ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

MARCH 13, 2023

White House Releases National Cybersecurity Strategy

by *Kim Peretti*, *Amy Mushahwar*, and *Kristen Bartolotta*

On March 2, 2023, the White House released its National Cybersecurity Strategy, the first new strategy since 2018 and the third to date. This Strategy includes five pillars around which the Administration seeks to build and enhance collaboration. Those pillars are: (1) Defend Critical Infrastructure; (2) Disrupt and Dismantle Threat Actors; (3) Shape Market Forces to Drive Security and Resilience; (4) Invest in a Resilient Future; and (5) Forge International Partnerships to Pursue Shared Goals.

To realize the vision the Administration lays out in these pillars, the White House will make two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace. First, the Administration aims to rebalance the responsibility to defend cyberspace. The goal is to shift responsibility from end users who have limited resources and competing priorities to the owners and operators of the systems that hold data and make society function, as well as the technology providers that build and service these systems.

Second, the Administration intends to realign incentives to favor long-term investments in cyberspace. In the National Cybersecurity Strategy, the Administration asserts that we must defend the systems we have now, while also building toward a future digital ecosystem that is more inherently secure and resilient. The federal government will use all tools available to reshape these incentives with an eye toward systemic defensibility and resilience.

Pillar One: Defend Critical Infrastructure

The first pillar addresses a recurring theme not only for the Administration but also with lawmakers—the defense of critical infrastructure. Through five strategic objectives, the Administration aims to "operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem."

- **Strategic Objective 1.1:** Establish Cybersecurity Requirements to Support National Security and Public Safety
- **Strategic Objective 1.2:** Scale Public-Private Collaboration
- **Strategic Objective 1.3:** Integrate Federal Cybersecurity Centers
- **Strategic Objective 1.4:** Update Federal Incident Response Plans and Processes
- **Strategic Objective 1.5:** Modernize Federal Defenses

At the outset of the first pillar, the Administration notes that the lack of mandatory requirements for critical infrastructure cybersecurity has resulted in inadequate and inconsistent outcomes. And while the Administration admits that the voluntary approach has produced meaningful improvements, critical infrastructure must be secure enough to have the confidence of the American people. The Administration intends to establish cybersecurity regulations to secure critical infrastructure, harmonizing and streamlining new and existing regulation and enabling regulated entities to afford security by leveling the playing field so companies do not compete to underspend their peers on cybersecurity. In some sectors, this may include incentivizing investment in cybersecurity through the rate-making process, tax structures, or other mechanisms.

In establishing further cybersecurity regulation for critical infrastructure, the federal government "will use existing authorities to set necessary cybersecurity requirements in critical sectors." Where there are gaps in statutory authorities to implement minimum cybersecurity requirements or mitigate related market failures in all industry segments, the Administration will work with Congress to close them. However, the Administration does not intend to push states or independent regulators out of the field; indeed, where those bodies have authority to set cybersecurity requirements, the Administration encourages them to do so.

Importantly, the Administration notes that regulations in this area should leverage existing cybersecurity frameworks and guidance, such as the Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals and the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, as well as existing international standards, to minimize the burden of unique requirements. However, the Administration makes clear its intention to ensure there are no gaps in the ability of the government to regulate the cloud computing industry and cloud-based services.

To increase collaboration between the public and private sectors, the Administration states in Strategic Objective 1.2 its intention to implement a mechanism for real-time, actionable, and multidirectional sharing. Additionally, Objective 1.4 notes that CISA will lead a process to update the National Cyber Incident Response Plan (NCIRP) to better identify how private-sector partners may reach the federal government for support and what support is available. The Administration notes that the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will also enhance the federal government's awareness and ability to respond effectively. CIRCIA was passed as part of the Strengthening American Cybersecurity Act in 2022 and also provides for increased sharing between the public and private sectors, including requirements for

entities deemed "critical infrastructure" to report certain cyber-incidents and ransom payments. For more information on CIRCIA and the implications for critical infrastructure, see our previous advisory.

Notably, the Administration aims to reduce redundancies and, hopefully, limit the reporting streams from the private sector into the federal government. Federal Cybersecurity Centers exist to unite whole-of-government capabilities across homeland defense, law enforcement, intelligence, and diplomatic, economic, and military missions. The Administration will also expand the National Cyber Investigative Joint Task Force (NCIJTF) to coordinate takedowns and disruption of threat actors with greater speed, scale, and frequency.

Pillar Two: Disrupt and Dismantle Threat Actors

The Administration again outlines five objectives through which it aims to enable more sustained and effective disruption of adversaries. Businesses across sectors suffer significant losses at the hands of threat actors, and the Administration calls for greater collaboration by public and private partners to thwart and disrupt the efforts of threat actors.

