnes, *Billions Spent on U.S. Defenses Failed to Detect Giant Russian Hack*, N.Y. TIMES (Dec. 16, 2020), https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html [https://perma.cc/2SJ9-UYS4].

must be assumed the suspected Russian hackers "long ago moved past their entry point, covered their tracks and gained what experts call 'persistent access,' meaning the ability to infiltrate and control networks in a way that is hard to detect or remove."[16] As Schneier advised, "Once inside a network, SVR hackers [Russia's foreign intelligence agency] followed a standard playbook: establish persistent access that will remain even if the initial vulnerability is fixed; move laterally around the network by compromising additional systems and accounts; and then exfiltrate data."[17] The compromise of technology companies like Cisco and Intel gives the SVR "a much deeper foothold into our networks than [was] first thought."[18] It will be years before the targeted networks are secure again . . . if ever.

In the meantime, as Cybersecurity and Infrastructure Security Agency (CISA) has warned, this hostile attack will continue to pose a "grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations."[19]

United States organizations are not the only organizations that have been attacked. The suspected Russian hackers also reportedly attacked networks in Canada, Mexico, Belgium, Spain, the United Kingdom, Israel, and the United Arab Emirates.[20] Microsoft President, Brad Smith asserted:

> This is not "espionage as usual," even in the digital age. Instead, it represents an act of recklessness that created a serious technological vulnerability for the United States and the world. In effect, this is not just an attack on specific targets, but on the trust and reliability of the world's critical infrastructure in order to advance one nation's intelligence agency. While the most recent attack appears to reflect a particular focus on the United States and many other democracies, it also provides a powerful reminder that people in virtually every country are at risk and need protection irrespective of the governments they live under.[21]

The SolarWinds attack provided the Russians with a treasure trove of data—from national secrets to corporate intellectual property.[22] It is highly unlikely that we will ever know the full extent of the data that was taken.

---

[16] Bossert, *supra* note 15.
[17] Schneier, *supra* note 4.
[18] Zachary Comeau, *Why the IT Community Should Be Concerned About the SolarWinds Hack*, MY TECH DECISIONS (Dec. 22, 2020), https://mytechdecisions.com/network-security/it-community-solarwinds-hack/ [https://perma.cc/H4DM-VVWA].
[19] *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Dec. 17, 2020), https://us-cert.cisa.gov/ncas/alerts/aa20-352a [https://perma.cc/7LVM-MAQ4].
[20] Brad Smith, *A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response*, MICROSOFT ON THE ISSUES (Dec. 17, 2020), https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/ [https://perma.cc/2Y3N-CUUU].
[21] *Id.*
[22] *See supra* notes 7–15 and accompanying text.

According to former Homeland Security Adviser Tom Bossert, the access the suspected Russian hackers now have can be used for purposes beyond spying.[23] Among other things, such access could be used to alter data; destroy data; degrade network performance; erase entire networks; impersonate people; or undermine public trust in data, communications, and services.[24] Bossert concluded, "The magnitude of this ongoing attack is hard to overstate."[25]

C. The Nation State Hacking Problem

The SolarWinds cyberattack highlights the rapidly evolving risks of nation state hacking. A large and growing number of countries are leveraging their technological capabilities to launch cyberattacks on our country and on other countries.[26] Each nation state is also developing more avenues of cyberattack, with increasing effectiveness.[27]

Nation states are widely believed to be behind many of the high-profile data breaches and cybersecurity incidents in the last decade. China is suspected of being behind the cyber theft of development data associated with the F-35 aircraft, which reportedly cost the U.S. government over $400 billion to develop.[28] Other costly cyberattacks, including those targeting the National Security Agency, FireEye, and SolarWinds, have been widely attributed to Russian-affiliated threat actors.[29] The cyberattack on Sony Pictures Entertainment, which resulted in the loss of over $41 million of film assets and stock value, was attributed to North Korean threat actors.[30]

Nation states hack for many reasons. A hack may serve a nation state by enhancing the national cyber defenses, collecting intelligence for purposes of

---

[23] Bossert, *supra* note 15.
[24] *Id.*; Schneier *supra* note 4.
[25] Bossert, *supra* note 15.
[26] Smith, *supra* note 20.
[27] MICROSOFT, MICROSOFT DIGITAL DEFENSE REPORT 6 (Sept. 2020), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf [https://perma.cc/MP2Q-LAMR] (indicating that nation states are employing new and more effective espionage, reconnaissance, credential harvesting, and VPN exploits).
[28] Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, THE WHITE HOUSE 35 (Feb. 16, 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [https://perma.cc/T773-2FHC].
[29] *The Growing Threat of Cyberattacks*, HERITAGE FOUND. (2021), https://www.heritage.org/cybersecurity/heritage-explains/the-growing-threat-cyberattacks [https://perma.cc/E85F-S8GJ]; Sanger & Perlroth, *supra* note 9; David E. Sanger, *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES (Dec. 13, 2020), https://www.nytimes.com/2020/12/ 13/us/politics/russian-hackers-us-government-treasury-commerce.html?campaign_id=60&emc= edit_na_20201213&instance_id=0&nl=breaking-news&ref=cta&regi_id=119369714&segment_ id=46817&user_id=f5f49d2cc314e0bd12d27915e9f6dbb8 [https://perma.cc/44RH-ELZF].
[30] Council of Economic Advisers, *supra* note 28, at 16; *see generally Economic Impact of Cybercrime – No Slowing Down*, MCAFEE (Feb. 2018), https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html [https://perma.cc/2ADU-JSK3] [hereinafter McAfee Report].

national security or political order (e.g., stealing military secrets or obtaining information about dissidents), destabilizing a potential enemy's ability to wage war, or performing counterintelligence.[31] From an economic perspective, nation states hack to increase leverage in important negotiations, gain a commercial advantage (e.g., stealing business secrets and intellectual property), or enhance domestic industry growth.[32] Nation states also hack to steal medical and scientific secrets,[33] promote political agendas or social change, control and manipulate the information environment, and meddle in elections. The cyberattacks that are most dangerous to victims are those that are designed to destroy or disable their targets' infrastructure and network capabilities.[34]

Without question, nation state cyberattacks are among the biggest challenges the Biden Administration and our country will face during the next four years. Nation state hacking seriously jeopardizes the economy, privacy, and security of our country.

D. The Evolving Nation State Threat Landscape

The current nation state threat landscape is "distinguished by an expanding array of state and non-state actors with access to various cyber tools or weapons, which may be combined to conduct advanced operations aimed at collection, criminal financial gain, or digital surveillance."[35] Nation states with the most significant hacking capabilities today—besides the United States—include Russia, China, Iran, and North Korea.[36] But the proliferation of cyber tools, either stolen or purchased, as well as the willingness of former U.S. government, intelligence, and military cyber experts to offer their expertise for hire to nation states, presents other nation states with the ability to conduct such attacks as well.[37] Today, thirty nation states are building their cyber capabilities, over twenty are "aggressively" building sophisticated attack technology, and all of

---

[31] *See* KENNETH GEERS, DARIEN KINDLUND, NED MORAN & ROB RACHWALD, WORLD WAR C: UNDERSTANDING NATION-STATE MOTIVES BEHIND TODAY'S ADVANCED CYBER ATTACKS, FIREEYE 3 (2014), https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf [https://perma.cc/T6U9-T65B]; 2019 Public-Private Analytic Exchange Program, *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*, DEPT'.OF HOMELAND SEC. 2 (2019), https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf [https://perma.cc/JA2S-7U9Y].

[32] *See* 2019 Public-Private Analytic Exchange Program, *supra* note 31, at 28.

[33] *See A Global Reset: Cyber Security Predictions 2021*, FIREEYE 5 (2020), https://www.fireeye.com/blog/executive-perspective/2020/11/a-global-reset-cyber-security-predictions-2021.html [https://perma.cc/TG6Y-NX6L] [hereinafter *A Global Reset*]; Jessica Davis, *The Risk of Nation-State Hackers, Government-Controlled Health Data*, HEALTH IT SEC. (Aug. 4, 2020), https://healthitsecurity.com/news/the-risk-of-nation-state-hackers-government-controlled-health-data [https://perma.cc/TYF7-WRKA].

[34] *See* Greg Dobie, *Cyber Attacks on Critical Infrastructure*, ALLIANZ (Apr. 11, 2016), https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html [https://perma.cc/V97P-WJXF].

[35] 2019 Public-Private Analytic Exchange Program, *supra* note 31, at 2.

[36] *A Global Reset*, *supra* note 33, at 7.

