



April 2021

# U.S. Cyber Policy: The Emerging U.S. Cyber Agenda and the Critical Role of Financial Services

Martin Boer, Director, Regulatory Affairs ([mboer@iif.com](mailto:mboer@iif.com))

Melanie Idler, Senior Policy Associate, Regulatory Affairs ([midler@iif.com](mailto:midler@iif.com))

## INTRODUCTION

As the priorities of the Biden administration begin to take shape, a U.S. government cybersecurity agenda is emerging that includes overhauling U.S. cybersecurity strategy and leadership, bringing in veteran cybersecurity experts, pledging vast digital and cyber defense investments, and laying the groundwork for renewed cooperation with the private sector, and international allies. Together, these developments offer early insights into the administration's cybersecurity policy, with important implications for the financial sector. This also comes at a time when the U.S. government is, like many organizations around the world, recovering from and assessing the full impact of several high-profile cyber incidents including the 2020 SolarWinds and 2021 Microsoft Exchange Server data breaches.

The SolarWinds breach exploited software and credentials at key vendors, and ultimately impacted thousands of organizations globally and multiple parts of the U.S. government. After the breach came to light in December 2020, then-incoming President Biden promised 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."<sup>1</sup>

Since then, two other major global cyber incidents have come to light: one exploiting a vulnerability in Microsoft's widely used Exchange Servers, which compromised tens of thousands of organizations around the world that use the popular email software; and another that used Pulse Secure, a popular remote-working tool, to break into government agencies, defense companies, and financial institutions in the U.S. and Europe.

### Main Takeaways

The U.S. government, and new administration, are overhauling U.S. cybersecurity strategy and leadership, pledging investments, and introducing new regulations and policies to improve national cybersecurity capabilities.

Three recent high-profile data breaches have increased scrutiny and oversight of supply chains, third-party relationships, and overall cyber and operational resilience both in the U.S. and internationally.

The new administration has already issued an executive order on securing U.S. supply chains, enhancing software cybersecurity standards, and requiring breach notifications by software vendors. It has also imposed new sanctions against Russia, including expanding prohibitions on banks trading in Russian government debt.

More effective information sharing, and incident reporting are industry priorities that can bolster overall security across the financial ecosystem, alongside the wider usage of cyber risk insurance and addressing data localization barriers.

The U.S. government is urged to work closely with the private sector, key allies, and global standard-setting bodies, and help reduce cross-border fragmentation in policy, standards, and regulations.

<sup>1</sup> The Hill 2020. "[Biden vows to make cybersecurity 'imperative' following massive hack](#)" Dec. 17. 2020.

The quick succession and high-profile nature of these incidents have increased the level of scrutiny and oversight of supply chains, vendors, third-party relationships, and their cyber resiliency. Grappling with the aftermath of two of the biggest cybersecurity breaches in the U.S. is an urgent priority for the new administration and U.S. government. This heightened attention will likely have a material impact on the private sector, especially the financial sector given its status as a vital component of the nation's critical infrastructure and where, as in areas like mitigating cyber incidents, there is close alignment with the public sector.

To make the overall financial system more resilient against cyberattacks, more strategic approaches to both voluntary information-sharing, between firms and with the authorities, and effective cyber incident reporting should also be key priorities. Given the global nature of cyber incidents, the new administration is encouraged to work more closely with key allies and global standard-setting bodies to coordinate and improve the sharing of information, make procedures more consistent, and support cross-border partnerships, including between the public and private sector. This includes regulations around cybersecurity, information and communications technologies, and the burgeoning area of operational resilience. Fragmented approaches across jurisdictions can be counterproductive, slowing down the ability of governments and firms to share information effectively that could otherwise help organizations mitigate, respond, and recover from cyber incidents, breaches, and operational disruption, thereby boosting cyber resilience across the industry and overall financial stability. Any new rules to strengthen financial firms should consider the entire financial ecosystem and not be limited solely to regulated firms. (See Appendix I for key priorities for addressing cyber risk in the financial services sector.)

