Cybersecurity Opportunities for the Public and Private Sectors

100 Days In, Cybersecurity Perspectives on the Biden Administration

By: **Cynergy Partners, Inc.** - **Paul Doherty**, **Jim Pflaging**, **Bryan Ware**, **Mark Weatherford**

May 12, 2021

Executive Summary

Cybersecurity threats pose a critical risk to our nation's security, while addressing those threats form an important foundation for growth and innovation. Federal, state, and local government agencies, government suppliers, and private sector organizations should work together on their individual and collective cybersecurity risk postures. The Biden administration should make specific policy, funding, and staffing decisions to improve Federal civilian agency cybersecurity and direct government suppliers, critical infrastructure organizations, and the rest of the private sector to make similar cybersecurity risk management changes. The administration has already made progress in its first 100 days, providing additional funds to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, U.S. General Services Administration's Technology Modernization Fund, and U.S. Digital Service with the passage of the American Rescue Plan Act of 2021. The public and private sectors, however, should move more quickly on the following recommendations, among others, to improve cybersecurity, especially in the wake of the SolarWinds Orion and Microsoft Exchange Server Hafnium breaches, as well as the recent Colonial Pipeline DarkSide ransomware attack.

Federal government cybersecurity staffing recommendations:

1. Fill cybersecurity leadership, policy, and operational positions with qualified candidates as soon as possible
2. Designate and increase defined number of leadership and operational positions for cybersecurity "innovators" and "protectors" from the private sector
3. Clarify the role of National Cyber Director to avoid duplicative positions and unnecessary bureaucracy

Federal government, government suppliers, and private sector recommendations based on recent breaches:

1. Require secure code and trusted software supply chain
2. Expand cybersecurity controls and standards and make them required and auditable
3. Mandate breach reporting

Federal government cybersecurity modernization and procurement recommendations based on COVID-19 relief:

1. Accelerate secure cloud infrastructure and general IT modernization
2. Modernize threat detection, monitoring, and response capabilities across and within the Federal government, state and local government, and government suppliers
3. Empower the Federal CISO to coordinate procurement for all civilian agencies

With these staffing, technology, governance, and procurement changes, the Biden administration would improve security, increase transparency and accountability, and enable innovation across government and private sector cybersecurity.

Introduction

Given the magnitude of the cybersecurity challenges facing the nation, the Biden administration is facing significant pressure to respond quickly and decisively to recent notable events including the Orion, Hafnium, and DarkSide breaches and to provide a meaningful vision for leadership in cybersecurity protection and innovation. Cybersecurity is in the news daily, and issues and lapses are criticized and analyzed with more attention than ever before. The gap in Federal cyber leadership carried over from the previous presidential administration and during the transition creates a separate but no less important challenge for responding with appropriate vigor and urgency. The Biden administration, Federal agencies, and their private sector partners and suppliers will be challenged not only to respond to the recent breaches with practical, near term fixes but also to enact the transformational IT infrastructure change required to better protect against future threats.

The administration's public commentary toward foreign cyber aggression from Russia and China is a clear signal that the new administration plans to behave differently than the previous one. They must now back up the rhetoric with action to capture the nation's adversaries' attention. The passage of the recent COVID-19 relief bill, which includes $650M for Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) cybersecurity risk management programs, and the February 2021 Executive Order on America's supply chains, represent encouraging progress on cybersecurity policy and funding fronts. However, requisite progress on other key issues remains open. The Biden administration should act with more urgency to fill the depleted Federal cybersecurity staff with entrepreneurs and operators and enact substantive changes around product security and standards in response to the recent breaches for both the public and private sectors. Without these important leadership and common-sense changes around standards and information sharing, the administration will find it difficult to execute on the big picture IT transformation required for the government and its suppliers: supply chain cybersecurity, technology modernization, cloud visibility, and coordinated but flexible procurement.

Within the national cybersecurity landscape, citizens, politicians, media, and industry pundits all have a proclivity to overuse the terms 'unprecedented' and 'wake-up call.' Many have made statements such as "The recent Orion breach is unprecedented and should serve as a wake up call to the government and its cybersecurity program" or "The government faces an unprecedented cyber threat from China after the Hafnium breach."

The reality is every breach is a wake-up call, and while some are shocking in their magnitude or audacity, none is truly unprecedented. The industry and media made similar proclamations after Target in 2012, OPM in 2016, and Equifax in 2017, and countless others. The routine use of hyperboles waters down the very real challenges and unique cybersecurity dynamics for the new administration. The private sector as well as Federal and state government organizations are bearing the brunt of cyber-intrusions from adversaries with far more resources and time than any individual organization can muster. A decade ago, nation-state aggressors were the sole responsibility of the government. Today, every organization, large or small, public or private, from every sector of our economy is in the cybersecurity fight from a disadvantaged position and must work better together to help counter the next threat. Though it is important and necessary to respond to each major breach, like SolarWinds Orion and Microsoft Exchange Server Hafnium, it is essential the entire United States cybersecurity industry, but especially the Federal government and its suppliers, does not become too focused on the latest attack at the expense of being prepared for the next one.

While this paper addresses the near-term challenges highlighted by the recent breaches, it is more precisely focused on the challenges and opportunities for the Biden administration, government agencies, government suppliers, and the rest of the private sector to enact the transformational technology and organizational changes necessary to harden the nation's infrastructure and protect against the next attack.