[37] 2019 Public-Private Analytic Exchange Program, *supra* note 31, at 3.

them are playing on an ever-more level playing field.[38] Nation state cyberattacks are increasing in volume, sophistication, effectiveness, and covertness.[39] Targets for nation state attacks are also expanding to include not only governmental entities and companies providing critical infrastructure, but also universities, think tanks, and a variety of profit and not-for profit organizations. As evidenced by nation state targeting of organizations involved in COVID-19 response efforts in 2020, targets change as political goals evolve.[40]

The level of risk posed to our country by any individual nation state evolves over time. The cyberattack risk posed by major nation state players like Russia, China, Iran, and North Korea increases from year to year. And the risk exponentially increases when major players join forces. In January of 2021, Russia and Iran entered into an agreement that "envisions 'international cooperation including detection' of cyber intrusions and 'coordination . . . to ensure national and international security.'"[41] The agreement calls for "broad cybersecurity cooperation, including coordination of actions, exchange of technologies, training of specialists, and coordination at the United Nations and other international organizations."[42] This cooperative agreement between two of the major nation state hacking players significantly increases the cyberattack threat posed by each of these countries.

Technological advances, such as artificial intelligence (AI), combined with our hyper-connectivity and the growing availability of big data through an ever-expanding attack surface (e.g., through social media sources, ubiquitous internet of things (IoT) devices, and application programming interfaces (APIs) used for sharing data), will present nation state hackers with new opportunities to

---

[38] Steve Ranger, *US intelligence: 30 countries building cyber attack capabilities*, ZDNET (Jan. 5, 2017), https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/ [https://perma.cc/9JBR-LVEV]; *Foreign Cyber Threats to the United States*, Before the S. Comm. on Armed Services, 117th Cong. (Jan. 5, 2017) (joint statement of James Clapper, Dir. of Nat'l I.; Marel Lettre, Undersec'y of Def. for I.; & Adm. Michael S. Rogers, USN, Cdr., Cyber Command Dir., NSA), https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf [https://perma.cc/4ZAR-RVSD]; Mike O'Malley, *Concerned About Nation State Cyberattacks? Here's How to Protect Your Organization*, SECURITY (Mar. 26, 2020), https://www.securitymagazine.com/articles/91889-concerned-about-nation-state-cyberattacks-heres-how-to-protect-your-organization [https://perma.cc/67YL-X6L7].

[39] 2019 Public-Private Analytic Exchange Program, *supra* note 31, at 7; GEERS ET AL., *supra* note 31; ACCENTURE, THE COST OF CYBERCRIME: NINTH ANNUAL COST OF CYBERCRIME STUDY: UNLOCKING THE VALUE OF IMPROVED CYBERSECURITY PROTECTION 7, 26 (2019), https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 [https://perma.cc/4A9K-RNEV].

[40] MICROSOFT DIGITAL DEFENSE REPORT, *supra* note 27, at 5.

[41] John Hardie & Annie Fixler, *Russia-Iran Cooperation Poses Challenges for US Cyber Strategy, Global Norms*, FOUND. FOR DEF. OF DEMOCRACIES (Feb. 8, 2021), https://www.fdd.org/analysis/2021/02/08/russia-iran-cooperation-challenges-cyber/ [https://perma.cc/N6ZU-P3BV]; *see also* Charlie Mitchell, *Foundation for Defense of Democracies: Russia, Iran Deal Poses Challenges on Cyber and ICT Security*, INSIDE CYBERSECURITY (Feb. 16, 2021), https://insidecybersecurity.com/daily-news/foundation-defense-democracies-russia-iran-deal-poses-challenges-cyber-and-ict-security [https://perma.cc/8VRH-68MM].

[42] Hardie & Fixler, *supra* note 41.

attack.[43] As 5G networks and eventually quantum computing deploy, the risks will increase exponentially.[44]

The Public-Private Analytic Exchange Program, a collaboration of private sector and government intelligence analysts focused on improving intelligence priorities and national security goals, has ominously warned that the "proliferation and commodification of cyber offensive capabilities is reshaping the cyber balance of power."[45] At this time, there are no clear international norms concerning how cyber actors may operate. There appears to be only one red line: the avoidance of the use of cyber capabilities that would lead to war. Activities below that threshold are not regulated.[46] Because the consequences and potential punishments for hacking are uncertain, nation states have an incentive to push the envelope with their hacks until the risks outweigh the benefits.

E. Key Risks Posed by Nation State Cyberattacks

Because of the openness of our society, our interconnectivity (e.g., through Internet of Things (IoT) devices), and our expansive, vulnerable attack surface, America will continue to face significant risks from nation state hacking.[47] Key risks posed by nation state cyberattacks range from economic risks to individual privacy risks to existential risks that threaten the survival of the people and ideals of our nation.[48]

1. Economic Risks to Our Nation and the World

Cyberattacks, including nation state attacks, inflict a host of injuries on the United States and global economy.[49] According to the Ninth Annual Cost of Cybercrime Study by Accenture, an estimated $5.2 trillion is at risk globally

---

[43] Danny Palmer, *The Dark Side of IoT, AI and Quantum Computing: Hacking, Data Breaches and Existential Threat*, ZDNET (Jan. 15, 2020, 10:41 AM), https://www.zdnet.com/article/the-dark-side-of-iot-ai-and-quantum-computing-hacking-data-breaches-and-existential-threat/ [https://perma.cc/CUT3-CN4M]; 2019 Public Private Analytic Exchange Program, *supra* note 31, at 5.

[44] *Most Pros are Concerned About Cybersecurity Risks Related to 5G Adoption*, HELP NET SECURITY (Dec. 8, 2020), https://www.helpnetsecurity.com/2020/12/08/5g-cybersecurity-risks/ [https://perma.cc/D2GV-C4ZD]; Ali El Kaafarani, *Why Quantum Computers Pose a Very Real Risk to Cybersecurity*, INFOSECURITY MAGAZINE (Mar. 10, 2021), https://www.infosecurity-magazine.com/blogs/quantum-computers-risk/ [https://perma.cc/72MB-7J8W].

[45] 2019 Public Private Analytic Exchange Program, *supra* note 31, at 1.

[46] *Id.* at 2.

[47] *Id.* at 5.

[48] *See* SAMANTHA BRADSHAW & PHILIP N. HOWARD, THE GLOBAL DISINFORMATION ORDER: 2019 GLOBAL INVENTORY OF ORGANISED SOCIAL MEDIA MANIPULATION 1 (2019), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf [https://perma.cc/R2AN-8NCX] (describing the dangers of disinformation and division to democracy); MICHAEL J. WALLACE, WILLIAM J. FEHRMAN, J. RICH BAICH, RICHARD H. LEDGETT, JR., CONSTANCE LAU & DR. BEVERLY SCOTT, TRANSFORMING THE U.S. CYBER THREAT PARTNERSHIP 4 (2019), https://www.cisa.gov/sites/default/files/publications/NIAC-Working-Group-Report-DRAFT-508.pdf [https://perma.cc/YZ2N-HHU5] [hereinafter NIAC Working Group] (describing the dangers cyberattacks pose to U.S. infrastructure).

[49] Council of Economic Advisers, *supra* note 28; ACCENTURE, *supra* note 39, at 10–11; McAfee Report, *supra* note 30, at 9.

from cybercrime for the five-year period of 2019 to 2023.[50] A recent report from cybersecurity software company McAfee estimated that, in 2020, over $1 trillion was spent world-wide to (1) recover from $945 billion of cyberattack losses; and (2) pay for $145 billion of cybersecurity investments.[51] These dramatic cybersecurity expenses are equivalent to slightly more than one percent of the global gross domestic product, a massive loss.[52] And the total annual cost of all types of cyberattacks is increasing.[53]

With respect to economic espionage cyberattacks (e.g., intellectual property theft) alone,[54] CyberTheory, an international cybersecurity firm, concluded, "[T]he potential economic harm to American businesses and the economy as a whole [from economic espionage] almost defies calculation."[55] In a 2018 report, the White House Council of Economic Advisers estimated that malicious cyber activity, including nation state cyberattacks, cost the U.S. economy between $57 billion and $109 billion in 2016.[56]

America's economic loss is a hostile nation state's gain. China uses data stolen through Chinese and Chinese-sponsored cyberattacks to boost its economy.[57] Reports indicate North Korean and Russian-affiliated threat actors routinely hack into banks as a source of income.[58]

A single cyber incident can disrupt thousands of systems worldwide and cost billions of dollars. For example, the 2017 Russian-backed NotPetya ransomware cyberattack, the most damaging cyberattack in history, resulted in over $10 billion in damages beginning with injuries to Ukrainian society and spreading to international companies, including FedEx, Merck, and Maersk.[59] Cyberattacks against critical infrastructure sectors, such as the financial and energy industries, could cripple the U.S. economy and decimate our standard of

---

[50] ACCENTURE, *supra* note 39, at 14.

[51] ZHANNA MALEKOS SMITH & EUGENIA LOSTRI, THE HIDDEN COSTS OF CYBERCRIME 3 (2020), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf [https://perma.cc/AVE4-CREK]; Lance Whitney, *How Cybercrime Will Cost the World $1 Trillion This Year*, TECHREPUBLIC (Dec. 7, 2020, 11:50 AM), https://www.techrepublic.com/article/how-cybercrime-will-cost-the-world-1-trillion-this-year/ [https://perma.cc/BUD3-WSU3].