Indeed, the new Biden administration is acting swiftly to address the ongoing cyber challenges. With its first hires and nominees, including Anne Neuberger as a Deputy National Security Advisor for Cyber and Emerging Technology at the National Security Council (NSC), the Biden administration has signaled that cybersecurity will be a key focus of his administration. Other significant nominations include Chris Inglis and Jen Easterly as the newly created National Cyber Director (NCD) and Director of the Cybersecurity and Infrastructure Security Agency (CISA), respectively. (See Appendix II for key U.S. government nominations and appointments.)

## CYBER THREAT LANDSCAPE

COVID-19 has been a boon for cybercriminals taking advantage of the increase in digitization and work-from-home arrangements brought on by the pandemic. In 2020, at least 2,500 U.S. government entities, health care facilities, and schools fell prey to ransomware,<sup>2</sup> resulting in USD 4.2 billion in losses.<sup>3</sup> While the financial industry has long been the sector most exposed to cyberattacks, it is also often credited for being the best at mitigating the cost of attacks, which could be an outcome of more proactive policy, regulation, and investment in risk management and governance practices with respect to IT.<sup>4</sup> Yet the financial sector is experiencing the second-largest share of cyberattacks, behind only the healthcare sector.<sup>5</sup> An increase in the incidence of attacks, rising losses, and the recognition of the potential for serious disruption to the functioning of critical financial infrastructure and the broader economy, has concentrated attention on cybersecurity as a central risk management issue for financial institutions and system-wide financial stability. The recent high-profile cyber incidents have focused minds on increasing cooperation and information-sharing between the public and private sector.

While cyberattacks are not a new challenge to federal security agencies, the scale, scope, and sophistication of three recent breaches involving Russia and China, two of the U.S.'s most powerful cyberspace adversaries, have triggered widespread concern, driving the White House and congressional leaders to rethink how to safeguard

<sup>2</sup> Emsisoft 2021. "[The State of Ransomware in the US: Report and Statistics 2020](#)" Jan. 18, 2021.

<sup>3</sup> Cyberscoop 2021. "[More than \\$4 billion in cybercrime losses reported to FBI in 2020](#)" Mar. 17, 2021.

<sup>4</sup> BIS 2020. "[BIS Working Papers No 865: The drivers of cyber risk](#)" May 2020.

<sup>5</sup> BIS 2021. "[Covid-19 and cyber risk in the financial sector](#)" Jan. 14, 2021.

the U.S. against the growing risk of state-backed cyberthreats. In April, Federal Reserve chairman Jerome Powell named cyber security as the biggest risk to the U.S. economy, especially for financial institutions.<sup>6</sup>

The massive SolarWinds cyberattack, which came to light a month before President Biden took office, was attributed by his administration to a group of hackers backed by Russia's intelligence agency.<sup>7</sup> In what Biden characterized as "a grave risk to our national security,"<sup>8</sup> the hackers inserted a backdoor (dubbed Sunburst) into the company's Orion software, a widely used IT infrastructure monitoring and management platform. By targeting a popular third-party vendor, the hackers were able to penetrate several hundred prominent organizations, including many Fortune 500 companies, multiple U.S. federal agencies such as the Commerce, Homeland Security, State, and Treasury Departments, as well as nuclear facilities.<sup>9</sup> As federal investigators come to grips with the full impact of SolarWinds, they have described it as one of the most damaging cyberattacks to have ever occurred given the sensitivity and high-profile nature of the targets – which reportedly also included NATO, the UK Government, European Parliament, and Microsoft among others – as well as the duration of the attack, as the breach went undetected for as long as nine months.