The paper will first cover the staffing challenges faced by the new administration and what they should do about it. Then, in response to the recent breaches, it will recommend some near- and long-term actions to strengthen the software supply chains of the Federal government, government suppliers, and relevant stakeholders in critical infrastructure and the rest of the private sector. It will then cover recommendations for public and private cybersecurity standards, product certifications, and breach reporting requirements. The paper will then review the nation's cybersecurity strategy including technology and cybersecurity modernization efforts and staffing and procurement considerations in the context of the recently passed COVID-19 relief legislation. Finally, the paper will conclude with a review of the first 100-day achievements of the administration that advance cybersecurity in the U.S. and what should be prioritized going forward. The whole paper will consider the private sector's role, specifically government suppliers, in enhancing cybersecurity across the government, critical infrastructure, and the rest of the private sector.

Federal Government Staffing

I. Fill cybersecurity leadership, policy, and operational positions with qualified candidates as soon as possible

Nearing the end of the Biden administration's first 100 days the leadership gap in critical cybersecurity roles across the executive branch of the Federal government remains stark. Whatever the reasons, the previous administration's firings of top-level DHS executives left a leadership gap at the worst possible time for Federal cybersecurity given the critical eye fixed on cybersecurity and the revelations of the Orion, Hafnium, and DarkSide breaches and election security drama at the end of the last administration. There should be more urgency across the executive and congressional branches to confirm and fill senior positions, including but not limited to CISA Director and National Cyber Director. Nonetheless, it is encouraging to see the appointment of the Deputy National Security Advisor, Cyber and Emerging Technologies, as the highest ranking cybersecurity position in the history of the NSC.

In addition to filling these senior leadership positions as soon as possible, the government must move quickly to fill operational and mid-level leadership positions. Congress and the Biden administration recognized this need with the inclusion of $200M in their COVID-19 relief plan to help with the rapid hiring of technology experts.[1] Though the details of this funding have not been announced, hiring IT and cybersecurity folks should be the number one priority. Across the public sector, approximately 33,000 positions, or one in three cybersecurity positions, remain unfilled.[2] The task will be challenging given the pervasive cybersecurity labor shortage which at the lower end is estimated at more than 470,000 open positions in the private sector. Despite the competition, there needs to be a national call to action across the industry for some, including innovators, technical experts, and even entry-level cybersecurity professionals, to serve their country in a time of significant need.

Filling cybersecurity roles in the Federal government has always been difficult due to an archaic hiring process and limitations on salary. According to former Assistant Director Bryan Ware, hiring new people at CISA and at other government agencies takes over a year because of bureaucracy with OPM, immature human capital programs at CISA, and security clearance requirements. The government should prioritize the hiring of cybersecurity professionals in the background check process and implement streamlined hiring processes in CISA like DHS has done previously at agencies like the Transportation Security Administration (TSA). Additionally, emphasis on the creation and distribution of training materials and opportunities could help increase the supply of operators for both the public and private sectors.

[1] https://thehill.com/policy/cybersecurity/534323-biden-includes-over-10-billion-in-cyber-it-funds-as-part-of-covid-19
[2] Cyberspace Solarium Commission, Pages 162 and 165.

II. Designate and increase defined number of leadership and operational positions for cybersecurity "innovators" and "protectors" from the private sector

The Biden administration should actively increase the number of designated roles that require recent private sector industry experience including innovators and technical security experts. The Federal government is responsible not only for its own infrastructure but also has significant responsibilities in the protection of state and local government organizations, government suppliers, critical infrastructure, and the rest of the private sector. Of the major cybersecurity nominations and appointments so far, few have relevant and recent private sector operational security experience. While legal and policy expertise is critical, the skills for working daily in a dynamic operational environment to design, select, and implement effective cybersecurity capabilities are too often overlooked. The government should seek out and appoint more 'doers,' entrepreneurs and operators to modernize government technology infrastructure and protect against new cybersecurity threats through innovation. Technology entrepreneurs and security professionals, such as Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs) from regulated, critical infrastructure industries, would provide valuable hands-on perspective and experience in leading cybersecurity and compliance programs, including ones that must adhere to strict government regulation, and innovating against advanced nation-state actors.

III. Clarify role of National Cyber Director (NCD) to avoid duplicative positions and unnecessary bureaucracy

Recognizing the present leadership challenges, Congress has attempted to impose greater control over the executive branch in response to the recent breaches and election security drama with the passage of the 2021 National Defense Authorization Act (NDAA) in December 2020 which established the position of the NCD. The president should immediately nominate a NCD to be approved by Congress. However, the role also needs clarification to avoid duplication with other government positions. Though the Federal government must have more coordinated leadership of civilian agencies the position as constructed today will not help further that goal and may hinder it. The position has little authority, and sits outside the National Security Council (NSC) process. This creates duplicative, conflicting authority and mandates between the NCD and Deputy NSA for Cyber in addition to overlapping responsibilities with the Federal CISO out of the Office of Management and Budget (OMB). Acknowledging the duplicative nature of the position as it stands today, the Biden administration has initiated a review of the NCD position eliciting criticism from Senators who allege violation of checks and balances of government. This decision to reevaluate potentially duplicative and bureaucracy amplifying positions may enable the government to move with greater haste to enact the change required to mitigate the damage of the next breach.

