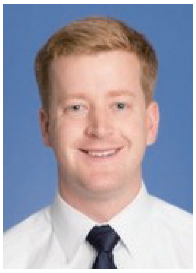
Cybersecurity in the Early Days of the Biden Administration



Author Robert Shields

By Robert Shields

In 2020, Joe Biden focused his presidential campaign on promoting national unity and ending the Covid-19 pandemic. Cybersecurity was not a top priority for either him or the incumbent, President Donald Trump, over the course of an unprecedented election cycle. US presidents, however, do not have full control of their policy agendas. They must respond to the most immediate challenges facing the country. Indeed, major cyber threats to US federal government networks, the rapid growth in ransomware targeting US industry, and troubling cyber vulnerabilities in US critical infrastructure have forced President Biden to prioritize cybersecurity since he took office on Jan. 20, 2021.

As with any policy challenge, there is no single "silver bullet" solution to "solve" cybersecurity in the United States. Biden, like his predecessors, is taking a step-by-step approach to better manage current cyber threats and prepare for the future cyber threat landscape.

Cyber Threats Facing the Biden Administration

Biden entered office amid a federal investigation of one of the most severe cyberattacks ever executed against the US government: the SolarWinds hack. In late 2020, the US government discovered a major supply chain hack impacting several government agencies. After months of investigation, the government concluded that a sophisticated, state-sponsored hacking group infiltrated potentially thousands of public and private computers through US software company SolarWinds. The hackers, likely of Russian origin, breached the networks of at least nine federal agencies and 100 private sector companies via a remote software update from SolarWinds.

SolarWinds was only the beginning for Biden. In early 2021, Microsoft announced that a Chinese government-backed hacking group called HAFNIUM had successfully infiltrated its "Microsoft Exchange" email servers, potentially impacting thousands of clients.

On May 7, cybercrime group DarkSide deployed ransomware against Colonial Pipeline, which operates the largest petroleum product pipeline in the US. The attack encrypted the company's information technology (IT) systems and requested a ransom payment in bitcoin for the "decryption key" to restore access to the encrypted data. In response, Colonial Pipeline took its operational technology (OT) systems offline to contain the threat, which temporarily halted all pipeline operations, causing major gasoline supply disruptions for a week before the company could resume normal operations of its pipeline. It was later reported that Colonial Pipeline paid a $5 million ransom to DarkSide for the "decryption key" to regain access to its digital systems. In fact, the decryption key it received was faulty, forcing Colonial Pipeline to work with a third-party company to reconstitute its IT systems without decrypting its data.

On June 1, the world's largest meat processing company, JBS, announced it was a victim of a ransomware attack that disrupted meat production at its North American facilities. Later that day, the White House stated that it believed that a "criminal organization likely based in Russia" was responsible for the ransomware attack. JBS paid an $11 million ransom for the decryption key to regain access to its digital systems.

On July 3, the FBI announced that it was partnering with the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security (DHS) to investigate a supply chain ransomware targeting US software company Kaseya. According to cybersecurity experts, hackers from the Russia-based REvil cybercrime group exploited a vulnerability in Kaseya's VSA remote monitoring and management software, which is used by managed service providers to provide remote services to their clients. The attack was estimated to have impacted thousands of Kaseya's clients.

Sophisticated cyber threat groups are expected to continue to accelerate attacks against US government and private sector organizations.

Biden's Approach to Cybersecurity

The string of major cyberattacks targeting US entities over the past year forced the Biden administration to make cybersecurity a top priority. Leading its initial "crisis response" activities has been White House Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger. In addition, the administration has begun to formulate key cybersecurity priorities to address the evolving cyber threats. These priorities are: federal government cybersecurity; ransomware; and critical infrastructure security. Notably, the issue of supply chain security cuts across each of these priorities.

The administration has also established a new office within the White House to foster a more integrated, whole-of-government cybersecurity approach. On July 12, Chris Inglis was sworn in as the first-ever National Cyber Director (NCD). The role of the NCD – a position created by Congressional legislation in late 2020 – is to coordinate the various cybersecurity components of the US government to develop a comprehensive and unified approach to the nation's cybersecurity.

Below is a detailed review of key actions and initiatives of the Biden administration with each of these three priority areas.

Priority 1: Federal Government Cybersecurity

On May 12, 2021, Biden issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*. The EO is the first step in a much larger campaign by the administration to improve the cyber defenses of the US federal government. It aims to prevent cyber intrusions into federal IT systems by upgrading the federal government's IT security protocols and securing the software used in federal IT systems. It also aims to establish uniform cyber incident response standards in cases when a significant cyberattack impacts federal government networks.