Two more recent cyberattacks, this time attributed to Chinese state-sponsored hacking groups, pose many of the same challenges as the SolarWinds breach, though the targets and methodologies of the attacks differ significantly. In an attack that came to light in March, what began as a clandestine cyberespionage campaign that exploited flaws in Microsoft's widely used Exchange email software escalated into an all-out hacking spree that used an automated program to scan for vulnerable Exchange servers and infect them, compromising over 60,000 businesses, including hundreds of financial firms and the European Banking Authority.<sup>10</sup> In April it was revealed that flaws in Pulse Secure's virtual private network servers, which enable employees to remotely access their company networks, allowed hackers to breach dozens of U.S. government agencies, defense contractors, financial institutions, and other critical sectors and allegedly steal intellectual property and project data.<sup>11</sup>

## ADMINISTRATION RESPONSE

In response to the state-backed hacking campaigns, President Biden unveiled an "urgent initiative to improve [the U.S.'s] capability, readiness, and resilience in cyberspace."<sup>12</sup> The American Rescue Plan Act of 2021 included USD 650 million for CISA and USD 1 billion for the launch of a Technology Modernization Fund focused on updating cybersecurity and IT shared services.<sup>13</sup> While significant, the final bill was a far cry from the nearly USD 10 billion investment the Biden administration had initially sought.<sup>14</sup> The next big legislative priority for the administration is a USD 2.25 trillion infrastructure bill that could include cybersecurity-related investments dedicated to securing critical infrastructure, such as hospitals and electric grids.<sup>15</sup>

President Biden has vowed to take a more aggressive stance against foreign adversaries. The administration has already issued an executive order focused on securing U.S. supply chains, enhancing software cybersecurity standards, and requiring breach notifications by software vendors.<sup>16</sup> In its most recent executive order, the

<sup>6</sup> AFP 2021. "[Fed Chair Says Cyberattacks Main Risk To US Economy](#)" Apr. 11, 2021.

<sup>7</sup> White House Briefing Room 2021. "[FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government](#)" Apr. 15, 2021.

<sup>8</sup> The Hill 2020. "[Biden faults Trump administration on cybersecurity following massive hack](#)" Dec. 22, 2020.

<sup>9</sup> New York Times 2020. "[Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit](#)" Dec. 14, 2020.

<sup>10</sup> Bloomberg 2021. "[Microsoft Attack Blamed on China Morphs Into Global Crisis](#)" Mar. 7, 2021.

<sup>11</sup> Washington Post 2021. "[Chinese hackers compromise dozens of government agencies, defense contractors](#)" Apr. 21, 2021.


<sup>12</sup> The Hill 2021. "[Biden: US taking 'urgent' steps to improve cybersecurity](#)" Feb. 4, 2021.

<sup>13</sup> H.R. 1319, "[An Act to provide for reconciliation pursuant to title II of S. Con. Res. 5.](#)" Mar. 6, 2021.

<sup>14</sup> The Hill 2021. "[Senate includes nearly \\$2 billion in cyber, tech funds to COVID-19 bill](#)" Mar. 4, 2021.

<sup>15</sup> The Hill 2021. "[Lack of cyber funds in Biden infrastructure plan raises eyebrows](#)" Apr. 2, 2021.

<sup>16</sup> Reuters 2021. "[Software vendors would have to disclose breaches to U.S. government users under new order](#)" Mar. 25, 2021.



administration imposed new sanctions against Russia, including expanding prohibitions on U.S. banks trading in Russian government debt.<sup>17</sup>

To bolster cyber resilience going forward, the White House and U.S. agencies are expected to strengthen relations between the private and public sector and increase coordination to address the ongoing fallout from the breaches, including with international partners.

---

<sup>17</sup> Wall Street Journal 2021. [“U.S. Puts Fresh Sanctions on Russia Over Hacking, Election Interference”](#) Apr. 15, 2021.