[52] SMITH & LOSTRI, *supra* note 51, at 6.

[53] ACCENTURE, *supra* note 39, at 11.

[54] *Id.* at 7.

[55] Steve King, *Chinese Ambition and Our Existential Threat*, CYBERTHEORY (Oct. 9, 2020), https://cybertheory.io/chinese-ambition-and-our-existential-threat [https://perma.cc/4AK2-8CJK].

[56] Council of Economic Advisers, *supra* note 28, at 56.

[57] Mike McConnell, Michael Chertoff & William Lynn, *China's Cyber Thievery Is National Policy—And Must Be Challenged*, WALL ST. J. (Jan. 27, 2012), https://www.wsj.com/articles/SB10001424052970203718504577178832338032176 [https://perma.cc/2CFY-GRH9].

[58] McAfee Report, *supra* note 30, at 9–10.

[59] *Petya Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (July 1, 2017), https://us-cert.cisa.gov/ncas/alerts/TA17-181A [https://perma.cc/6ZG5-39R9]; CBS News, *What Can We Learn from the 'most devastating' Cyberattack in History?*, CBS THIS MORNING (Aug. 22, 2018, 1:04 PM), https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/ [https://perma.cc/L9VE-BPBK]; *What Is Petya and NotPetya Ransomware?*, MCAFEE (2021), https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html [https://perma.cc/WDH5-E8KM].

living and overall quality of life.[60]

Economic effects of cyberattacks touch every level of our society—from governments to private organizations to individuals. The most sophisticated and costly cyberattacks are often orchestrated by nation state threat actors.[61] According to the Ponemon Institute's 2020 Cost of a Data Breach Report, cyberattacks by nation states cost victim organizations an average of $4.43 million per breach.[62] The economic loss suffered by the victim organizations often extends well beyond breach victims, "thereby magnifying the damage to the economy."[63]

2. Privacy Risks to Individuals

Nation state cyberattacks also pose a serious threat to individual citizens' privacy. For example, American information stolen in Chinese hacks—such as highly confidential job application and security clearance information on over twenty-two million individuals (including more than four million federal government employees) through the Office of Personnel Management data breach; and credit card, passport, and travel information (e.g., who traveled where, when, and with whom) stolen through the Marriott/Starwood data breach—has been collected as raw data for China's Ministry of State Security in order to build data sets on U.S. citizens.[64] The *New York Times* reports the Chinese aim to "build a rich repository of Americans' personal data for future targeting."[65] *Forbes* warned that the "[Chinese] target has increasingly become the individual consumer and small business, both of whom mistakenly believe they are of little value to nation-state hackers."[66] Dmitri Alperovitch, of

---

[60] Council of Economic Advisers, *supra* note 28, 37–43.

[61] *See* IBM SECURITY, COST OF A DATA BREACH REPORT 11 (2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf [https://perma.cc/ZZ5R-JYUG].

[62] *Id.*

[63] Council of Economic Advisers, *supra* note 28, at 1.

[64] Eli Lake, *China's Cache of Hacked American Data Poses Huge Security Risk*, POST & COURIER (Sept. 14, 2020), https://www.postandcourier.com/opinion/commentary/chinas-cache-of-hacked-american-data-poses-huge-security-risk/article_ed06dfde-ff13-11e8-a82b-d3d177a0249c.html [https://perma.cc/JV78-25MD]; Mike Levine & Jack Date, *22 Million Affected by OPM Hack, Officials Say*, ABC NEWS (July 9, 2015, 2:17 PM), https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731 [https://perma.cc/59EJ-CAD2]; Evan Perez, *FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach*, CNN POL. (Aug. 24, 2017, 6:29 PM), https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html#:~:text=The%20FBI%20has%20arrested%20a,officials%20briefed%20on%20the%20investigation [https://perma.cc/7U6C-P66R]; Ellen Nakashima & Craig Timberg, *U.S. investigators point to China in Marriott hack affecting 500 million guests*, WASH. POST (Dec. 11, 2018, 8:53 PM), https://www.washingtonpost.com/technology/ 2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/ [https://perma.cc/R4HG-Z26T].

[65] David E. Sanger, Nicole Perlroth, Glenn Thrush & Alan Rappeport, *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html [https://perma.cc/BF7X-MA8D] [hereinafter NYT Marriott Data Breach].

[66] Paul Lipman, *Why Nation-State Hacking Should Matter to Everyone*, FORBES (June 22, 2018, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/06/22/why-nation-state-hacking-should-matter-to-everyone/?sh=5d50f63c413e [https://perma.cc/HFX4-UPFZ].

cybersecurity firm CrowdStrike, explained in an interview that all the raw data from the Marriott/Starwood breach "is all going back to a data lake that can be used [by Chinese] counterintelligence."[67] The Chinese could use such data for a variety of purposes—from blackmailing corporate executives to influencing political figures, elections, and public debates.[68]

3. National Welfare and Existential Risks

Nation state cyberattacks present serious threats not only to our economic and privacy interests, but also to our stability as a nation. Nation state hacking events pose a very real, immediate threat to our national welfare. Individual livelihoods can be wrecked by malicious code and intellectual property theft; individual freedoms challenged through surveillance and content manipulation; and individual lives lost through attacks on critical infrastructure.

Of highest concern are risks to our critical infrastructure. For many years, the vast majority of us have felt immune to life-threatening consequences of any kind of nation state attacks. With the proliferation in cyber tools and cyberattacks, that is no longer the case. The possibility of a nation state attack on our country's critical infrastructure systems—such as power grids, hospitals, financial systems, and transportation—is no longer science fiction or fantasy. Such attacks have already taken place. In December 2015, an attack on Ukraine's electrical grid attributed to the Russian Advanced Persistent Threat (APT) group Sandworm "targeted power distribution centers and left 230,000 residents without power the day before Christmas."[69] The attackers also disabled backup generators.[70] "'BlackEnergy,' the same Sandworm malware that caused the blackout in Ukraine, has been detected in electric utilities in the United States," including locations like Los Angeles and Salt Lake City.[71] The Brookings Institution warns that "[a] massive and debilitating attack on critical infrastructure in Western Europe and the United States is inevitable."[72]

In December 2019, the President's National Infrastructure Advisory Council (NIAC), composed of representatives from industry and government, warned the "[e]scalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security."[73]

The SolarWinds attack is an important reminder of the vulnerability of our nation and the danger of the digital world it inhabits. An absence of international norms and domestic engagement has granted nation state hackers free rein to steal and destroy valuable data belonging to individuals, organizations, and

---

[67] NYT Marriott Data Breach, *supra* note 65.
[68] Lake, *supra* note 64.
[69] ALINA POLYAKOVA & SPENCER P. BOYER, THE FUTURE OF POLITICAL WARFARE: RUSSIA, THE WEST, AND THE COMING AGE OF GLOBAL DIGITAL COMPETITION 13–14 (2018), https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf [https://perma.cc/6KAG-A82V].
[70] *Id.*
[71] *Id.* at 14.
[72] *Id.*
[73] NIAC Working Group, *supra* note 48, at 4.

countries around the world. Because more nation states have begun to participate in nation state hacking and more private actors have begun to sell their expertise, the risks of destructive and costly cyberattacks are growing rapidly. To check this spiraling threat to global stability and harmony, both the Biden Administration and the whole of our national and global society must take decisive action against it.

III. A "WHOLE-OF-SOCIETY RESPONSE" IS REQUIRED TO ADDRESS THE NATION STATE CYBERATTACK THREAT

Nation state cyberattacks will continue. And the economic, privacy, and security risks posed by such cyberattacks will continue to increase as more and more hostile nations develop their cyberattack capabilities and as attacks further increase in number and sophistication. Deterring and reducing the damage caused by such cyberattacks will require what FBI Director Christopher Wray has described as "a whole-of-society response."[74] In the wake of SolarWinds, corporate executives have touted the importance of collaboration. SolarWinds CEO Sudhakar Ramakrishna asserted, "'The severity and complexity of this attack has taught us that more effectively combatting similar attacks in the future will require an industry-wide approach as well as public-private partnerships that leverage the skills, insight, knowledge and resources of all constituents.'"[75] Microsoft's President Brad Smith similarly advised:

> For four centuries, the people of the world have relied on governments to protect them from foreign threats. But digital technology has created a world where governments cannot take effective action alone. The defense of democracy requires that governments and technology companies work together in new and important ways – to share information, strengthen defenses and respond to attacks.[76]

Moving forward, the defense of democracy clearly will require our government and technology companies to work closely together. It also will require significantly increased collaboration, information-sharing, and sharing of responsibility on the part of a very broad group of stakeholders—including the executive, legislative, and judicial branches of our federal government, state and local governments, governments of other countries, academia, technology companies and other for-profit companies, think tanks, NGOs and other non-profit organizations, and even individual citizens and residents of the United States.