- **Strategic Objective 2.1:** Integrate Federal Disruption Activities
- **Strategic Objective 2.2:** Enhance Public-Private Operational Collaboration to Disrupt Adversaries
- **Strategic Objective 2.3:** Increase the Speed and Scale of Intelligence Sharing and Victim Notification
- **Strategic Objective 2.4:** Prevent Abuse of U.S.-Based Infrastructure
- **Strategic Objective 2.5:** Counter Cybercrime, Defeat Ransomware

Federal law enforcement, including the FBI, has long discouraged the payment of ransoms to decrease the profitability of criminal cyber activity. Strategic Objective 2.1 reiterates that criminal cyber activity must be rendered unprofitable. While the Administration's focus in this objective is on enhancing federal defenses, it notes that coordination with civilian partners will be required. Because the private sector has broader and more detailed information on the threat landscape, the Administration encourages the private sector to organize efforts through nonprofit organizations that can serve as operational hubs with the federal government.

The Administration further emphasizes the need for timely sharing of intelligence between federal and non-federal partners in Objective 2.3. Notably, the federal government will increase the speed and scale of sharing cyber-threat intelligence with "cyber defenders" and will notify potential victims when there is information that they may be targeted or already compromised. And while many laws and regulations are already in place to provide for sharing of information related to data security incidents with the government, the Administration intends to create additional mechanisms through which the private sector may provide threat intelligence to the federal government.

In addition to the increased federal efforts, the Administration states that all service providers must make reasonable attempts to secure the use of their infrastructure against abuse or other criminal behavior. This includes the virtual currency industry, which the Administration notes is abused to launder ransom payments. The Administration will adopt and enforce a "risk-based approach to cybersecurity across Infrastructure-as-a-Service providers that addresses known methods and indicators of malicious activity." This will be done

in part through implementation of EO 13984, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," published on January 25, 2021 by former President Donald Trump. This EO directed the Secretary of Commerce to propose regulations that require U.S. infrastructure as a service (IaaS) providers to verify the identity of a foreign person who obtains an account or maintains an existing account.

Long-term, the United States will support the implementation of international anti-money laundering and countering the financing of terrorism standards to mitigate the use of cryptocurrencies for illicit activities. This is consistent with the Administration's efforts in EO 14067, "Ensuring Responsible Development of Digital Assets." The Administration again discourages the payment of ransoms and encourages reporting of ransomware incidents to federal law enforcement and other appropriate agencies.

Pillar Three: Shape Market Forces to Drive Security and Resilience

In this pillar, the Administration intends to shape market forces to appropriately assign responsibility for cybersecurity controls. Market forces alone have not done enough to drive broad adoption of best practices in cybersecurity, and data stewards must be held accountable for the protection of that data.

- **Strategic Objective 3.1:** Hold the Stewards of Our Data Accountable
- **Strategic Objective 3.2:** Drive the Development of Secure IoT Devices
- **Strategic Objective 3.3:** Shift Liability for Insecure Software Products and Services
- **Strategic Objective 3.4:** Use Federal Grants and Other Incentives to Build In Security
- **Strategic Objective 3.5:** Leverage Federal Procurement to Improve Accountability
- **Strategic Objective 3.6:** Explore a Federal Cyber Insurance Backstop

Throughout the third pillar, the Administration takes a strong stance on consumer privacy and securing personal data. When organizations that have data on individuals fail to act as responsible stewards for the data, they externalize costs onto everyday Americans. Accordingly, the Administration provides its support for legislative efforts that impose "robust, clear limits on the ability to collect, use, transfer, and maintain personal data" and provide even stronger protections for sensitive data, and calls for legislation that sets national requirements to secure personal data, consistent with standards developed by NIST. Relatedly, in Strategic Objective 3.3, the Administration reiterates its intention to shift liability from American citizens to the entities that release products and services without adequate security. The Administration states that companies that make software owe a duty of care to businesses, critical infrastructure, and consumers that use their products.

Additionally, in Objective 3.2, the Administration alleges that many IoT devices currently in circulation or being deployed do not have sufficient protections against cybersecurity threats. Businesses can expect the Administration to continue development of IoT labeling programs, as directed in Section 4 of EO 14028, "Improving the Nation's Cybersecurity."

Putting its money where its mouth is, the Administration notes in Objective 3.5 that it will continue to use contracting requirements for vendors that sell to the federal government as a tool for improving cybersecurity. Entities that have contracts with the government should pay close attention to any changes in security requirements—the Civil Cyber-Fraud Initiative (CCFI) uses DOJ authorities under the False Claims Act to pursue civil actions against government contractors that fail to meet cybersecurity obligations. For more information on the CCFI, please see our previous advisory. The Administration is further exploring the possibility of a federal insurance response that will serve as an aid package when there are catastrophic cyber events.