Notably, however, EOs can only provide directions to federal Executive Branch agencies. The EO includes the following directives:

- First, remove barriers to sharing threat information between federal contractors and the US government.
- Second, modernize federal government cybersecurity.
- Third, enhance software supply chain security.
- Fourth, establish a Cyber Safety Review Board.
- Fifth, standardize the federal government's playbook for responding to cybersecurity vulnerabilities and incidents.
- Sixth, improve detection of cybersecurity vulnerabilities and incidents on federal government networks.
- Seventh, improve the federal government's investigative and remediation capabilities.
- Eighth, ensure consistency between civil and national security systems *(Photo 1)*.

Since then, the Executive Branch has been busy implementing these EO provisions. For example, the National Institute of Standards and Technology (NIST), National Telecommunications and Information Administration, and the White House Office of Management and Budget (OMB) have worked to implement the EO's sections on software supply chain security by publishing recommended security measures for critical software, the minimum elements for a software bill of materials, and a new Memorandum instructing how federal agencies can "protect critical software through enhanced measures". OMB also issued Memoranda on improving the US federal government's investigative and remediation capabilities as well as on implementing a federal "zero trust" network strategy. These are only the initial steps to implement Biden's EO.

Photo 1: White House

Biden hosts national security briefing on cyber threats.

While the primary purpose of Biden's EO is to secure federal networks, US government officials also hope that the benefits of cyber-secure federal networks cascade across the US private sector. For example, some of the EO's requirements involve improving the cybersecurity posture of government contractors. The significant purchasing power of the federal government as a market mover is therefore being used as a driver for higher cybersecurity standards across US industry.

From a Congressional perspective, the US Senate's Committee on Homeland Security and Governmental Affairs is supporting legislation that would update the US government's primary federal cybersecurity law. Under the *Federal Information Security Modernization Act of 2014* (FISMA 2014), the DHS was designated as the authoritative administrator of cybersecurity policies across federal agencies. FISMA 2014 also gave OMB oversight power over federal cybersecurity activities. A new bill being considered by Congress, called FISMA 2021, aims to provide important updates to federal cybersecurity practices. For example, the bill would require all federal civilian agencies to report major cyber incidents to CISA and to Congress.

The Senate Homeland Security Committee's support for the FISMA 2021 demonstrates Congress's concern for federal cybersecurity and its resolve to improve the situation. Indeed, both the Senate and the

House are positioning the US Congress to continue its close oversight of federal cybersecurity and to drive additional legislation aimed to bolster federal network security.

Priority 2: Combatting Ransomware

The US government is now facing an unprecedent surge in ransomware attacks targeting a wide range of economic sectors. In response, the Biden administration is developing a multi-faceted approach to disrupt and deter cybercriminal groups and help US businesses protect their networks against attacks. The administration has already taken several steps to disrupt cybercriminal networks and undermine their ability to operate. While these actions primarily serve to preempt future ransomware attacks, the administration also hopes that these actions, in time, will make US industry a less-attractive target for cybercriminals.

In the summer of 2021, the Department of Justice (DOJ) elevated the priority of ransomware attacks to a level similar to terrorist investigations. This prioritization aims to promote better coordination of DOJ investigations into ransomware across US Attorneys General offices in all 50 states. The DOJ also established a Task Force to advance these efforts. In addition, the Department of Treasury issued an advisory warning in September 2021 stating that ransomware payments to cybercriminal groups may violate Office of Foreign Assets Control (OFAC) sanctions. Under this new policy, the Department of Treasury may impose civil and/or financial penalties against US citizens or organizations that make or facilitate ransomware payments to entities on OFAC's sanctions list *(Photo 2)*.

The US Department of State (DOS) is also now offering rewards of up to $10 million for information leading to the identification of persons who participate in cyberattacks against US infrastructure. This new reward policy will be administered through DOS's "Rewards for Justice" program, which traditionally issues rewards for identifying international terrorists. In addition, US military and intelligence organizations such as US Cyber Command and the National Security Agency (NSA) are executing cyber operations to address cybercriminal threats.

Photo 2: Department of Justice

DOJ leadership holds conference on ransomware threats.

The Biden administration is also working to bolster US industry's resiliency against ransomware attack. The White House, DHS's CISA, and NIST are spearheading outreach efforts and publishing resources to improve the US private sector's cyber readiness. For example, Neuberger sent a letter to corporate executives and business leaders in June 2021 listing best practices to protect their networks from ransomware attacks.