---

[74] Christopher Wray, The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States (July 7, 2020), 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 [https://perma.cc/BA85-6DFT].

[75] Brian Krebs, *SolarWinds: What Hit Us Could Hit Others*, KREBSONSECURITY (Jan. 12, 2021), https://krebsonsecurity.com/tag/teardrop-malware/ [https://perma.cc/CW7C-476Q].

[76] Smith, *supra* note 20.

The Biden Administration can, and must, take on a strong leadership role in improving the cybersecurity of our nation and the world. As Tom Bossert, former Homeland Security Adviser to President Trump, stated in December of 2020: "We are sick, distracted, and now under cyberattack. Leadership is essential."[77]

IV. BIDEN ADMINISTRATION: RECOMMENDED PRIORITIES

The Biden Administration has a huge task before it. It must not only manage the federal government's efforts to eradicate and recover from the SolarWinds incident, but must also significantly improve our country's defensive and offensive cybersecurity moving forward.

A. Responding to the SolarWinds Cyberattack

Shortly after the SolarWinds cyberattack came to light, Biden pledged his administration "will make cybersecurity a top priority at every level of government—and we will make dealing with this breach a top priority from the moment we take office."[78] Biden vowed to "elevate cybersecurity as an imperative across the government, further strengthen partnerships with the private sector, and expand our investment in the infrastructure and people we need to defend against malicious cyberattacks."[79] Biden also signaled an intent to go on the offense against nation state hacking:

> A good defense isn't enough; We need to disrupt and deter our adversaries from undertaking significant cyber attacks in the first place . . . We will do that by, among other things, imposing substantial costs on those responsible for such malicious attacks, including in coordination with our allies and partners. Our adversaries should know that, as President, I will not stand idly by in the face of cyber assaults on our nation.[80]

1. Eradicating and Recovering from the SolarWinds Cyberattack

On December 13, 2020, CISA issued an emergency directive ordering all federal civilian agencies to disconnect or power down SolarWinds Orion software products from their networks immediately.[81] On January 21, 2021,

---

[77] Bossert, *supra* note 15.

[78] Morgan Chalfant & Maggie Miller, *Biden Vows to Make Cybersecurity 'imperative' Following Massive Hack*, THE HILL (Dec. 17, 2020, 2:37 PM), https://thehill.com/policy/cybersecurity/530706-biden-vows-to-make-cybersecurity-imperative-following-massive-hack [https://perma.cc/AG26-3ZP4].

[79] *Id.*

[80] Christina Wilkie, *Joe Biden Warns He Will Be Tough on State Sponsors of Cyberattacks, as U.S. Suffers Massive Hack*, CNBC (Dec. 17, 2020, 5:59 PM), https://www.cnbc.com/2020/12/17/biden-hints-at-a-tougher-stance-against-state-sponsors-of-cyberattacks.html [https://perma.cc/VWT3-W39T].

[81] *CISA Issues Emergency Directive to Mitigate the Compromise of SolarWinds Orion Network Management Products*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Dec. 13, 2020), https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-

President Biden's first full day in office, he ordered the intelligence community to provide a "full assessment" of Russia's involvement in the SolarWinds attack.[82] A key point of inquiry for intelligence officials will be whether the SolarWinds hack "was limited to espionage, or whether 'back doors'[83] placed in government and corporate systems give Russia new abilities to alter data or shut down computer networks entirely."[84]

Eradicating and recovering from the SolarWinds cyberattack will be an extensive process. The government will have to replace huge numbers of computers, network hardware and servers across vast federal networks, while keeping sensitive networks operational.[85] It will need to isolate new networks from the compromised networks. "Cyber threat hunters that are stealthier than the Russians" will need to search for and remove hidden, persistent access controls.[86] Such threat hunters will have to "actively search for, isolate and remove advanced, malicious code that evades automated safeguards."[87] And network operators will need to increase monitoring of internet traffic "to detect and neutralize unexplained anomalies and obvious remote commands from hackers."[88]

The Biden Administration will need to actively manage this process and provide adequate resources—personnel, equipment, and funding—for CISA and the affected agencies to eradicate and recover from the SolarWinds cyberattack. Even with adequate resources, as Vimesh Patel, a former official at the National Counterterrorism Center asserted, "it is unlikely federal agencies will ever have certainty that remnants of the [SolarWinds] hacking campaign have been removed."[89]

2. Implementing an Appropriate Offensive Response

The Biden Administration also will need to determine and implement an appropriate offensive response to the Russian cyberattack. Even before the attack was attributed by the FBI and CISA to Russia, Biden promised to impose

---

solarwinds-orion-network [https://perma.cc/2Q3E-KGL2].

[82] Kylie Atwood, Jennifer Hansler & Vivian Salama, *Biden Orders Investigation into Russian Misdeeds as Admin Seeks Nuclear Arms Treaty Extension*, CNN (Jan. 21, 2021, 6:53 PM), https://www.cnn.com/2021/01/21/politics/biden-new-start-extension/index.html [https://perma.cc/Q3LJ-NL2L].

[83] Kim Zetter, *Hacker Lexicon: What Is a Backdoor?*, WIRED (Dec. 11, 2014, 6:35 AM), https://www.wired.com/2014/12/hacker-lexicon-backdoor/ [https://perma.cc/WSL8-TYVG] ("A backdoor in software or a computer system is generally an undocumented portal that allows an administrator to enter the system to troubleshoot or do upkeep. But it also refers to a secret portal that hackers and intelligence agencies use to gain illicit access.").

[84] David E. Sanger & Julian E. Barnes, *Biden Orders Sweeping Assessment of Russian Hacking, Even While Renewing Nuclear Treaty*, N.Y. TIMES (Jan. 21, 2021), https://www.nytimes.com/2021/01/21/us/politics/biden-russia-cyber-hack-nuclear.html [https://perma.cc/W9CJ-K3KG].

[85] Bossert, *supra* note 15.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] Justin Katz, *Biden Promises 'overwhelming focus' on Hack Recovery*, FED. COMPUT. WEEK (Dec. 22, 2020), https://fcw.com/articles/2020/12/22/biden-cyber-solarwinds-hack-attribute.aspx [https://perma.cc/W6N5-FCV8].

"substantial costs" on the parties responsible.[90] Days after the cyberattack's discovery, Biden's White House Chief of Staff Ron Klain stated the United States' push back will go beyond sanctions: "It's not just sanctions. It's steps and things we could do to degrade the capacity of foreign actors to engage in this sort of attack."[91] *Reuters* reported that options being considered "include financial penalties and retaliatory hacks on Russian infrastructure."[92] On April 15, 2021, the Biden Administration issued an executive order imposing wide-ranging sanctions on Russia for the SolarWinds attack, as well as interference in the 2020 U.S. Presidential election, Russia's occupation of Crimea, and other malign actions.[93] In response to the SolarWinds attack, the Administration formally attributed that attack to the SVR and sanctioned six Russian tech companies that support Russian intelligence services' hacking efforts.[94] Other notable punitive measures for Russia's misdeeds include expelling ten diplomats from the Russian Embassy in Washington, D.C. who were "identified as intelligence officers working under diplomatic cover," imposing sanctions "on all debt Russia issues after June 14, barring U.S. financial institutions from buying government bonds directly from the Russian Central Bank, the Russian National Wealth Fund and the country's Finance Ministry," and imposing sanctions on more than 30 entities and individuals involved in election interference and other disinformation efforts.[95] These sanctions are likely only part of what National Security Adviser Jake Sullivan has previously described as the response of our country to Russia's actions using "a mix of tools seen and unseen."[96]

In determining and exacting punishment on Russia for the SolarWinds attack, the Biden Administration has a key opportunity not only to sanction Russia for the attack, but also to deter other hostile nation states from future cyberattacks on the United States. As James Lewis, senior fellow at the Center for Strategic and International Studies (CSIS), warned, "If we are not willing to do something back, then the bad guys will never stop."[97]

---

[90] Wilkie, *supra* note 80.

[91] Raphael Satter, *Biden Chief of Staff Says Hack Response Will Go Beyond 'just sanctions'*, REUTERS (Dec. 20, 2020, 9:00 AM), https://www.reuters.com/article/usa-cyber-breach/biden-chief-of-staff-says-hack-response-will-go-beyond-just-sanctions-idUSKBN28U0IK [https://perma.cc/5ZKW-YUYU].

[92] *Id.*

[93] Nahal Toosi & Quint Forgey, *Biden Sanctions Russia, Expels Diplomats Over Election Interference*, POLITICO (Apr. 15, 2021, 6:05 PM), https://www.politico.com/news/2021/04/15/biden-sanctions-russia-election-interference-481794 [https://perma.cc/E5HS-WGB2].

[94] Ellen Nakaskima, *Biden Administration Imposes Significant Economic Sanctions on Russia Over Cyberspying, Efforts to Influence Presidential Election*, WASH. POST (Apr. 15, 2021, 4:25 PM), https://www.washingtonpost.com/national-security/biden-to-announce-tough-sanctions-on-russia-over-cyber-spying/2021/04/15/a4c1d260-746e-11eb-948d-19472e683521_story.html [https://perma.cc/KF57-NZAL].