## APPENDIX I: FINANCIAL SECTOR PRIORITIES

As the U.S. government moves to overhaul U.S. cybersecurity strategy and leadership, there will be significant opportunities to improve the cyber resilience of the financial sector. For industry, priorities should include clear and consistent approaches to supply chains and third parties, information sharing, cyber incident reporting, operational resilience, combatting financial crime, cyber insurance, data localization, technology fragmentation, and regulatory convergence.

### Securing Supply Chains and Third Parties

The SolarWinds and Microsoft data breaches underscore the risk of using third-party vendors. President Biden issued an executive order requiring a review of supply chain security risks across industries including information technology. The White House is also contemplating another executive order on developing cybersecurity ratings and standards for software used in critical areas. This also complements initiatives being undertaken at the global level. Policymakers are encouraged to promote transparent approaches to third parties and outsourcing, and to supply chains, that rely on firms' own risk management frameworks in the first instance and impose supervisory measures only if those frameworks are inadequate. A national cyber security certification and labeling authority could help in attesting the security and resilience of suppliers and vendors. Authorities could also encourage software development teams to adopt tamper-evident practices paired with transparency techniques that allow for third-party validation and discoverability. Using modern computing architectures that isolate potentially compromised software components could also help limit the effects of attacks.

### Strategic Information Sharing

More effective information-sharing on threats, attacks, and responses across the private and the public sectors would enhance the ability to deter and respond effectively to threats. Voluntary platforms such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Analysis and Resilience Center (ARC) already play an important role. Yet serious barriers remain, often stemming from national security concerns and data protection laws. Financial institutions are a critical infrastructure that can both help identify and address threats as they enter the financial ecosystem. More effective information sharing protocols and practices should be developed that work effectively within security and data protection constraints. Increased use of common information platforms, and expansion of trusted networks could help reduce barriers to information sharing. That includes exploring ways in which existing information sharing initiatives can provide legal protections from liability. The U.S. Treasury Department should promote broader use of industry initiatives such as the Financial Sector Profile, which would enable greater coordination and consistency in sharing threat-specific information.

### Effective Cyber Incident Reporting

Financial firms are uniquely positioned to play an important role in supporting and protecting overall cyber resilience by quickly reporting cyber incidents to relevant authorities. But these efforts are often less effective because rules vary dramatically, both domestically and internationally, about what constitutes a "cyber incident", what information must be shared, in what format, and by what timeframe. There is also very little feedback to firms from authorities about the information that is shared. The OCC, Federal Reserve, and FDIC released a joint proposal in January to help expand and expedite reporting requirements. This would give regulators a broader sectoral overview and could also provide industry with critical information. It would be a welcome development if cyber incident reporting could be approached more consistently globally. Firms would also benefit from a single regulatory reporting hub, where all relevant authorities can obtain pertinent information, which would be more efficient than multiple bilateral conversations.

## Sectoral Operational Resilience

Operational resilience is a relatively new approach to operational risk that focuses on the ability of firms and the financial system to deliver key services and continue to serve the needs of customers through disruptions, including cyberattacks and data breaches. U.S. Agencies released Sound Practices in October 2020 to provide firms with ways to strengthen their operational resilience in the face of internal and external risks, which if left unchecked could lead to wide-scale disruption. Given the outsized potential for cyber incidents to have disruptive operational and business impacts, we can expect operational resilience to be a greater priority for U.S. authorities. Actions for strengthening cyber resilience include proper risk-management and ensuring that controls and mitigation mechanisms are in place, as well as implementing best practices for responding, recovering, and learning from a cyber breach. It is important that any new rules apply to the entire financial ecosystem, and not only regulated firms. Promoting vendor diversity in the procurement process, would help ensure resilience, avoid redundancy, and promote continuity of operations.