Cybersecurity Recommendations for the Public and Private Sectors

The response to the SolarWinds Orion and Microsoft Exchange Server Hafnium breaches has been an early test for the Biden administration. While over 18,000 companies were vulnerable and potentially exposed, nine federal agencies and around 100 companies were actually compromised breach victims with the Orion breach and over 33,000 US and 250,000 global companies exposed in the Hafnium breach. The magnitude and severity of these two cybersecurity events are intimidating to the point where it's challenging to know where to begin prioritizing remediation efforts. There was nothing done two years ago, which is about as fast as the Federal budget system can move, to budget for these kinds of attacks. Nonetheless the current administration must take responsibility and act quickly and decisively to mitigate the effects. Second, we must focus on applying the most important lessons from notable breaches and enact the transformational changes required to prevent or at least mitigate the next breaches. Public and private sectors must consider long-term systemic priorities as well as near-term threats. For example, though the security of the 2020 election was an undeniable USG cybersecurity success and these recent breaches were likely impossible to prevent, Russian election meddling the past five years consumed so much of the government's focus that it likely presented a distraction Russian and Chinese actors were able to capitalize on with Orion and Hafnium. Existing government cybersecurity initiatives, such as the U.S. Cyberspace Solarium Commission (CSC), are addressing many of the issues exposed by the recent breaches, including processes and procedures of secure code development, developing new models for a trusted supply chain, new cybersecurity standards, and national cybersecurity breach reporting requirements. The recommendations below will not only address the primary factors contributing to the damage from the recent breaches, but also will be key factors in the Federal government's long term cybersecurity strategy around modernization, incident response, and public-private collaboration.

I. Require secure code and trusted software supply chain

The Orion breach exposed a major technological gap: vulnerabilities in the government's software supply chain. Related, the supplier in question, SolarWinds, appears to have had security gaps in their own software development process. This situation is not unique and is in fact endemic across the public and private sectors including many, perhaps most, global software companies. As a result, many government agencies and private enterprises could have easily been victims of the same type of supply chain attack. Though there is a tendency for the cybersecurity industry to focus on how their own products would have 'stopped' Orion, industry and government should focus on the bigger issue of vulnerable software supply chains. The administration should mandate that government entities and suppliers procure secure software. In a desired state, the government will only buy software from suppliers who have robust supply chain processes and follow good cybersecurity hygiene practices. Developing and delivering secure code takes a concerted effort but the implications of this international supply chain event are clear: the Biden administration must take an active role in mandating that software companies, especially government suppliers, build secure code and that government entities procure secure software.

For the government:

The Orion breach exposed security gaps in SolarWinds' software development processes. These gaps in turn exposed gaps in the government's security operations through the software supply chain. This domino effect is hardly unique, and is in fact endemic across the public and private sectors. When analyzing breaches, the cybersecurity industry and media tend to focus solely on the specific source or vulnerability. Answering the questions such as 'How can we prevent this in the future?' or even 'How did they get in?' require a more holistic approach. Software is both a complex supply chain and highly interconnected operational environment. The Cyberspace Solarium Commission, whose recommendations report was published months before the Orion breach announcement, says it simply and best: "Providers of information technology submit software transparency and software bills of materials for the systems they provide in support of government missions."[3] With insecure code, like most supply chain vulnerabilities, the later in the process a defect is discovered the more difficult and expensive it is to repair. Identifying vulnerabilities in code is challenging and oftentimes occurs after a breach has occurred. The government should mandate that vendors plan for and design out as many of the failures and vulnerabilities as they can to save everybody pain and heartache down the road. For these reasons, the Federal government must focus on 1) developing requirements for the secure development and delivery of software and 2) establishing controls around the acquisition of software that prevents government agencies, government suppliers, and other organizations responsible for critical infrastructure from procuring insecure software.

The President's February 24, 2021 "Executive Order on America's Supply Chains" calls for a one-year review of the vulnerable supply chain, with a particular emphasis on the cyber vulnerabilities associated with the digital supply chain. Fortunately, this initiative is not starting at zero and the administration can utilize existing government initiatives like the U.S. Air Force's secure and agile software delivery program Kessel Run and the Department of Commerce's National Telecommunications and Information Administration's (NTIA) Software Component Transparency effort around the Software Bill of Materials (SBOM). The NTIA's effort around SBOM is already moving rapidly toward standardization. A SBOM is a model for tracking the wide variety of components, modules, sub-routines, etc. of a software application. A SBOM is "effectively a list of ingredients or a nested inventory; a formal record containing the details and supply chain relationships of various components used in building software."[4] Similar to food ingredients and labels, safety labels in chemicals, and hardware bills of materials in industry and manufacturing, the transparency of the SBOM across government and the private sector, especially in critical infrastructure applications will do the following:

- Enable easier detection and tracking of vulnerabilities
- Establish a common set of practices among vendors and industry
- Streamline cooperation among stakeholders; and
- Drive innovation to meet market expectations

Though the NTIA has focused its initial SBOM efforts on the energy community, the model is sound and customizable for different critical infrastructure sectors, the government, and government suppliers.