[95] *Id.*

[96] Julian E. Barnes, David E. Sanger & Lara Jakes, *Biden Administration to Impose Tough Sanctions on Russia*, N.Y. TIMES (Apr. 14, 2021), https://www.nytimes.com/2021/04/14/ us/politics/biden-russia-sanctions.html [https://perma.cc/QZ3B-X8XN].

[97] Robert Lemos, *Five Ways Government Can Help Businesses Fight Nation-State Attacks*, EWEEK

B. Improving the Nation's Cybersecurity

The SolarWinds cyberattack once again demonstrates the vulnerability of our government networks to clandestine infiltration and attack, and highlights our country's need to drastically improve our offensive and defensive cyber capabilities. President Biden is keenly aware of the need for action. Biden noted that "[w]e need to close the gap between where our capabilities are now and where they need to be to better deter, detect, disrupt, and respond to these sorts of intrusions in the future."[98] As noted above, President Biden vowed to "make cybersecurity a top priority at every level of government."[99]

Congress has recognized the need for improvements in cybersecurity. The bi-partisan U.S. Cyberspace Solarium Commission (the Commission) was "established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to 'develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences.'"[100] In its final report issued on March 11, 2020 (the Report), the Commission advocated for "a new strategic approach to cybersecurity: layered cyber deterrence. The desired end state of layered cyber deterrence is a reduced probability and impact of cyberattacks of significant consequence."[101] The Commission proposed three layers of cyber deterrence—(1) shape behavior, (2) deny benefits, and (3) impose costs[102]—which are in turn "supported by six policy pillars[103] that organize more than 75 recommendations. These pillars represent the means to implement layered cyber deterrence."[104] On January 19, 2021, the Commission released its "Transition Book for the Incoming Biden Administration," which is intended as a guide for the Administration in "identifying possible early policy achievements and suggesting priorities for

---

(Sept. 5, 2018), https://www.eweek.com/security/five-ways-government-can-help-businesses-fight-nation-state-attacks [https://perma.cc/8BR8-D3ZU].

[98] Maggie Miller, *Biden Calls for Modernizing US Defenses Following Massive Hack*, THE HILL (Dec. 28, 2020, 4:33 PM), https://thehill.com/policy/cybersecurity/531868-biden-calls-for-modernizing-us-defenses-following-massive-hack [https://perma.cc/6XYA-LJLK].

[99] Chalfant & Miller, *supra* note 78.

[100] *Introduction*, U.S. CYBERSPACE SOLARIUM COMM'N, https://www.solarium.gov/ [https://perma.cc/HAF3-46UE].

[101] U.S. CYBERSPACE SOLARIUM COMM'N, FINAL REPORT 1 (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view [https://perma.cc/TBS3-M3GU].

[102] The Commission describes these deterrent layers as follows:

1. *Shape behavior*. The United States must work with allies and partners to promote responsible behavior in cyberspace.
2. *Deny benefits*. The United States must deny benefits to adversaries who have long exploited cyberspace to their advantage, to American disadvantage, and at little cost to themselves. This new approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem.
3. *Impose costs*. The United States must maintain the capability, capacity, and credibility needed to retaliate against actors who target America in and through cyberspace.

Id.

[103] *Id.* at 2–6.

[104] *Id.* at 2.

action over the coming months and years," based on the Commission's original Report.[105]

Improving our nation's ability to defend itself against nation state cyberattacks is a monumental task, and we do not try to cover the entire waterfront of necessary actions in this article, but instead recommend three key actions in each of three different categories that we think are most important: (1) overhauling cybersecurity; (2) improving information governance; and (3) improving America's cybersecurity leadership. Most of the cybersecurity and leadership-related recommendations set forth in this article will have a familiar ring to those who are familiar with the Commission's Report, but we also include recommendations and raise finer points not covered by the Report that we think are similarly important.

1. Significantly Overhauling Federal Cybersecurity

First and foremost, the Biden Administration needs to significantly overhaul the federal government's[106] cybersecurity program. The approach to such an overhaul will have to be multifaceted and well-funded. An entire book could be devoted to this topic. But, for purposes of this article, we will highlight three recommended actions: (1) selecting strong, experienced cybersecurity leaders and team members; (2) significantly improving offensive and defensive cyber capabilities; and (3) markedly updating the federal government's supply chain risk management processes.

a. Selecting and Retaining Strong, Experienced Cybersecurity Leaders and Team Members

The Biden Administration must select and retain well-respected, experienced people to lead and staff the government's cybersecurity initiatives. Leaders with years of high-level cybersecurity expertise are needed to develop strong policies, issue spot, and effectively respond when critical problems arise. The Biden Administration clearly recognizes the importance of this. President Biden's picks for top national security positions are highly regarded and have considerable cybersecurity experience.

Alejandro Mayorkas, the new Secretary of the Department for Homeland Security, spearheaded multiple international cybersecurity agreements as the former deputy DHS secretary under President Obama.[107] Avril Haines, the new Director of National Intelligence, served as CIA deputy director under Obama

---

[105] U.S. CYBERSPACE SOLARIUM COMM'N, TRANSITION BOOK FOR THE INCOMING BIDEN ADMINISTRATION 2 (2021), https://drive.google.com/file/d/1gEx3_3Dlo6eyXX9tia1SnZAJFwcxKlM8/view [https://perma.cc/V6JE-MT7Y].

[106] In this section of the article, the recommendations for the Biden Administration often reference the "federal government." To be clear, the Biden Administration has the ability to set policy for the executive branch federal departments and agencies. Due to the Constitution's separation of powers, the Biden Administration cannot unilaterally set policy for the legislative and judicial branches, but it can coordinate with those branches and can also advocate for legislation to protect those branches of government.

[107] Lucas Ropek, *How Biden Could Change the Conversation on Cybersecurity*, GOV'T TECH. (Nov. 30, 2020), https://www.govtech.com/security/How-Biden-Could-Change-the-Conversation-on-Cybersecurity.html [https://perma.cc/P9M5-WHE5].

during a period that included more integration of cyberoperations into the agency's mission.[108] The new Secretary of the Department of Defense, Retired Army Gen. Lloyd Austin, has significant cyberattack experience.[109] Lisa Monaco, the new Deputy Attorney General, played "a prominent cybersecurity role in the Obama Administration as homeland security adviser."[110] These leaders will all have critical roles to play in carrying out President Biden's pledges on cybersecurity.[111]

On April 12, 2021, the White House announced President Biden would nominate Chris Inglis as the nation's first National Cyber Director and would nominate Jen Easterly as Director of CISA.[112] Inglis "served as Deputy Director of the National Security Agency during both the Bush and Obama Administrations," from 2006 to 2014.[113] Easterly served on the National Security Council under President Obama and "was also a senior official at the National Security Agency and helped build U.S. Cyber Command."[114] On June 17, 2021, the Senate confirmed Inglis, and on July 12, 2021, it confirmed Easterly.[115] The National Defense Authorization Act (NDAA) for fiscal year 2021 created the new National Cyber Director position, representing a key step forward. The National Cyber Director will be the President's principal advisor on cybersecurity policy and strategy[116] and will play a key role in coordinating

---

[108] *Id.*

[109] Caitlin Chin, *After the SolarWinds Hack, the Biden Administration Must Address Russian Cybersecurity Threats*, BROOKINGS INST. (Jan. 11, 2021), https://www.brookings.edu/blog/techtank/2021/01/11/after-the-solarwinds-hack-the-biden-administration-must-address-russian-cybersecurity-threats/ [https://perma.cc/TB9Q-ERPC].

[110] Tim Starks, *Biden Transition Fills Some Top Cybersecurity Personnel Spots*, CYBERSCOOP (Jan. 8, 2021), https://www.cyberscoop.com/biden-transition-cybersecurity-nominees/ [https://perma.cc/92ER-W5QL].

[111] Other notable selections of cyber veterans include Anne Neuberger as deputy national security adviser for cyber and emerging technology on the National Security Council, and Rob Joyce as National Security Agency cybersecurity director. Shannon Vavra, *Rob Joyce Named New NSA Cybersecurity Director*, CYBERSCOOP (Jan. 15, 2021), https://www.cyberscoop.com/rob-joyce-nsa-cybersecurity-director-neuberger/ [https://perma.cc/KVM3-RQPC].

[112] Eric Geller, *Biden Names Former NSA Officials to Key Cybersecurity Positions*, POLITICO (Apr. 12, 2021, 10:38 AM), https://www.politico.com/news/2021/04/12/biden-nominates-former-nsa-officials-480945 [https://perma.cc/B57T-DCFF].

[113] *Id.*

[114] Charlie Mitchell, *Reports: Silvers in Line for CISA post, Easterly to be Nominated for New National Cyber Director Position*, INSIDE CYBERSECURITY (Jan. 22, 2021), https://insidecybersecurity.com/share/12010 [https://perma.cc/4LRR-VGPN]. Earlier news reports indicated that Easterly had been in contention for the National Cyber Director position. *Id.*

[115] Eric Geller, *Senate Confirms Chris Inglis as Biden's Top Cyber Adviser*, POLITICO (June 17, 2021), https://www.politico.com/news/2021/06/17/senate-confirms-chris-inglis-cyber-495075; Tim Starks, *Senate Confirms Former White House, NSA official Jen Easterly as CISA Director After Delay*, CYBERSCOOP (July 12, 2021), https://www.cyberscoop.com/jen-easterly-cisa-director-senate-vote/ [https://perma.cc/89BR-DEQL].

[116] The NDAA for 2021 established a new Office of the National Cybersecurity Director within the Executive Office of the President. The NCD, a Senate-confirmed position, will serve as "'the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of' defensive strategies for federal and critical infrastructure organizations, incident response, diplomatic initiatives relating to cybersecurity, efforts to deter adversaries and industry engagement." Andrew J. Grotto, *How to Make the National Cyber Director Position Work*,

discussions with cybersecurity leaders of federal agencies.

Significantly improving our nation's cybersecurity will require not only great leaders, but also talented people to support them. The Biden Administration should seek to hire and retain the best and brightest cybersecurity and technology personnel, and should pay them accordingly. The Biden Administration should embed cybersecurity into the fabric of the federal government, and regularly and effectively train all of its employees, not just those in cybersecurity or technology-related roles, to always think and act with cybersecurity in mind. In furtherance of increasing our country's cybersecurity and technology talent pool, the Biden Administration also should support educational initiatives designed to increase student knowledge and interest in cybersecurity and technology at the primary, secondary, and post-secondary levels.

b. Significantly Improving Defensive Cybersecurity, while Continuing to Improve Offensive Capabilities

The old adage that the best defense is a good offense does not hold true in the area of cybersecurity. In the cybersecurity realm, a strong offense and a strong defense are both required. The Biden Administration will, of course, need to continue to improve our country's offensive cyber capabilities. And it will need to carefully consider when and how to best use those capabilities in retaliation for nation state cyberattacks on the United States. As cybersecurity consultant Charles Denyer asserted, "The more advanced the United States is in terms of cyber offensive measures, the less likely our adversaries will want to attack the United States, as they'll know full well what the repercussions are."[117] Denyer further stated, "[A] digital detente may be the best or only course that plays out in the long term."[118]

But the Biden Administration also will need to significantly improve the government's defenses against cyberattacks. Bonnie Kristian, a fellow at the think tank Defense Priorities, contends that the United States' current approach to cybersecurity has been too focused on offense, to its peril.[119] Kristian stated, "We do way too many strikes and far too little defense, exposing our agencies and secrets to breaches like [SolarWinds]."[120] In 2017, Reuters reported that

---

LAWFARE INST. (Jan. 15, 2021, 2:40 PM), https://www.lawfareblog.com/how-make-national-cyber-director-position-work#:~:text=The%20head%20of%20the%20ONCD,and%20critical%20infrastructure%20organizations%2C%20incident [https://perma.cc/DFD7-CSNA].

[117] Grant Gross, *Experts See a Shift in Cybersecurity Under a Biden Administration*, WASH. EXAMINER (Dec. 3, 2020, 11:00 PM), https://www.washingtonexaminer.com/policy/technology/experts-see-a-shift-in-cybersecurity-under-a-biden-administration [https://perma.cc/H5BU-QS5L].

[118] *Id.*

[119] Bonnie Kristian, *Sweeping Hack Gives Biden a Mandate to Reorient America's Cyber Strategy*, DEFENSE ONE (Dec. 15, 2020), https://www.defenseone.com/ideas/2020/12/sweeping-hack-gives-biden-mandate-reorient-americas-cyber-strategy/170772/ [https://perma.cc/28LL-LEFN].

[120] *Id.* The United States is understandably guarded about its offensive cyber maneuvers. However, it is widely accepted that Stuxnet—a malicious computer worm that "targets centrifuges used to produce the enriched uranium that powers nuclear weapons and reactors"—was developed by U.S. and Israeli intelligence agencies and used in 2010 to target an Iranian nuclear facility, ultimately

about 90 percent of U.S. federal spending on cyber programs is "dedicated to offensive efforts, including penetrating the computer systems of adversaries, listening to communications and developing the means to disable or degrade infrastructure."[121] As demonstrated by the SolarWinds cyberattack, ten percent of funding focused on defensive efforts clearly is not enough. The federal government needs a stronger, layered cybersecurity program with defense in depth and robust cyber threat detection, as well as cyber threat hunting capabilities to better identify unusual behavior that might signal the presence of malicious activity within networks. A strong cybersecurity program will require continued and significant investments in advanced cybersecurity tools, tradecraft, and emerging technologies.

Ultimately, the Biden Administration should strike a balance between cyber offense and defense—one that shows both strength of capabilities and keen vigilance against threats. Our country must quickly harness its current, albeit arguably fleeting, competitive advantage in technology to prepare offensively and defensively for the increasing dangers that will be posed by future nation state cyberattacks against the United States.

c. Markedly Improving the Federal Government's Supply Chain Risk Management Processes

As SolarWinds reminds us, it is not enough for the Biden Administration to focus only on the government's internal security measures. It also must significantly upgrade the federal government's supply chain risk management processes. As Accenture noted in its Third Annual State of Cyber Resilience report, "40 percent of security breaches are now indirect," with threat actors targeting "the weak links in the supply chain or business ecosystem."[122] Great care must be taken by both the public sector and the private sector in selecting, contracting with, and monitoring third-party vendors, particularly vendors with access to sensitive personal data and other highly confidential data.

With respect to vendor selection, particularly because of the large number of vendors that are permitted to either store or access the federal government's data, it is important for the Biden Administration to have a risk-based process in place for selecting vendors. Vendors with access to large volumes of highly confidential data and IoT vendors should be given a significantly higher degree of scrutiny than non-IoT vendors with access to small volumes of non-confidential data. The selection process should consider not only factors like business reputation, financial condition, and experience, but also a vendor's third-party security assessments and audits, specific data protection and privacy

---

destroying Iranian uranium centrifuges. Josh Fruhlinger, *What is Stuxnet, Who Created It and How Does It Work?*, CSO (Aug. 22, 2017, 2:39 AM), https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html [https://perma.cc/CZ44-MSLP].

[121] Dustin Volz, *Global cyber attack fuels concern about U.S. vulnerability disclosures*, REUTERS (May 12, 2017, 4:48 PM), https://www.reuters.com/article/us-britain-security-hospitals-nsa-idUSKBN1882ZF [https://perma.cc/5VGK-JD7D].

[122] Kelly Bissell, Ryan M. LaSalle & Paolo Dal Cin, *Third Annual State of Cyber Resilience*, ACCENTURE 10 (2020), https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf [https://perma.cc/8MFL-UN2J].

practices, and data breach history.[123] If there is a high degree of risk posed by a vendor data breach, an in-person audit to confirm compliance with applicable regulations and best practices should be required. If there is a low degree of risk, then review of the vendor's third-party security audits and policies and practices may be sufficient.

As SolarWinds teaches us, inquiring about vendor locations is also important. SolarWinds is headquartered in Austin, Texas, but during the last decade, the company moved much of its engineering to Eastern European satellite offices—including the Czech Republic, Poland, and Belarus—"where engineers had broad access to the Orion network management software."[124] SolarWinds has not publicly addressed the possibility of insider involvement in the hack, but Russian intelligence operatives are known to be "deeply rooted" in Eastern Europe.[125]

In contracting with vendors, the federal government should not only include specific contractual terms required by applicable laws and regulations, but also terms requiring compliance with all applicable laws, regulations (e.g., for DoD contractors, Defense Federal Acquisition Regulation Supplement (DFARS)), and industry best practices. Contracts should require vendors to promptly notify the government in the event of any identified non-compliance with applicable laws, regulations, or contractual terms, or in the event of identified security incidents that rise to a specified level of significance. Contracts should require participation in joint security incident response exercises and cooperation in the event of security incidents rising to a specified level of significance or data breaches. In addition, contracts should specify obligations, penalties, and liabilities in the event of non-compliance or data breaches. Contracts also should permit the government to audit the vendor's security practices moving forward at specified intervals and in the event of any identified potential security issues. Correspondingly, the federal government should implement risk-based compliance monitoring processes for confirming that its vendors are, in fact, complying with their cybersecurity obligations.

2. Markedly Improving Information Governance

A second area with certain room for improvement is the federal government's information governance program. Information governance encompasses "the various legal and compliance requirements and risks faced by different information-focused disciplines, such as Records and Information Management (RIM), data privacy, information security, and electronic discovery (eDiscovery)."[126] Good information governance is the foundation of every good cybersecurity program. In this next section of the article, we will highlight three key recommended information governance actions required to

---

[123] *See, e.g.*, Kim Johnson, *Vendor Due Diligence Checklist: 31 Steps to Selecting a Third Party*, BITSIGHT (Apr. 23, 2019), https://www.bitsight.com/blog/vendor-due-diligence-checklist-31-steps-to-selecting-a-third-party [https://perma.cc/3P2Q-9AYP].