CISA has been leading US government outreach efforts to the US private sector and providing updated guidance on the latest ransomware threats. On Sept. 22, 2021, CISA partnered with the FBI and NSA to issue a new a joint cybersecurity advisory alerting organizations to increased cyberattacks using the "Conti" ransomware strain. The advisory provided technical information related to this type of ransomware and encouraged network defenders to examine their current cybersecurity posture and apply the recommended mitigation policies.

NIST is also developing new voluntary, technical guidance to help companies guard against ransomware attacks. NIST is working to finalize a draft publication entitled *NIST Internal Report (NISTIR): Cybersecurity Framework Profile for Ransomware Risk Management*. This document aims to create a "Ransomware Profile" that identifies security objectives to prevent, respond to, and recover from ransomware events.

Biden also understands the global nature of ransomware campaigns. Indeed, many of these attacks are carried out by transnational criminal groups that offer "ransomware-as-a-service" to customers. To address these sophisticated and transnational threats, Biden is seeking to leverage the capabilities of international allies and partners. Indeed, on Oct. 6-7, the White House hosted a two-day virtual meeting with over 30 allies and partners (including Japan) with the goal of accelerating international cooperation to address ransomware threats. The meeting, called the "Counter Ransomware Initiative", resulted in the publication of a joint statement of all the participants that outlined their future priorities for ransomware:

- **Network Resilience:** The participants committed to working together with the private sector to promote basic cyber hygiene and to bolster network resiliency to mitigate ransomware risk. The participants also aimed to promote cyber threat information sharing, including the broad disruption of steps to mitigate cyber risks.

- **Countering Illicit Finance:** The participants dedicated themselves to leverage national anti-money laundering frameworks to combat the ransomware business model, which is propelled by cryptocurrencies.
- **Disruption and other Law Enforcement Efforts:** The participants announced their intention to cooperate on enhancing information sharing and providing other relevant assistance across law enforcement authorities to degrade and hold accountable cybercriminal groups.
- **Diplomacy:** The participants also committed to continuing to leverage diplomacy to complement other law enforcement and cybersecurity activities to combat ransomware.

Notably, China and Russia were not involved in the Counter Ransomware Initiative talks. China remains the US's top cyber adversary and diplomatic relations currently remain frosty. On the other hand, the US government and Russia established a bilateral working group called the "US-Kremlin Experts Group" that aims to counter ransomware threats within Russia's borders. In this case, the White House prefers direct, bilateral discussions to enable frank dialogue to pressure the Kremlin to rein in Russian cybercriminal groups. However, the Biden administration does not have any illusions about trying to change Russian behavior.

Meanwhile, Congress is also considering new legislation to address ransomware threats. For example, the Senate floor is considering the *Cyber Incident Reporting Act of 2021*, which would, among other things, require organizations to notify the federal government within 24 hours if they make a ransomware payment.

Priority 3: Critical Infrastructure Cybersecurity

Critical infrastructure protection is another key cybersecurity priority for the Biden administration. It continues to advance new initiatives to promote security of industrial control systems (ICS) within critical infrastructure sectors.

Most notably, on July 28, 2021, Biden issued National Security Memorandum 5 (NSM-5), *Improving Cybersecurity for Critical Infrastructure Control Systems*. NSM-5 outlines two key cybersecurity programs for the 16 critical infrastructure sectors in the US.

First, NSM-5 established the ICS Cybersecurity Initiative, a voluntary, collaborative effort between the federal government and the critical infrastructure community to deploy technologies that enhance threat visibility, indicators, detections, and warnings against cyberattacks and cyber threats. This initiative originally began with the administration's 100-day plan to bolster the cybersecurity of the US electricity subsector running from April 20 through July 29. During this exercise, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response partnered with electric utilities to conduct a 100-day "sprint" to enhance the security and resiliency of electric ICS and associated OT and IT networks. This 100-day electricity subsector initiative was deemed successful. Since then, over 150 electricity utilities representing almost 90 million residential customers are either deploying, or have agreed to deploy, control system cybersecurity technologies through this initiative.

The ICS Cybersecurity Initiative is now expanding beyond the administration's work in the electricity subsector by focusing on the oil and natural gas pipeline subsector (in response to the Colonial Pipeline hack). Later in 2021, the initiative will turn to the water and wastewater sector and the chemical sector. The government hopes to eventually expand its ICS Cybersecurity Initiative across all 16 critical infrastructure sectors in time.