## Combatting Financial Crime

As evidenced through the increasing use of ransomware, often demanding bitcoin and other virtual assets, many cyber incidents include financial, anti-money-laundering (AML) & countering financing of terrorism (CFT) components. U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) introduced in January bank-like regulation of virtual asset transactions, including an AML reporting requirement. While more emphasis can be expected by FinCEN and other authorities on combatting online financial crime, it is important to align the U.S. reform effort with the Financial Action Task Force (FATF) and other jurisdictional work on systemic effectiveness in AML/CFT. Industry would benefit from two-way communication to help mitigate financial crime, and any new measures should be technology-agnostic as opposed to focusing on current technologies.

## Promoting Usage of Cyber Risk Insurance

The use of cyber risk insurance is expected to grow given the high-profile nature of recent cyberattacks and the overall increase in ransomware attacks. There are many benefits to the broader adoption of cyber insurance, as recently identified by the New York Department of Financial Services, which has outlined industry best practices and interprets existing laws and requirements. Effective cyber incident reporting and information sharing would also enable broader insurance coverage. To help this market develop more broadly, policymakers, regulators, and supervisors are encouraged to continue their efforts to better understand cyber risk, the market for cyber risk insurance, and advances in insurers' risk management and governance through dialogue with providers of cyber risk cover and reinsurance, academics and experts in risk management and modeling, and other public sector authorities. They can also help promote the wider adoption of insurance and voluntary utilization of cyber risk prevention services as a complement to robust cyber risk management in reducing the likelihood and impact of cyber events.

## Addressing Data Localization Barriers

A growing number of jurisdictions have introduced or strengthened data localization requirements, citing law enforcement, national security, personal data protection, or economic protectionism. These requirements can have far-reaching implications for the financial system and the overall economy: they may increase IT and data complexity; undermine the risk management, cybersecurity, and AML practices of FIs; and reduce access to financial services and markets in some countries. To minimize the cross-border restrictions to the flow of data, international cooperation is essential, particularly to address the challenges related to privacy, security, regulatory supervision, and law enforcement. The U.S. has already been vocal in negotiating with its trade partners on clauses that restrict or minimize the introduction of data localization measures. The Biden administration may want to prioritize negotiating a new EU-U.S. Privacy Shield, which was invalidated by the courts in July 2020. More data flows between the U.S. and the EU than anywhere else in the world, underpinning

the global financial system, enabling cybersecurity cooperation, and allowing for cross-border, digital commerce.

### Technology Fragmentation

Another area of increasing divergence is technology, where companies often face local regulations and localization requirements for technologies (e.g., applications, software, cloud usage) that make it difficult to manage these technologies from an enterprise-wide perspective across borders and business lines, which is often more effective and efficient given the global nature of disruptions. Regulators could pursue alternative solutions to technology sovereignty concerns such as Memorandums of Understanding, co-operation agreements and the college of supervisors that allow operational risk to be managed holistically across borders. Outsourcing rules should allow for firms to make use of global technology, processes and governance that recognizing the greater control and different risk profile of intra-group outsourcing to external outsourcing.

### Achieving Regulatory Convergence

Cyberattacks and data breaches do not respect national borders and often impact multiple jurisdictions simultaneously. But the regulatory and supervisory landscape to mitigate the impact of such incidents has become increasingly fragmented. Inconsistent and conflicting cyber-related regulations differ across jurisdiction and add undue complexity for firms with operations in multiple jurisdictions. Moreover, regulatory fragmentation redirects scarce cyber-related resources and personnel away from security activities and toward reporting and compliance efforts. To continue building cyber resilience, the Biden administration is encouraged to help develop and promote a globally accepted cyber-related regulatory landscape that addresses the increase in regulatory and technology fragmentation. They should work with the Financial Stability Board and other standard-setting bodies internationally to support initiatives that improve and align regulatory oversight efforts for the cybersecurity and operational resilience of financial services. A more common and consistent approach in all these areas would help mitigate the full impact of future cyber breaches and attacks while strengthening the U.S. financial system and the broader economy.