[124] Sanger, Perlroth & Barnes, *supra* note 6.

[125] *Id.*

[126] The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95, 104–05 (2019).

support the federal government's cybersecurity. The first is ensuring there is an information governance program in place in all federal agencies in which all employees and contractors with access to information share responsibility for managing data within their systems. The second recommended information governance action is the maintenance of evergreen data maps and data flows. And the third is the timely and secure disposition of information that is no longer needed.

a. Structuring an Information Governance Program in which Federal Employees Share Responsibility for Managing Data

First, the Biden Administration should create an overarching program to ensure each agency has a structured, audited information governance program involving a core committee of cross-functional information governance stakeholders, including not only IT and Legal/Compliance representatives, but also representatives from all other parts of the agency that create, collect, or store data. Each such agency committee should be tasked with assessing the current state of the agency's information governance; developing prioritized plans for improving the agency's governance of information throughout the information lifecycle; setting quantifiable risk reduction and cost reduction goals and measuring and reporting on progress; drafting and updating policies and procedures; and acquiring necessary, secure technology to support the program. Each agency's committee should prioritize its efforts on information governance processes to better manage and protect high risk and high value data. Each committee also should be responsible for obtaining input from employees concerning their actual information governance practices and recommendations for improvement, and for training employees in the agency on required information governance practices. Good information governance requires consistently good information governance practices on the part of all individuals with access to information.

b. Maintaining Evergreen Data Maps and Data Flows

Second, the Biden Administration should hold each federal agency accountable for regularly inventorying its data and developing and maintaining evergreen data maps and data flows. Undergoing a thorough data inventory process will enable each agency to identify the different categories of data it holds (including sensitive personal data and other highly confidential data), and to determine who has access to it, who the agency is sharing it with, and how the agency is protecting it. To keep the data map and data flows "evergreen," the data map and data flows must be timely updated as data collection, storage, and transfer practices change. Knowing what data an agency holds, where it is stored, who has access to it internally, who it is shared with and how, and how it is protected, will enable each agency to make better cybersecurity decisions throughout the information lifecycle, including decisions concerning the level of security required for different systems based on the amount and type of sensitive data contained within such systems.

c. Disposing of Data Debris

Third, the Biden Administration should mandate each agency to implement

processes to dispose of data that is no longer needed. Several years ago, the Compliance, Governance & Oversight Council (CGOC) released survey results showing that sixty-nine percent of data retained by organizations is "data debris" with absolutely no legal, regulatory, or business value.[127] In light of continued, explosive data growth, it is doubtful this percentage would be any lower today. Data debris increases cybersecurity risks, along with other negative consequences (e.g., degraded application performance and difficulty locating needed documents in the midst of the data debris). Steps that will enable the federal government to better manage and better protect the data that is needed to fulfill governmental purposes and legal obligations include: (1) decommissioning applications no longer containing useful information and redundant systems; and (2) implementing legally defensible processes to dispose of unneeded data, including both prospective processes (e.g., implementing automatic deletion processes) and retrospective processes (e.g., conducting legacy information review and remediation processes) to securely dispose of data debris.

3. Improving America's Cybersecurity Leadership

A final area for improvement is America's cybersecurity leadership, both at home and abroad. Although this is an expansive area, we will highlight three recommendations: (1) lead cybersecurity initiatives in America; (2) lead efforts to promote the passage of a comprehensive national data protection law; and (3) play a leadership role in international cybersecurity initiatives.

a. Leading Cybersecurity Initiatives in America

A significant obstacle to the prevention and mitigation of cyberattacks is the dearth of effective collaboration, cooperation, and information sharing—between federal agencies, between governmental entities at the federal, state, and local level, between the federal government and the private sector, and between the government and individuals.[128]

To overcome this obstacle, the Biden Administration first will need to support and promote cybersecurity collaboration, cooperation, and timely information sharing at the governmental level—within the executive branch, with other branches of the federal government, and between federal, state, and local governments. Effective collaboration, cooperation, and information sharing is challenging even within the executive branch level of the federal government because of the different missions, cultures, and legal authorities guiding different government agencies. "This is exacerbated by the different committees and sub-committees that provide congressional oversight."[129]

Second, the Biden Administration will need to increase collaboration, cooperation, and timely information sharing between the government and

---

[127] COMPLIANCE, GOVERNANCE & OVERSIGHT COUNCIL, INFORMATION LIFECYCLE GOVERNANCE LEADER REFERENCE GUIDE 5 (2d ed. 2014), https://cedar.princeton.edu/sites/cedar/files/media/information_lifecycle_governance.pdf [https://perma.cc/DHN9-FJEQ].

[128] *See* Wray, *supra* note 74; Smith, *supra* note 20.

[129] Derek S. Reveron & John E. Savage, *Cybersecurity Convergence: Digital Human and National Security*, 64 ORBIS 555, 569 (2020).

private organizations. This is particularly important because our national security is so closely tied to our economic security, which is closely tied to the cybersecurity of private American organizations. This is also important because much of our country's technology infrastructure and critical infrastructure is owned and controlled by private corporations. As Microsoft President Brad Smith has asserted:

> Unlike attacks from the past, cybersecurity threats also require a unique level of collaboration between the public and private sectors. Today's technology infrastructure, from data centers to fiberoptic cables, is most often owned and operated by private companies. These represent not only much of the infrastructure that needs to be secured but the surface area where new cyberattacks typically are first spotted. For this reason, effective cyber-defense requires not just a coalition of the world's democracies, but a coalition with leading tech companies.[130]

Because our government does not exclusively control the technology that supports it, the government cannot exclusively manage its cybersecurity risks.

The importance of public-private collaboration, cooperation, and information sharing cannot be overstated. As former Director of National Intelligence Dennis Blair testified before the Senate Armed Services Committee in March 2009, "'The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructure.'"[131] Cyberattacks on our nation's critical infrastructure[132] have the potential to cripple our economy and society. In December 2019, the President's National Infrastructure Advisory Council (NIAC) issued a report that, in part, concluded: "U.S. companies find themselves on the front lines of a cyber war they are ill-equipped to win against nation-states intent on disrupting or destroying our critical infrastructure. Bold action is needed to prevent the dire consequences of a catastrophic cyberattack on energy, communication, and financial infrastructures."[133] The Biden Administration should prioritize collaboration, cooperation, and information sharing with private organizations in critical infrastructure sectors, with a particular focus on

---

[130] Smith, *supra* note 20.

[131] Reveron & Savage, *supra* note 129, at 563.

[132] Critical infrastructure is a collection of sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." *Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors [https://perma.cc/NW2T-GXAR]. There are 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear materials, reactors, and waste; transportation systems; and water and wastewater systems. *Id.*

[133] NIAC Working Group, *supra* note 48, at 1.

assisting smaller entities lacking the resources required to fend off nation state cyberattacks.

Both the U.S. government and private sector organizations need each other's support in order to have any chance of adequately addressing the serious risks we face from nation state hacking. Prompt sharing of cyberthreat information by both the government and private organizations is absolutely critical, as are better collaboration and cooperation on both proactive and reactive fronts.

Third, the Biden Administration will need to educate individual Americans on cybersecurity and disinformation risks, as well as cybersecurity best practices. Nation state cyberattacks pose a risk to individual Americans whose personal data has been compromised through nation state hacking attacks (e.g., the "'huge pots of data'" on Americans stored in a Chinese data lake to be used for "'counterintelligence, recruiting new assets, anticorruption campaigns or future targeting of individuals or organizations'"),[134] and to individual Americans who are targeted by disinformation campaigns designed to meet hostile nation states' interests (e.g., the creation of fake social media personas by Russian operatives used to post thousands of advertisements and messages designed to promote racial divisions in the United States).[135] A broad educational initiative, including required courses for American students and public service announcements for the broader public, could go a long way toward informing individuals of the risks of their own behavior in the cyber world. Such efforts could also help convey the gravity of the efforts of nation states and other bad actors to shape individuals' views through disinformation efforts on social media, and to steal and misuse individuals' personal data through nation state and nation state-sponsored cyberattacks. And as future disinformation campaigns and cyberattacks unfold, our government needs to act quickly to educate the broader public on such events and any actions individuals can take to mitigate their individual risk.

b. Leading Efforts to Promote the Passage of a Comprehensive National Data Protection Law

In addition, the Biden Administration needs to play an active role in promoting the passage of a comprehensive federal law focused on personal data protection. As observers have noted, national privacy legislation is a "national-security imperative."[136] According to the Brookings Institution, two primary reasons driving the current view of U.S. officials that data privacy is a national security concern are: (1) the nature of emerging technologies, such as artificial intelligence; and (2) concerns about technology powers of hostile nation states.[137]

