JENNER&BLOCK

Client Alert: Biden-Harris Administration Cybersecurity Strategy

Publications

March 9, 2023
By: Shoba Pillay, Aaron R. Cooper, David Bitkower

On March 1, 2023, the White House released a new National Cybersecurity Strategy (the Strategy) documenting the Biden-Harris administration's approach to improving cybersecurity across the digital ecosystem.[1] The Strategy signals important changes to come in the cybersecurity landscape for both the federal government and the private sector and creates new risks and opportunities. In particular, the Strategy breaks new ground in seeking to shift cybersecurity responsibilities from front-line users (including individuals, small businesses, and local governments) to larger and better-resourced organizations, such as software developers and device manufacturers.

The Strategy is not self-executing, however. Instead, it provides high-level principles that the Office of the National Cyber Director will have the responsibility of implementing, and also envisions efforts by regulators and Congress to accomplish its objectives.[2] As a result, federal contractors and software vendors, among others, will want to pay close attention to the steps that follow, whether they include establishment of new regulatory standards, updated enforcement priorities, federal spending and grants, or enactment of new legislation. For example, the federal government will ramp up efforts to invest in secure software, secure critical infrastructure, and modernize its IT systems, and continue its efforts to disrupt cybercrime using law enforcement tools and sanctions. In the private sector, tech industry stakeholders and companies in critical infrastructure sectors will want to engage with the federal government and regulators about how best to implement the Strategy, including the administration's renewed efforts to penalize entities that, in its view, fail to adequately protect data.

A. The Strategy

The Strategy outlines five "pillars" to developing a more secure digital ecosystem: (1) defense of critical infrastructure; (2) disruption of threat actors; (3) use of market forces to incentivize security and resilience; (4) federal investment; and (5) international partnerships. The Strategy's overarching goals are to "rebalance" the burdens of cybersecurity protection away from individuals and small businesses and toward larger organizations better positioned to carry that burden, and to "realign incentives" for better cybersecurity compliance with defensive practices and forward-looking

investments.[3] Throughout, the Strategy builds on existing administration initiatives[4] as well as themes from the prior administration's 2018 National Cyber Strategy (the 2018 strategy).[5]

1. Defend Critical Infrastructure

The Strategy signals that the federal government plans to create new mandatory cybersecurity requirements in critical infrastructure sectors.[6] The federal government has already done so in some sectors (*e.g.*, transportation), and continues to work with existing regulatory authorities to develop mandatory cybersecurity directives in others.[7] However, in situations where federal departments and agencies lack statutory authority to implement cybersecurity regulations, the White House will look to Congress to create authority to do so.[8] The creation of cybersecurity mandates will be a marked difference from the current landscape, which encourages businesses in critical infrastructure industries to voluntarily comply with cybersecurity best practices.[9]

Recognizing the burden that new requirements may place on the private sector, the Strategy encourages regulators to minimize duplicative regulations.[10] The administration also urges regulators to work directly with regulated entities to develop tailored requirements specific to each sector in order to create a "level playing field," recognizing that some sectors have a greater ability to absorb cybersecurity costs than others.[11] Where existing regulations overlap, the Cyber Incident Reporting Counsel will work to mitigate those issues to reduce the burden on critical infrastructure entities. Companies thus have an opportunity to identify limitations and burdens affecting their industry, and to engage in a dialogue with regulators to shape future actions.

2. Disrupt and Dismantle Threat Actors

The federal government intends to further coordinate its defenses—including diplomatic, military, and intelligence defenses—to pursue disruption of cyber-focused threat actors.[12] The Department of Justice already prioritizes investigation and prosecution of cybercrime, including ransomware, and the Strategy signals support to continue scaling up those efforts. The Strategy directs the Department of Defense (DoD) to develop a cybersecurity strategy to define how the DoD uses cyberspace operations to defend the nation against both state and non-state actors.[13]

While the federal government—with its unique authorities—will bear the weight of enforcement, the Strategy encourages collaboration with the private sector, acknowledging that the private sector has a distinct ability to collect information on threats.[14] In addition, the Strategy indicates that the federal government will lean on Sector Risk Management Agencies, the Cybersecurity and Infrastructure Security Agency (CISA), law enforcement agencies, and the Cyber Threat Intelligence Integration Center to develop operations to "increase the speed and scale of cyber threat intelligence sharing" both inside and outside of the government.[15]