[3] Cyberspace Solarium Commission, Page 82.
[4] Software Bill of Materials: Transparency in the Software Supply Chain. Information Session for the Energy Community, January 26, 2021. https://www.ntia.gov/files/ntia/publications/ntia_sbom_energy_jan2021overview_0.pdf

For government suppliers:

Digital transformation projects are changing the way business and government deliver goods and services and communicate with citizens, customers, and other stakeholders. As a result, every industry, government agency, and company is in the software business today. Government technology suppliers need to adapt and respond to this reality. According to Microsoft President Brad Smith, over 80% of the organizations affected by the Orion breach were private sector organizations. The SolarWinds corporation reported to the SEC that 18,000 of its 33,000 Orion customers received the malicious updates. Only a small portion of those 18,000 were actually targeted and breached by the Russian espionage operation.

Government suppliers must improve the security of their software supply chains, particularly when providing services to the government. Just like government agencies will eventually verify the security and integrity of their supply chain through the SBOM initiative, government suppliers should do the same. Government suppliers represent an even earlier step in the government's software supply chain and must act accordingly both preemptively and reactively to secure it. Programs like the Cybersecurity Maturity Model Certification (CMMC), discussed in greater detail in a later section, will greatly increase the visibility and accountability of suppliers to deliver secure goods and services.

For the rest of the private sector:

As new vulnerabilities are discovered, private sector companies must behave in a timely manner to secure their code and supply chains and patch their systems. For example, with Hafnium, the Chinese entity responsible for the initial breaches released the exploit information about the vulnerabilities, giving other external threat actors the opportunity to exploit the 250,000 companies using Microsoft Exchange Server. Microsoft quickly released the patches to mitigate the vulnerability. Now each organization now has the responsibility to acknowledge and apply the software patches. According to the Verizon Data Breach Investigations Report, 99.9% of vulnerabilities in use by attackers had been known for more than a year, most with a patch available.[5] Private sector organizations should implement efforts to secure their supply chains, especially software, and at least maintain a timely and more rigorous patching program, a foundational component of any effective cybersecurity operations program.

II. Expand cybersecurity controls and standards and make them required and auditable

For many in both the private and public sectors, cybersecurity is a top, if not number one, risk to their organization.[6] Unfortunately cybersecurity far too often does not receive the proper focus from business or mission leadership. Some use compliance as a proxy for assurance they are secure. In security circles it is often said 'compliance does not equal security.' Translated, this means compliance is necessary but not sufficient. More directly it means achieving compliance does not mean the job is done with security.

Leadership needs to create clear, reliable, auditable standards and controls. For instance, in many organizations cybersecurity risks are discussed superficially with executive leaders and not framed in proper context. Executive leadership across the public and private sectors must prioritize requisite cultural, governance, and operational controls across their senior staff and board of directors. In addition, security leaders need to understand their business or mission and communicate in language that non-technical staff can understand.

Without a culture of security, where the CEO is the head cheerleader and the board of directors is supportive, organizations will continue to allocate the minimum number of resources, believe that a compliance check is real security, and eschew disclosure in an attempt to preserve brand and reputation. With a security culture at the leadership level, organizations have a chance against the adversaries. Without it, organizations will experience the effects of increasingly severe reputational, financial, operational, and strategic risk.

Self-regulation in the cybersecurity industry has not had great success in the private sector. Some members of private industry, wary of government regulation, have attempted to change security culture on their own, but their success has been limited, and now government should step in to encourage it more broadly. Free markets operate best in transparency, and in the case of cybersecurity, the government must encourage companies to be more transparent with legislation and the proper incentives to prioritize security.

For the government:

The Biden administration and Congress should mandate compliance to previously voluntary frameworks like NIST 800-53, NIST Cybersecurity Framework, ISO 27000-1, or any other applicable standards for any organization, but especially government and critical infrastructure suppliers. The current cybersecurity framework landscape is a patchwork of partially voluntary, partially required Federal, state, and industry regimens that leave many organizations with only partial coverage of their infrastructure footprint. As mentioned above, an axiom in cybersecurity is that compliance does not equal security, and in the absence of standards or compliance requirements, companies will often fail to do the "right thing" or to invest sufficient resources in cybersecurity risk management without some incentive. In the electricity industry, the North American Electric Reliability Corporation (NERC) created Critical Infrastructure Protection (CIP) standards in 2008. At the current time, the electricity sector is the only critical infrastructure with mandatory cybersecurity standards and severe financial penalties for non-compliance.

The government should further clarify and modernize existing regulations like the Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA) to specifically account for cybersecurity in other sectors. The Cyberspace Solarium Commission report addresses many of the specific changes, including in the case of SOX: risk assessment requirements, cyber hygiene requirements, and penetration testing metrics, among others, that should be required as part of these amendments.[7] In addition to standards, the Federal government should mandate the rollout of cyber risk committees and incident response plans at the board level for all companies above a certain size, including nonpublic, or any that provide services as government suppliers. The Federal government should also require cybersecurity insurance for those companies rolling out a cyber risk committee and incident response plan.

[7] Cyberspace Solarium Commission, Page 83.