---

[134] Sanger, Perlroth, Thrush & Rappeport, *supra* note 65.
[135] William J. Aceves, *Virtual Hatred: How Russia Tried to Start a Race War in the United States*, 24 MICH. J. OF RACE & L. 177, 177 (2019).
[136] Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation is Just a Start*, BROOKINGS INST. (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ [https://perma.cc/D7TY-RF7P].
[137] *Id.*

The United States has an increasingly complex patchwork of local, state, and federal data protection and privacy laws and regulations. One way to better protect privacy and to secure sensitive information in the United States would be to pass a comprehensive national data protection law that preempts state laws that conflict or are inconsistent with the national law. A comprehensive national data protection law that preempts state law would provide organizations with one set of rules for collecting, using, transferring, and storing personal information that they could apply across the board. A comprehensive data protection law would have the benefits of reducing compliance costs; minimizing inefficiencies inherent in the current U.S. patchwork quilt framework; enhancing organizations' abilities to meet their obligations under other global, comprehensive data protection laws; and reducing the likelihood that foreign nations will seek to prohibit or limit cross-border data flows to the United States out of concerns that the United States does not have an adequate level of data protection.[138]

Bipartisan support is growing for a federal data protection law. In 2019 and 2020, the 116th Congress generated "at least 20 proposed privacy bills or drafts."[139] Some of the more prominent recent proposals for a comprehensive national data protection law include the Consumer Data Privacy and Security Act of 2020 (CDSA),[140] the Consumer Online Privacy Rights Act (COPRA),[141] and the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act).[142] Many data protection and privacy experts believe the likelihood of passage of a comprehensive federal data protection law is greater than at any time the past. As Future of Privacy Forum Senior Fellow Peter Swire asserted, "This new Congress has the best chance for comprehensive federal legislation that I've ever seen."[143]

In addition to promoting the passage of a broadly applicable national data protection law, the Biden Administration should consider promoting the passage of additional federal legislation governing Internet of Things (IoT) device security. One such law, the Internet of Things Cybersecurity Improvement Act of 2020—which will "require the federal government's use of IoT devices to conform to basic security requirements"[144]—was signed into law by President

---

[138] *Id.*

[139] Sara M. Watson, *Insider Intelligence Predicts that Congress Will Finally Pass a Federal Data Privacy Law in 2021*, BUS. INSIDER (Dec. 28, 2020), https://www.businessinsider.com/congress-may-finally-pass-federal-data-privacy-law-in-2021-2020-12 [https://perma.cc/LN5K-RG69].

[140] Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020).

[141] Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

[142] Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act, S. 4626, 116th Cong. (2020).

[143] Jennifer Bryant, *2021 'best chance' for US privacy legislation*, IAPP (Dec. 7, 2020), https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/ [https://perma.cc/64DT-MTW4].

[144] Dan Lohrmann, *Groundbreaking IoT Legislation Close to Becoming Law*, GOV'T TECH. (Dec. 5, 2020), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/groundbreaking-iot-legislation-close-to-becoming-law.html [https://perma.cc/P7KK-Q6EP].

Trump on December 4, 2020.[145] The new law orders NIST to develop and publish standards and guidelines for the federal government "on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices."[146]

The Biden Administration should also consider promoting the passage of a broader law imposing specific cybersecurity obligations on all manufacturers of IoT devices sold in the United States. The Brookings Institution has proposed requiring IoT manufacturers "to certify the security of systems built into their products and to clarify cyber risks for consumers over the life cycle of their products."[147] Such an IoT law, combined with a broadly applicable, comprehensive data protection law, could significantly improve our nation's cybersecurity.

c. Playing a Leadership Role in International Cybersecurity Initiatives

Lastly, the Biden Administration should seek to be a cybersecurity leader on the international stage. It should work hard to improve our country's relationship with our current allies, to develop new allies, and to increase our collaboration, cooperation, and timely information sharing with our allies. As hostile nation states continue to launch cyberattacks against the United States and other world democracies, "it is more important than ever for democratic governments to work together—sharing information and best practices, and coordinating not just on cybersecurity protection but on defensive measures and responses."[148]

As the Solarium Commission noted, international law enforcement tools such as criminal indictments and international extraditions "contribute to layered cyber deterrence by signaling the difference between responsible and unacceptable behavior in cyberspace, thereby helping to reinforce norms."[149] Two additional law enforcement tools include Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAs), which help enable the U.S. prosecution of cybercriminals.[150] The Commission recommends streamlining the MLAT/MLAA process and contends doing so would improve attribution and extradition of accused cybercriminals.[151] The Biden

---

[145] Internet of Things Cybersecurity Improvement Act of 2020, H.R. 1668, 116th Cong. (2020).

[146] Sara Friedman, *NIST: Ongoing Work to Establish IoT Security Guidance Will Help on Compliance with New Law*, INSIDE CYBERSECURITY (Jan. 11, 2021), https://insidecybersecurity.com/daily-news/nist-ongoing-work-establish-iot-security-guidance-will-help-compliance-new-law [https://perma.cc/UWP7-TQSZ] (explaining that "[t]he law requires NIST to submit its work to the Office of Management and Budget by early March [2021]. OMB will have 180 days to examine 'agency information and security policies and principles' across the federal government outside 'national security system[s]' and potentially issue 'policies and principles' that align with NIST's work.").

[147] Williams, *supra* note 136.

[148] Smith, *supra* note 20.

[149] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 101, at 51–52.

[150] *Id.* at 52.

[151] *Id.*

Administration should consider this specific recommendation and should also promote and encourage other efforts to strengthen international law enforcement tools.

In addition, the Biden Administration should consider working with its allies to expand and update the Budapest Convention on Cybercrime to provide a more consistent approach to international norms in cyberspace and more predictable consequences for nation state hacking. The Convention on Cybercrime of the Council of Europe (more commonly known as the Budapest Convention) opened for signatures in 2001 and is the only legally binding international treaty on cybercrime.[152] The Budapest Convention "sets common standards on investigations and facilitates criminal justice cooperation in cybercrime cases for its 65 member countries."[153] It has "been ratified by many non-Council of Europe members, including by the United States" in 2006.[154] This treaty is important because it provides "a guidepost for nations to create and harmonize their own comprehensive national legislation on cybercrime. If done adequately, this helps ensure the legal framework is in place to allow for US cooperation with these countries in cybercrime cases."[155] Notably, the Budapest Convention "is not a static treaty and can be updated to meet evolving needs, as is currently being done for a new protocol dealing with electronic evidence."[156]

The Biden Administration also should participate in other global efforts to set clearer boundaries in terms of what is and is not acceptable nation state behavior in cyberspace. As CSIS's James Lewis asserted, "Norms help set behavioral standards . . . . You have to say here are norms that everyone has agreed to, and your behavior deviated from those norms, and so that justifies some kind of punitive action, whether it's public censure or sanctions or something else."[157]

V. CONCLUSION

Nation state cyberattacks will continue—against our government and against private organizations. We are a vulnerable nation because of our heavy reliance on technology in day-to-day living and in the operation of our critical infrastructure, and because of the ever-expanding attack surface as IoT devices continue to proliferate.

Still, there are reasons to be hopeful. For one thing, President Biden clearly understands the nation state cyberattack risk and the importance of improving our nation's cybersecurity, as do leaders of corporate giants, like Microsoft, who

---

[152] Allison Peters & Anisha Hindocha, *US Global Cybercrime Cooperation: A Brief Explainer*, THIRD WAY (June 26, 2020), https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer [https://perma.cc/9JRV-BFUH].
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] Lemos, *supra* note 97.

are increasingly speaking up.

And really, what other choice do we have? We must act as hopeful people. As renowned 20th century inventor and visionary R. Buckminster Fuller asserted, "We are called to be architects of the future, not its victims."[158] This is a critical time, and we must act with a proper sense of urgency. The point made by Steve King of cybersecurity firm CyberTheory with respect to Chinese cyber threats also holds true with respect to cyber threats from other nation states: "It is easy to see where this is headed. If we don't act soon to stop this advance, we will be inevitably taken over and consumed by our own inattention and acquiescence . . . . Tomorrow may be too late."[159]

The Biden Administration's success in the war against nation state cyberattacks will hinge, in large part, on its ability to massively overhaul the federal government's cybersecurity; significantly improve the federal government's information governance; and improve America's cybersecurity leadership. It will also hinge on the willingness of other players in this game, including not only American allies, American universities, and American corporations, but also individual Americans, to recognize and take action to address the serious risks posed by nation state cyberattacks and disinformation campaigns. It is through such collaborative actions that our nation can evolve from America the vulnerable into America the vigilant.

---

[158] *Community Architects Network*, BUCKMINSTER FULLER INST., https://www.bfi.org/ideaindex/projects/2015/community-architects-network [https://perma.cc/6DCE-R643].
[159] King, *supra* note 55.