Second, NSM-5 tasked CISA and NIST to develop "Critical Infrastructure Cybersecurity Performance Goals" to help form an understanding of the baseline cybersecurity practices that critical infrastructure owners and operators can adopt.

On Sept. 22, CISA published its preliminary Critical Infrastructure Cybersecurity performance goals, pursuant to NSM-5. The preliminary list is intended to provide helpful guidance to critical infrastructure owners and operators. It includes nine top-level categories: Risk Management and Cybersecurity Governance; Architecture and Design; Configuration and Change Management; Physical Security; System and Data Integrity, Availability, and Confidentiality; Continuous Monitoring and Vulnerability Management; Training and Awareness; Incident Response and Recovery; and Supply Chain Risk Management. Moving forward, NSM-5 requires CISA and NIST to issue a finalized list by July 2022.

Overall, NSM-5 aims to forge closer voluntary government-industry ties to address cyber threats against critical infrastructure, and create a comprehensive, coordinated (albeit voluntary) approach toward securing the critical infrastructure sectors of the US. White House officials have noted that current policies and regulations for critical infrastructure security are promulgated on a sector-by-sector basis. As such, NSM-5's ICS Cybersecurity Initiative and the Critical Infrastructure Cybersecurity Performance Goals aim to promote a cross-sector approach for securing critical infrastructure sectors.

Notably, however, under current US laws, the administration cannot require critical infrastructure owners and operators to engage in these activities or share cyber threat information with the government. As such, these initiatives depend upon voluntary participation by industry. That said, Congress's proposed *Cyber Incident Reporting Act of 2021* would require critical infrastructure organizations to notify the federal government of a major cyber incident within 72 hours.

At the same time, the administration is also taking some small steps to regulate cybersecurity for certain critical infrastructure sectors. On May 27, the Transportation Security Administration (TSA) (within the DHS) issued a mandatory Security Directive for the oil and gas pipeline sector – the first-ever cybersecurity regulation for this sector in response to the Colonial Pipeline cyberattack. The key provisions of this new regulation include:

- Companies must designate a Cybersecurity Coordinator who will be the point-of-contact with the DHS and TSA officials in case of a future cyber-attack;
- Companies must alert the DHS about a cyber incident within 12 hours of discovery;
- All oil and gas pipeline owners and operators must immediately conduct a cyber vulnerability assessment.

In July, the TSA issued a second Security Directive requiring owners and operators of oil and natural gas pipelines to:

- Implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems within prescribed timeframes;
- Develop and implement a cybersecurity contingency and recovery plan;
- Conduct an annual cybersecurity architecture design review.

There will likely be additional cybersecurity regulations coming from the TSA – and possibly other government entities responsible for critical infrastructure security – in the months and years ahead.

Key Questions Moving Forward

In its first year, the Biden administration has identified some of the most pressing cybersecurity challenges facing the US – insecurity of federal systems, the growth in ransomware, and critical infrastructure cyber vulnerabilities. In response, it has taken a multi-faceted, whole-of-government approach to address these concerns.

Now that these top challenges have been identified and prioritized, NCD Inglis is working to ensure that all US government entities and relevant private sector organizations have the necessary resources and proper responsibilities to ensure national cyber resiliency in the face of these threats. However, there remain many significant impediments to this vision of a "cyber-resilient" nation. These include cybersecurity workforce shortages, limited funding available for cybersecurity budgets (especially within small companies), and the rapidly evolving nature of cyber threats, among many other things.

Moreover, US policymakers will continue to debate and discuss how to best balance federal agencies' mission to cooperate with industry on cybersecurity, but also engage in appropriate regulatory oversight for critical infrastructure sectors. For example, should CISA focus exclusively on fostering voluntary public-private partnerships with critical infrastructure sectors, as some claim? Or should CISA play more of a regulatory and oversight role with these sectors, as others argue? There are no easy or perfect policy solutions to address the relationship between the US government and the private sector in establishing a cyber-resilient nation. Indeed, the administration, Congress, and federal officials will likely continue to take various, incremental steps to build this relationship with the private sector to address the current and future cyber threat landscape.

Overall, whether the current administration's cybersecurity policies will succeed remains to be seen. Biden, like all 21st century US presidents, must quickly adapt his policy approaches to address the continuously evolving cyber threat landscape. He (and his successors) will continue to face a winding and bumpy road to manage cyber threats in this new digital age. JS

Robert Shields is a director at International Technology and Trade Associates, Inc. (ITTA), supporting clients on a wide range of issues involving US space, cybersecurity, and technology policies.