For government suppliers:

For government suppliers, of which there are over 300,000 for the Defense Industrial Base alone, driving alignment between cybersecurity program standards, objectives, and certifications can be daunting. These suppliers need to go further than their non-government supplier competitors in not only achieving adherence to standards like NIST or ISO but also Federal certifications of their products' security and their overall company risk maturity. It is essential for government suppliers to complete government certifications such as the Federal Risk and Authorization Management Program (FedRAMP) for their software and cloud services for civilian agencies and the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) for overall supplier cybersecurity maturity within the DoD. FedRAMP will become even more important in the coming years as the government increasingly moves to the cloud (see section below) and transitions to software-based services. Software suppliers to the government must develop processes for implementing security controls and continuous improvement to achieve FedRAMP Authorized status.

CMMC is a rollup of standards that include the NIST Cybersecurity Framework, ISO 27000-1, and NIST SP 800-171/53, into a simpler approach to identify, measure, and improve supplier compliance. When audited or reviewed, suppliers should be able to not only show compliance but also continuous improvement. CMMC went into effect on January 1, 2021 and will be implemented over the next five years across all DoD contracts.

In 2021, FedRAMP only applies to civilian agencies, and CMMC only applies to DoD. However, suppliers should monitor these programs as they could change in the future as the government centralizes and streamlines these certifications. All government technology suppliers should continuously improve their security qualifications to achieve and maintain these certifications in addition to implementing the other private sector-focused changes outlined below.

For the rest of the private sector:

Each private sector firm should make cybersecurity an ongoing part of their board governance. Within a few years, a dedicated cybersecurity committee at the board will be one sign of a trusted firm. Gartner believes "by 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% in 2020."[8] These committees should require written incident response plans that include clear definitions of events that require board notification and public disclosure. Benefits include:

- Improved cybersecurity literacy, hygiene, and behavior across the entire organization
- Improved trust from investors, customers, stakeholders, and employees
- Improved cybersecurity operations and risk management programs
- Improved ROI on technology initiatives as security is built into the process from the beginning
- A shift toward value-based and risk-based cybersecurity investment decisions

Secondly, trusted organizations should have regular third-party audits of their security controls and operations. At a minimum, companies should be required to conduct annual reviews of their incident response plans and penetration testing of their applications and networks. The board and senior leadership should review all findings associated with these audits and reports.

[8] Gartner Group, January 28, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-

Thirdly, just as the government requires every person to have car insurance, companies should be required to have cybersecurity insurance.

Finally, organizations should promptly and consistently disclose cybersecurity breaches (described in greater detail below). Following a cybersecurity incident, along with legal counsel and an incident response vendor on call to respond quickly to any breaches, companies should begin the notification process and start sharing information with any relevant authorities or industry stakeholders facing similar threats.

Some companies have already begun implementing many of these common sense strategies, but the government should mandate compliance to accelerate adoption and reduce risk across the public and private sectors.

III. Mandate breach reporting

For the government:

The Biden administration and Congress must pass legislation requiring companies to report breaches in a timely manner. Since there is no Federal breach disclosure requirement, the current landscape is a patchwork of compliance obligations and varying state regulations requiring companies to notify breach victims. Since companies struggle to navigate the confusing landscape of state laws and compliance obligations, the Federal government should establish a single Federal law for victim notification, national security, and transparency purposes.

Though greater transparency through this new breach notification requirement is an important consideration and end goal, the security and confidentiality of this threat and incident information is essential as well, especially for national security purposes. Threat intelligence is currently shared broadly and transparently to the point where other threat actors can take advantage of announced vulnerabilities before organizations can patch (i.e. Hafnium). In cases of breach notifications with national security implications, transparency should be limited at least initially to the relevant government authorities (FBI/CISA) and other organizations, including agencies and suppliers, immediately affected by the breach.

Though there should be some liability protections afforded to those who report breaches, especially those with potential national security implications, the government must not excuse sloppy or subpar protections by extending complete protection to companies who disclose breaches.

For government suppliers:

This new breach disclosure requirement would enable more streamlined information sharing and incident response in coordination with other suppliers, the government, and any affected downstream organizations. For instance, without this mandate, the primary entities involved in the Orion breach, FireEye, Microsoft, and SolarWinds had no legal obligation to report it. Though one can argue the ethical or patriotic obligation to do so, and credit to FireEye for first reporting it, government suppliers who handle classified, national security and other important information on a daily basis must immediately report all cybersecurity incidents.

For the rest of the private sector:

Though nearly 100 companies have been identified as victims of the breach, few have reported it in their official documentation. As stated earlier in the standards section, companies will more likely choose to protect themselves and their brands rather than do the “right thing” and report the breach unless legally required to do so. Whether it’s for national security (discussed above), victim notification, or market transparency, companies should report breaches to the Federal government no matter how many people or records were affected.

USG Cybersecurity Strategy

In conjunction with the near-term and priority policy fixes in response to the recent breaches, the Biden administration must implement several fundamental steps to modernize their technology infrastructure and reduce technical debt. During the previous administration, CISA recognized the need for technology modernization to enable greater security visibility, monitoring, and response through its "Five Year Plan" announced June 2020. The Biden administration must empower the General Services Administration's (GSA) Technology Modernization Fund to implement a foundation based on CISA's Five Year Plan to modernize, and then secure, the technology infrastructures of Federal, state, and local governments through flexible and streamlined procurement processes.

I. Accelerate secure cloud infrastructure and general IT modernization

President Biden signed the American Rescue Plan Act of 2021 on March 11, 2021 which, among many relief efforts focused on the American people and businesses, dedicated nearly $2 billion dollars to technology modernization, cybersecurity, and personnel development for the Federal, state, and local governments. The bill included provisions for the following:

- $1 billion for the GSA Technology Modernization Fund
- $650 million for CISA
- $200 million for the U.S. Digital Service[9]

Though these numbers are meaningful, the $1B for the Technology Modernization Fund (TMF) is a fraction of the $9B originally proposed by the Biden administration during the transition. The $650M approved for CISA is only $40M less than what was originally proposed. Though the CISA budgeting approval is an encouraging sign, the reduction in the IT modernization bucket makes the ratio of IT to security spend off by a significant factor. Information technology spending versus cybersecurity spending in most operational organizations is roughly about 10 to 1. Though the total Federal IT budget is $90B, much of that budget is dedicated to maintaining legacy, insecure systems.[10] The administration and Congress should prioritize additional and continuous infusions for technology modernization through the TMF. The ability for CISA and the cybersecurity products and services they procure to secure legacy and broken infrastructure will be very challenging, and there will always be a disproportionate number of incidents on legacy infrastructure. For instance, since Windows 7 is no longer supported by Microsoft and therefore does not receive any more patches from the company, it is challenging to secure no matter how much anyone pays in cybersecurity products and services. Some government agencies and critical infrastructure still rely on Windows 7, such as the Florida water utility plant that suffered a breach in February 2021,[11] and should receive funding to upgrade to a more modern and secure operating system.

[9] https://www.budget.senate.gov/imo/media/doc/American%20Rescue%20Plan%20Act%20SENATE.pdf
[10] https://fcw.com/articles/2021/03/26/comment-wennergren-tmf.aspx
[11] https://www.pcmag.com/news/hacked-water-plant-in-florida-relied-on-shared-password-windows-7

At the end of the day, the Federal government will end up spending more money securing legacy systems than it would if initial resources were deployed to modernize the technology infrastructure in the first place. Through the TMF, the Federal government should prioritize making modern technology improvements, including:

- Moving to the cloud
- Updating its computer operating systems
- Updating or replacing the thousands of other legacy systems and applications with more modern, shared software-as-a-service applications across agencies
- Improving customer (citizen) experience through digital transformation efforts
- Improving system resiliency
- Improving data availability and analytics
- Standardizing secure, strong identity management controls such as those based on FIDO 2.0 including broad adoption of multi-factor authentication and context-based authorization
- Using these modernization efforts as a foundation to move to a cybersecurity zero trust approach (see below)

The government should also prioritize assisting state and local governments and government suppliers with the same. If the federal government mandates that critical infrastructure and private sector organizations patch their systems in a timely manner, the Federal government should do the same. Modern technology environments still have vulnerabilities, as evidenced by an estimated two hundred thousand insecure cloud configurations in use today, 43% of cloud databases unencrypted, and 40% of cloud storage services with logging capabilities disabled.[12] However, if scoped, managed, and configured properly, the USG will suffer fewer and narrower incidents after technology modernization, especially if implemented with security in mind. Historically CISA has had a minimal, board advisory type of role with the TMF. That must change with the new administration especially as the TMF embarks on this major infrastructure modernization program. CISA should play a major role in the TMF, defining and helping implement the security roadmap in conjunction with TMF actions in 2021 and beyond. With only $175M appropriated to the TMF in its first few years and less than $100M cumulatively awarded in TMF projects, the $1B award is a gamechanger for TMF and its leaders should act expeditiously to distribute the funds to agencies.

Government suppliers, specifically the large prime contractors and members of the Defense Industrial Base (DIB), should modernize similarly. Though CISA, which currently dedicates 60% of its budget to Federal cybersecurity and only 15% to private sector protection,[13] intends to increase its assistance to the private sector, given the monumental challenges facing the government to modernize and secure its own technology, suppliers must act as if they are on their own to move to the cloud and upgrade and secure their infrastructure to protect against the next threat.

[12] Cyberspace Solarium Commission, Page 84.
[13] CISA Virtual Industry Day, May 2020, CISA 5 Year Plan.

II. Modernize threat detection, monitoring, and response capabilities across and within the Federal government, state and local government, and government suppliers

Paired with a massive investment in technology modernization through the TMF, CISA, through its American Rescue Plan infusion, must enhance its cybersecurity capabilities to better monitor, detect, and respond to threats utilizing innovative cybersecurity technologies across Federal agencies. Federal government cybersecurity in civilian agencies, led by CISA, is currently highly reactive and defensive because of antiquated infrastructure as well as systems not designed with security in mind. CISA and other cybersecurity defenders often lack visibility and are uncertain about their risk postures of government agencies. Threat actors are innovating and keeping pace with the massive digital transformation underway utilizing automation combined with other offensive capabilities to evade defenders. CISA and the rest of government should match their innovation with:

- Context-based visibility
- Secure cloud
- Data analytics
- Scalable operational enablement and prevention

Of the $650M provided to CISA with the COVID-19 relief act, CISA is making early progress, dedicating portions to the following:

- Improving visibility through the EINSTEIN intrusion detection program, the Continuous Diagnostics and Mitigation (CDM) cybersecurity program, and other programs to help detect anomalous activity on unencrypted workstations and servers and respond to supply chain attacks[14]
- Implementing endpoint protection and response tools to actually block anomalous behavior
- Improving incident response specifically CISA's Hunt and Incident Response Program (CHIRP), which was deployed to agencies in December following the Orion breach (an estimated one third will go to incident response in total)[15]
- Launching a website on best practices for remediating compromised systems from the Orion breach
- Providing detailed guidance to the nine compromised agencies on evicting the Russian adversaries associated with the Orion breach from their networks
- Adding to existing analytics capabilities

Future CISA plans for the relief funding include a transition to a zero trust approach for government systems and applications. The transition to a zero trust approach, where users are assumed to be malicious until they prove otherwise through authentication and context-based authorization, is encouraging. As discussed earlier, the less the government invests in modernizing technology the more challenging a modern approach like zero trust will be to implement. Also, without modernization, the more the share of incident response spend will grow taking funds away from visibility and proactive defense strategies. Though the quick actions and use of relief funding by CISA to shore up its technology programs and help remediate the effects of the Orion breach represent encouraging early progress, CISA and the rest of government must move faster to improve visibility, shore up defenses, and wherever necessary, hire additional talent and procure technologies in an agile and secure fashion.

[14] https://www.fedscoop.com/cisa-network-monitoring-after-solarwinds/
[15] https://www.hstoday.us/subject-matter-areas/infrastructure-security/cisa-leader-agency-must-expand-visibility-into-risks-incident-response-capacity-after-solarwinds/

III. Empower the Federal CISO to coordinate procurement for all civilian agencies

As discussed earlier, though the National Cyber Director (NCD) position as constructed today is potentially duplicative, there remains an opportunity for greater coordination across the Federal civilian sector particularly in procurement. The Biden administration should empower the Federal CISO to coordinate procurement for the Federal civilian sector. Though the position exists today within the OMB, the Biden administration should strengthen it by elevating it and tying it closely with CISA as the two primary organizations for Federal civilian cybersecurity. In this structure, CISA should still lead risk management and information security strategy, assist with operations and response, and define product requirements and overall strategy. At the same time, the Federal CISO would oversee the procurement process and approved vendor and product lists for all civilian government agencies and be able to leverage massive collective buying power to achieve the best pricing for cybersecurity products and services. CISA and this Federal CISO must be tightly integrated so that they can help achieve the delicate balance between procuring premium products with inevitable Federal government budget pressures. In addition to managing the existing product and vendor lists, the Federal CISO should have wide ranging flexibility in conjunction with CISA to procure innovative and cutting edge products in a compressed timeline that do not sit on the product lists in cases of extreme need or in case of major breaches requiring a new or novel technology. Though programs like the U.S. Department of Homeland Security Continuous Diagnostic and Mitigation (CDM) program, established in 2012 to help secure civilian networks, was innovative and forward thinking for its time, the CDM product lists have become so numerous and the process so onerous they ended up favoring entrenched incumbents. The government must avoid this problem by retaining one civilian security product and vendor list while providing flexibility to the government to procure new technologies to combat new threats.

For government suppliers, especially the large prime contractors, they should work with the Federal CISO on government-wide procurement initiatives and provide volume-based, friendly pricing to not only capitalize on the massive market opportunity for themselves but also improve cybersecurity for the entire government. They should also encourage their own suppliers to achieve relevant government certifications while maintaining flexibility to partner with innovative security software vendors who may not have not yet achieved security certifications like FedRAMP or CMMC, but who can otherwise demonstrate mature security practices and controls. Though relevant certifications should be on their roadmap, otherwise demonstrably secure companies should be able to receive waivers from the Federal CISO in cases of immediate need such as after a breach.

Conclusion: First 100 Days and Beyond

The Biden administration has much work to do with little time to waste to mitigate the effects of the recent breaches and implement a long-term strategy to modernize and secure the Federal government's technology infrastructure. The Biden administration, Congress, government agencies, and government suppliers have started moving in the right direction in the administration's first 100 days, including:

- The administration appointing a Deputy National Security Advisor, Cyber and Emerging Technologies, which is the most senior NSC position given to a cybersecurity professional in the history of the White House
- Congress recommending many common sense changes to the country's long term cybersecurity strategy based on Cyberspace Solarium Commission report published during the transition
- The administration initiating a review of the National Cyber Director role to clarify function and avoid duplication of efforts
- Department of Commerce's NTIA SBOM efforts to secure the software supply chain;
- President Biden signing an Executive Order initiating a review on the nation's supply chain, specifically around cybersecurity
- President Biden and Congress passing $2B in IT and security modernization and personnel funding for GSA, CISA, and the Digital Service through the American Rescue Plan Act of 2021
- CISA utilizing the COVID-19 relief funding quickly to remediate the effects of the Orion breach for both the public and private sectors, improve visibility and detection capabilities for civilian agencies, and improve incident response

Though these initial efforts are encouraging, the Federal government, including the administration and Congress, and the private sector must move faster and act decisively on the following recommendations:

- Fill the open cybersecurity leadership and operational positions with not only seasoned government policy professionals, as has been the case historically, but also entrepreneurs and operational technology experts from the private sector with experience in innovation and the actual protection of critical infrastructure
- Clarify the duplicative roles and coordinate the various cybersecurity initiatives across the government to improve cybersecurity strategy from the White House, enable better operational oversight from CISA, and empower the Federal CISO in procurement
- As immediate responses from the Orion, Hafnium, and DarkSide events, and also as long-term strategic actions, mandate secure software procurement for the Federal government, government suppliers, and the rest of the private sector especially critical infrastructure
- Require government and private sector adherence to clear cybersecurity standards, compliance regimens, and product certifications especially for government suppliers
- Require clear and transparent breach reporting across the public and private sectors
- Modernize technology and cybersecurity through additional funding for the Technology Modernization Fund and CISA

If the government fails to hire the right talent, coordinate across branches and agencies, demand improved transparency and cybersecurity risk management in the private sector, and modernize technology and cybersecurity across government, it will spend even more money and time responding to incidents in the future. With momentum and public awareness around cybersecurity at the highest point in history during the early months of the Biden administration in 2021, the Federal government and the private sector has a unique opportunity to improve cybersecurity and transparency to better protect Americans and enable greater innovation across the public and private sectors.

About the Authors

Bryan Ware is a highly regarded technology leader and innovator, having started companies, patented technologies, raised venture capital and private equity, and recently served as the Nation's lead cybersecurity executive at CISA. Bryan is the CEO of Next5, a technology-focused business intelligence company, ensuring US leadership in critical and emerging technologies including AI, quantum, space, bio, and more. He serves on the World Economic Forum's Global Future Council on Cybersecurity and as an advisor to technology companies and investors.

Prior to founding Next5, Bryan was the first Presidentially appointed Director of Cybersecurity at CISA, leading the one thousand person, $1.25 billion organization through a period of intense volatility and aggressive interference from Nationstate adversaries. At CISA, he developed the agency's first five year strategy and plan to modernize its sensor and computing infrastructure, transform the way the agency delivers services, and scale the agency to protect US critical infrastructure. Under his leadership, CISA's operational partnerships with the private sector, national security community, and international partners were significantly enhanced. Prior to his operational role at CISA, Bryan was an Assistant Secretary at DHS, serving as the Secretary's advisor on cybersecurity and emerging technology matters, and leading strategic initiatives across the US government and allies to counter Chinese espionage and unfair business practices.

Bryan is an entrepreneur, co-founding an artificial intelligence company in 1998 which he led as CEO through multiple rounds of Venture Capital investment until it was acquired in 2013 by Haystax. After serving as CTO of Haystax for several years during which he helped the company acquire leading cloud technology and cybersecurity companies, Bryan took over as CEO of Haystax in 2016 until its acquisition in 2018. Bryan started his professional career at leading defense contractors working on advanced technology programs like the Star Wars program, early UAV payloads, and immersive simulations. He holds a degree in Applied Optics from Rose-Hulman Institute of Technology.

Mark Weatherford is the Chief Information Security Officer at AlertEnterprise, the Chief Strategy Officer (and a Board member) at the National Cybersecurity Center, and the Founding Partner at Aspen Chartered Consulting, where he provides cybersecurity consulting and advisory services to public and private sector organizations around the world.

Mark has held a variety of executive level cybersecurity roles including Global Information Security Strategist at Booking Holdings, Chief Cybersecurity Strategist at vArmour, a Principal at The Chertoff Group, Chief Security Officer at the North American Electric Reliability Corporation, and Chief Information Security Officer for the state of Colorado. In 2008 he was appointed by Governor Arnold Schwarzenegger to serve as California's first Chief Information Security Officer and in 2011 he was appointed by the Obama Administration as the Deputy Under Secretary for Cybersecurity at the U.S. Department of Homeland Security.

Mark is a former naval officer where he served as a cryptologist and was Director of Navy Computer Network Defense Operations, Director of the Navy Computer Incident Response Team (NAVCIRT), and established the Navy's first operational red team. He is an investor and on the Advisory Board of several cybersecurity technology companies where he has a very successful track record in helping startups through the M&A process to acquisition.

Jim Pflaging is the founder and managing partner at Cynergy Partners and has over 30 years of Silicon Valley experience including 15 years as CEO of cybersecurity and data management companies. Jim has a proven track record of translating cybersecurity and related technology, policy, and market dynamics into competitive advantage. Currently, he serves on the board of directors of several leading cybersecurity companies including Coalfire, Imperva, SailPoint, Secure Code Warrior, Sophos, and Veracode. Previously he served as the head of the technology sector and strategy practice at The Chertoff Group. He holds a B.S. in Commerce with dual concentrations in Finance and Marketing from the University of Virginia.

Paul Doherty is co-founder and regional manager at Cloudrise, a managed data protection firm powered by automation. A 7+ year cybersecurity entrepreneur, investor, and advisor, Paul oversees business operations for the Americas, Western region and contributes to corporate strategy, business development, and partnerships globally at Cloudrise. He previously led sales at identity and access management startup OverWatchID through its acquisition by SailPoint (NYSE: SAIL) and consulted companies from startups to F500 enterprises while at The Chertoff Group. He's published articles for FCW and The Cipher Brief. He graduated magna cum laude from Georgetown University where he was a member of the USA Rugby National Academic Honor Roll.