The Strategy focuses in particular on combating ransomware by: 1) using foreign policy to isolate countries that are "safe havens" for threat actors; 2) using law enforcement tools to investigate and prosecute ransomware crimes; 3) improving the resilience of our critical infrastructure; and 4) addressing "the abuse of virtual currency" in ransomware attacks.[16] The White House strongly discourages companies from paying ransoms and encourages timely reporting of ransomware events to reduce the profitability of ransomware campaigns.[17]

3. Shape Market Forces to Drive Security and Resilience

In recognition that "market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience," the Strategy supports Congress's efforts to enact comprehensive legislation on the protection of personal data and even stronger protection for geolocation and health data specifically.[18] The Strategy asks Congress to formulate a national personal data security policy consistent with the National Institute of Standards and Technology (NIST) guidelines.

The Strategy also supports federal research and development of secure "Internet of Things" (IoT) devices, which are often a target of threat actors.[19] Under authority of Executive Order 14028, "Improving the Nation's Cybersecurity," the White House will expand its program of labeling those devices with security labels akin to nutritional labels.[20] IoT device-makers will want to track the federal government's work in this space.

Finally, the administration will encourage adoption of secure software development practices by working with Congress and the private sector to develop legislation that creates liability for software companies in data breach litigation, while establishing a "safe harbor" for software companies that follow best cybersecurity practices.[21] Software developers should look for opportunities to engage productively in this effort.

4. Invest in a Resilient Future

The Strategy signals that the federal government will invest further resources into securing the internet, researching cybersecurity advancements, and advancing strong encryption practices, in a variety of ways.[22] It will fund those efforts with public investments like the National Science Foundation's Regional Innovation Engines program, the Secure and Trustworthy Cyberspace program, and funding opportunities through other programs such as the CHIPS and Science Act.[23]

In particular, to defend against the threat to encryption presented by quantum computing, the Strategy commits to transitioning the US's "cryptographic systems" (like vulnerable public networks) into "interoperable quantum-resistant cryptography."[24] The federal government also plans to devote resources to developing a secure clean energy system—to ensure resilient energy sources; and a digital identity ecosystem—to promote security and reduce fraud.[25]

5. Forge International Partnerships to Pursue Shared Goals

Working with other nations, the Strategy asserts that the United States will leverage existing international partnerships like the Declaration for the Future of the Internet,[26] a political commitment to advance common goals regarding the internet signed by more than 60 countries, to develop strategies to combat shared threats, establish cybersecurity norms, and hold countries accountable for reckless behavior.[27]

B. Anticipated Effects

The strategy outlines lofty goals but—as is common—leaves most implementation decisions to executive agencies and Congress. As such, Kemba Walden, Acting National Cyber Director, and Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, previewed that implementation of the Strategy will be a multi-year process, [28] and it will likely take some time to see the effects of the Strategy reflected in the digital ecosystem. As the strategy is implemented, we anticipate a number of significant effects on the private sector.

- **Federal Investment:** Utilizing funds available through the Bipartisan Infrastructure Law, Inflation Reduction Act, and CHIPS and Sciences Act, the federal government will invest in secure critical infrastructure products. Companies that manufacture digital infrastructure, software, IoT devices, or other products that impact our digital ecosystem should be mindful of the federal government's interest in funding cybersecure products and services. The Strategy loosely envisions a federal cyber insurance system that could be leveraged in the event of a devastating cyber event. The White House will explore whether such a system is necessary with input from Congress, state regulators, and private sector industry stakeholders.

- **Mandatory Cybersecurity Requirements:** Primarily, companies in critical infrastructure sectors may become subject to mandatory cybersecurity requirements.[29] Once implemented, companies will face repercussions for failing to comply with these requirements which are not yet defined but will likely expand beyond incident reporting. However, the Strategy states that the Biden-Harris administration will also seek to reduce the burden of duplicative requirements.[30] One example of duplicative reporting burdens is the SEC proposed rule on cybersecurity incident reporting[31] and CISA's Cyber Incident Reporting and Critical Infrastructure Act of 2022—each with its own overlapping cybersecurity incident reporting requirements.[32] In theory at least, efforts to mitigate these overlapping requirements could reduce burdens on those companies.