## APPENDIX II: KEY U.S. CYBER SECURITY PERSONNEL

As the new Biden administration takes shape, key officials are being nominated and appointed, both in the White House and across agencies, who will help transform the U.S. cyber policy agenda. Although there are still some positions that need to be filled, the new group of officials come from a wide variety of backgrounds, bringing extensive experience from prior administrations, agencies, Congress, defense, and the private sector.

Three notable developments include the appointment of Anne Neuberger as Deputy National Security Advisor on Cyber and Emerging Technology, as well as the nominations of Jen Easterly as the Director of the Cybersecurity and Infrastructure Security Agency, and Chris Inglis as the first head of the Office of the National Cyber Director. In one of his first public appearances since being nominated, Inglis said one of his top priorities would be to establish a collaborative environment for the private sector and federal agencies to share cyber threats and intelligence. Given the old Washington adage that “people are policy” in presidential administrations, we can expect these key appointees to play pivotal roles in shaping the U.S. cybersecurity agenda.

### Key U.S. Administration Cybersecurity Appointees:

Appointee	Title	Background	Status
<b>The White House: U.S. National Security Council (NSC)</b>			
Anne Neuberger	Deputy National Security Advisor for Cyber and Emerging Technology	NSA, White House, Pentagon, Navy	Appointed
Daleep Singh	Deputy National Security Advisor	New York Fed, U.S. Treasury	Appointed
Tarun Chhabra	Senior Director for Technology and National Security	Brookings, Georgetown, White House, Pentagon	Appointed
Caitlin Durkovich	Senior Director of Resilience and Response	Toffler Associates, Atlantic Council, DHS	Appointed
Jeff Greene	Acting Senior Director for Cyber Defense	U.S. NIST, Symantec, Senate	Appointed
Andrew Scott	Director for International Cyber Policy	White House, State Department	Appointed
Michael Sulmeyer	Senior Cyber Director	U.S. Cyber Command, Defense	Appointed
Carole House	Cybersecurity Director	U.S. Treasury (FinCen), OMB, Senate	Appointed
<b>The White House: Office of the National Cyber Director (ONCD)</b>			
Chris Inglis	National Cyber Director	NSA	Nominated
<b>The White House: Office of Management and Budget (OMB)</b>			
Chris DeRusha	Federal Chief Information Security Officer (CISO)	State of Michigan, Ford, White House, DHS	Appointed
Clare Martorana	Federal Chief Information Officer	Office of Personnel Management, White House	Appointed
<b>U.S. Department of Commerce: Bureau of Industry and Security (BIS)</b>			
To be nominated	Under Secretary of Commerce for Industry and Security		N/A
<b>U.S. Department of Commerce: National Institute of Standards and Technology (NIST)</b>			
Natalia Martin	Director of National Cybersecurity Center of Excellence (NCCoE)	FDA, NIH	Acting
<b>U.S. Department of Defense: National Security Agency (NSA)</b>			
Rob Joyce	Cybersecurity Director	White House, DHS, NSA	Appointed
<b>U.S. Department of Homeland Security (DHS)</b>			
Tim Maurer	Senior Counselor for Cybersecurity	Carnegie Endowment for International Peace	Appointed
Robert Silvers	Under Secretary for Strategy, Policy, and Plans	Paul Hastings, DHS	Nominated
<b>U.S. Department of Homeland Security: Cybersecurity and Infrastructure Security Agency (CISA)</b>			
Jen Easterly	Director	Morgan Stanley, NSA	Nominated
Nitin Natarajan	Deputy Director	Avantus Federal, EPA, White House, HHS	Appointed
Eric Goldstein	Executive Assistant Director	Goldman Sachs, CSIS, O'Melveny & Myers, DHS	Appointed
<b>U.S. Department of Treasury</b>			
Michael Mosier	Acting Director, Financial Crimes Enforcement Network (FinCEN)	Chainalysis, OFAC, DOJ, White House	Acting
<b>U.S. Department of State</b>			
Michelle Markoff	Deputy Coordinator for Cyber Issues	State Department career official	Appointed