For a more detailed analysis of the implications of this pillar on the technology industry, please refer to the advisory from our IP colleagues, "New National Cybersecurity Strategy Seeks to Hold Technology Companies Accountable."

Pillar 4: Invest in a Resilient Future

In the fourth pillar, the Administration asserts that the federal government must leverage strategic public investments in innovation, R&D, and education to ensure that both public and private investments in cybersecurity outpace the challenges the country and entities currently face. The Administration's goal is to ensure that the United States continues to be a leader in technology and innovation.

- **Strategic Objective 4.1:** Secure the Technical Foundation of the Internet
- **Strategic Objective 4.2:** Reinvigorate Federal Research and Development for Cybersecurity
- **Strategic Objective 4.3:** Prepare for Our Post-Quantum Future
- **Strategic Objective 4.4:** Secure Our Clean Energy Future
- **Strategic Objective 4.5:** Support Development of a Digital Identity Ecosystem
- **Strategic Objective 4.6:** Develop a National Strategy to Strengthen Our Cyber Workforce

Beginning with Strategic Objective 4.1, the Administration outlines its intent to "clean up" the internet by mitigating "Border Gateway Protocol vulnerabilities, unencrypted Domain Name System requests, and the slow adoption of IPv6." Notably, IPv6 has existed for about 35 years, but its adoption has been delayed in part due to the effectiveness of network address translation (NAT), which is used by many network operators to address the number shortage in the current IP address system (IPv4) and is a technical workaround that allows multiple devices to use by time sequencing a single IP address.

The Administration goes on to express its intention to accelerate investment in the hardening of software, hardware, and services that are currently vulnerable to attack from quantum computing. A balance must be struck between encouraging advancement and ensuring current infrastructure can adequately safeguard information because quantum computing has the potential to break even the strongest encryption standards deployed today. The Administration also intends to promote cybersecurity in electric distribution and distributed energy resources, secure digital identity solutions, and an expanded cybersecurity workforce.

Pillar 5: Force International Partnerships to Pursue Shared Goals

In the final pillar, the Administration promises to continue engaging with countries to maintain an open, free, global, and secure internet. The United States will also continue to collaborate with other countries to make cyberspace more secure and to counter threats and build a shared, resilient digital ecosystem.

- **Strategic Objective 5.1:** Build Coalitions to Counter Threats to Our Digital Ecosystem
- **Strategic Objective 5.2:** Strengthen International Partner Capacity
- **Strategic Objective 5.3:** Expand U.S. Ability to Assist Allies and Partners
- **Strategic Objective 5.4:** Build Coalitions to Reinforce Global Norms of Responsible State Behavior
- **Strategic Objective 5.5:** Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services

Strategic Objective 5.5 contains the Administration's goals for securing the global supply chain, particularly as it relates to data, semiconductors, and telecommunications. It notes U.S. dependency on foreign suppliers to remain globally connected and to produce products and services critical to our digital ecosystem. Businesses should be on notice that the Administration is looking to mitigate risks in this area in part by rebalancing global supply chains. This should not come as a surprise in the wake of the CHIPS Act, signed by President Biden in 2022, which set aside more than $50 billion to expand U.S.-based semiconductor manufacturing and research in order to make the country less dependent on foreign resources.

Key Takeaways

- The Administration is interested in ensuring further information-sharing between the public and private sectors, particularly for entities classified as critical infrastructure. Importantly, the Administration does not express intent to create a liability shield for information shared with the government. However, the federal government aims to make this a two-way street with additional information flowing to businesses when appropriate to defend against cyber-threats.
- China and Russia were identified as the top threats to U.S. security, and the Administration has a clear intention to continue to reduce U.S. dependency on foreign products and services, including from these countries. This may have implications for the businesses that rely heavily on those products and resources.
- The Administration is intent on shifting liability for cyber-threats and cyber-crime from users to developers (the entities are perceived by the Administration as releasing products and services without adequate security). Businesses can expect not only additional regulation but also increased agency authority to oversee and enforce new regulations.

You can subscribe to future *Privacy, Cyber & Data Strategy* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team**:

Kimberly Kiefer Peretti
+1 202 239 3720
kimberly.peretti@alston.com

Daniel J. Felz
+1 404 881 7694
daniel.felz@alston.com

Katherine Doty Hanniford
+1 202 239 3725
kate.hanniford@alston.com

Amy Mushahwar
+1 202 239 3791
amy.mushahwar@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333