- **New Vectors of Liability:** As a result of the Strategy, companies that develop software products and services may soon face liability for data breaches stemming from alleged failures to adequately secure products.[33] The White House will seek to coordinate with Congress and the

private sector to create legislation shifting that liability, noting that the legislation should prohibit companies from contracting out of liability, including through Terms of Service.[34]

- **False Claims Act Risk:** Companies that contract with the federal government should be mindful that, under the Civil Cyber Fraud Initiative, DOJ has pursued False Claims Act liability for "knowingly provid[ing] deficient cybersecurity products or services, knowingly misrepresent[ing] their cybersecurity practices or protocols, or knowingly violat[ing] obligations to monitor and report cyber incidents and breaches."[35] The Strategy underscores the administration's support for DOJ's approach, and as a result DOJ may be more aggressive with False Claims Act enforcement moving forward.

D. Conclusion

A robust federal cybersecurity strategy is a positive development for digital security. However, plans for implementation remain to be seen, and private sector entities should look for opportunities to help shape the resulting policies, regulations, and legislation. Jenner & Block's Data Privacy and Cybersecurity Practice stands ready to assist clients in assessing risk, monitoring and preparing for the Strategy's implementation, and engaging productively with decision makers.

Footnotes

[1] National Cybersecurity Strategy (March 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (Strategy).

[2] Strategy at 34.

[3] FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy (March 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[4] Executive Order 14028, Executive Order on Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ National Security Memorandum 5, Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021); https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/. M-22-09, Moving the U.S. Government Toward Zero-Trust Cybersecurity Principles (January 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf; National Security Memorandum 10, Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (May 4, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/; National Security Strategy, 34 (October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf, at 34.

[5] National Cyber Strategy (September 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (2018 Strategy).

[6] Strategy at 8.

[7] Strategy at 8.

[8] Strategy at 8.

[9] The Biden-Harris Administration's National Cybersecurity Strategy Event Transcript (March 2, 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230303_Biden_Harris_Cybersecurity.pdf?VersionId=0O9c61rbwZu4.9QxpMKUAiouGay_WTY3.

[10] Strategy at 9.

[11] Strategy at 9.

[12] Strategy at 14.

[13] Strategy at 15.

[14] Strategy at 15.

[15] Strategy at 16.

[16] Strategy at 17-18.

[17] Strategy at 18.

[18] Strategy at 19.

[20] Strategy at 20;

[21] Strategy at 20; The Biden-Harris Administration's National Cybersecurity Strategy Event Transcript (March 2, 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230303_Biden_Harris_Cybersecurity.pdf?VersionId=0O9c61rbwZu4.9QxpMKUAiouGay_WTY3.

[21] Strategy at 21.

[22] Strategy at 25.

[23] Strategy at 23.

[24] Strategy at 24.

[25] Strategy at 25-26.

[26] Department of State, Declaration for the Future of the Internet, https://www.state.gov/declaration-for-the-future-of-the-internet.

[27] Strategy at 29-33.

[28] The Biden-Harris Administration's National Cybersecurity Strategy Event Transcript (March 2, 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230303_Biden_Harris_Cybersecurity.pdf?VersionId=0O9c61rbwZu4.9QxpMKUAiouGay_WTY3.

[29] Strategy at 8.

[30] Strategy at 9.

[31] SEC Proposed Rule, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

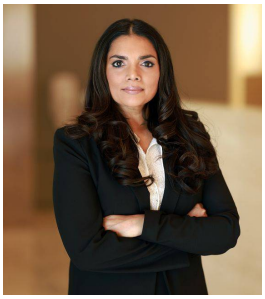
[32] H.R. 2471, 117th Cong. Div. Y (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[33] Strategy at 21.

[34] Strategy at 21.

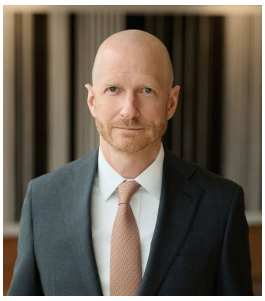
[35] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, at 22.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333



David Bitkower
Partner
dbitkower@jenner.com
+1 202 639 6048

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →