COVINGTON
Inside Privacy

Updates on developments in data privacy and cybersecurity

White House Releases National Cybersecurity Strategy

By Ashden Fein, Micaela McMurrough, Susan B. Cassidy, Dana Remus, Matthew Harden & Shayan Karbassi on March 6, 2023

The United States **National Cybersecurity Strategy**, released on March 2, 2023, is poised to place significant responsibility for cybersecurity on technology companies, federal contractors, and critical infrastructure owners and operators. The Strategy articulates a series of objectives and recommended executive and legislative actions that, if implemented, would increase the cybersecurity responsibilities and requirements of these types of entities. The overall goal of the Strategy is to create a "defensible, resilient digital ecosystem" where the costs of an attack are more than the cost of defending those systems and where "neither incidents nor errors cascade into catastrophic, systemic consequences." The Strategy outlines **two fundamental shifts** to how the federal government will attempt to allocate roles, responsibilities, and resources in cyberspace.

- First, the White House plans to work with Congress to shift the burden for mitigating cyber risks from end users (*e.g.*, individuals, small businesses, state and local governments, and infrastructure operators) to owners and operators of systems that hold data and technology providers that build and service these systems (*e.g.*, technology firms, software vendors, cloud service providers, and others). To this end, the Strategy proposes that legislation be developed to establish liability for software vendors that fail to take reasonable precautions to secure their software.

- Second, the federal government will focus on realigning incentives to favor long-term investments in renewing infrastructure, digitizing and decarbonizing U.S.

energy systems, securing semi-conductor supply chains, and modernizing cryptographic technologies.

The Strategy is built on the following five pillars, which are further discussed below:

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.

Pillar One: Defend Critical Infrastructure

The Strategy calls for building new capabilities that allow owners and operators of critical infrastructure, federal agencies, product vendors, service providers, and other stakeholders to effectively collaborate at speed and scale. In particular, the Strategy outlines the need to use minimum cybersecurity requirements, as opposed to voluntary measures, in critical sectors to enhance national security and public safety. In addition, the federal government plans to implement a zero-trust architecture strategy and modernize information technology ("IT") and operational technology ("OT") infrastructure with the goal of creating a model for critical infrastructure across the country.

Within the first pillar, the Strategy outlines five objectives:

- **Establish Cybersecurity Requirements to Support National Security and Public Safety** – The Strategy outlines the need to use minimum cybersecurity requirements in critical sectors to enhance national security and public safety, shifting from a voluntary approach to mandatory minimum requirements in key sectors. As examples, the Strategy cites the administration's progress in establishing cybersecurity requirements for oil and natural gas pipelines, aviation, and rail, led by the Transportation Security Agency ("TSA"), and waterways, led by the Environmental Protection Agency. The Strategy calls for using both existing statutes and regulations and working with Congress to enact new statutory authorities. In particular, the Administration plans to identify gaps in authorities to

drive better cybersecurity practices in the cloud computing industry and for other essential third-party services. Additionally, the Strategy directs the federal government to leverage existing standards, such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework and the Cybersecurity and Infrastructure Security Agency ("CISA") Cybersecurity Performance Goals, and to harmonize current cybersecurity regulatory requirements, including those addressing assessments and audits.

- **Scale Public-Private Collaboration** – The Strategy will attempt to combine organizational collaboration and technology-enabled connectivity to create a trust-based "network of networks" that builds awareness of threat activity and drives collective action among cyber defenders protecting critical infrastructure. It will do this by enabling the government to scale its coordination with critical infrastructure owners and operators. The Strategy aims to require the use of technology solutions to share information and coordinate defensive efforts, with a focus on enabling machine-to-machine data sharing and security orchestration to enable real-time, actionable, and multi-directional sharing to drive threat response.

- **Integrate Federal Cybersecurity Centers** – The Strategy calls on the federal government to coordinate the authorities and capabilities of the departments and agencies that are collectively responsible for supporting the defense of critical infrastructure.

- **Update Federal Cyber Incident Response Plans and Processes** – The Strategy calls on the federal government to provide clear guidance on how private sector partners can reach federal agencies for support during cyber incidents and the type of support available and to enhance its awareness of incidents through the **Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA")**.

- **Modernize Federal Defenses** – The Strategy calls on the Administration to drive long-term efforts to defend and modernize federal systems in accordance with zero-trust principles that acknowledge that threats must be countered both inside and outside traditional network boundaries.

Pillar Two: Disrupt and Dismantle Threat Actors

The second pillar outlines the government's strategy to use "all instruments of national power to disrupt and dismantle threat actors." This effort is driven by five objectives:

- **Integrate Federal Disruption Activities** – To increase the volume and speed of integrated disruption campaigns, the Strategy calls on the federal government to further develop technological and organizational platforms that enable continuous, coordinated operations.

- **Enhance Public-Private Operational Collaboration to Disrupt Adversaries** – The Strategy encourages private sector partners to organize their efforts through one or more nonprofit organizations that can serve as hubs for operational collaboration with the government, such as the National Cyber-Forensics and Training Alliance. Using virtual collaboration platforms, members of the cell would share information bi-directionally and work rapidly to disrupt adversaries.

- **Increase the Speed and Scale of Intelligence Sharing and Victim Notification** – The Strategy calls on the federal government to increase the speed and scale of cyber threat intelligence sharing to proactively warn cyber defenders and notify victims when the government has information that an organization is being actively targeted or may already be compromised.

- **Prevent Abuse of U.S.-based Infrastructure** – The Strategy calls on the federal government to work with cloud and other internet infrastructure providers to quickly identify malicious use of U.S.-based infrastructure, share reports of malicious use with the government, facilitate victim reporting of abuse of these systems, and impede efforts by malicious actors to gain access to these resources in the first place. The Strategy states that all service providers must make reasonable attempts to secure the use of their infrastructure against abuse or other criminal behavior. The Administration will prioritize adoption and enforcement of a risk-based approach to cybersecurity across Infrastructure-as-a-Service providers that addresses known methods and indicators of malicious activity, including through implementation of Executive Order 13984, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."

- **Counter Cybercrime, Defeat Ransomware** – Finally, the Strategy outlines the Administration's willingness to use national power to counter the ransomware threat along four lines of effort: (1) leveraging international cooperation to disrupt the ransomware ecosystem and isolate those countries that provide safe havens for criminals; (2) investigating ransomware crimes and using law enforcement and other authorities to disrupt ransomware infrastructure and actors; (3) bolstering critical infrastructure resilience to withstand ransomware attacks; and (4) addressing the abuse of virtual currency to launder ransom payments.

Pillar Three: Shape Market Forces to Drive Security and Resilience

The Strategy outlines the Administration's plans to shift cybersecurity risk to those best situated to address it in the following ways:

- **Hold Stewards of Data Accountable** – The Strategy calls on the federal government to support legislative efforts to impose robust, clear limits on the ability to collect, use, transfer, and maintain personal data and provide strong protections for sensitive data, like geolocation and health information. The Strategy specifies that this legislation should be consistent with standards and guidelines developed by NIST.

- **Drive the Development of Secure IoT Devices** – The Strategy aims to improve IoT cybersecurity through federal research and development (R&D), procurement, and risk management efforts, as directed in the IoT Cybersecurity Improvement Act of 2020. In addition, the Administration will continue to advance **the development of IoT security labeling programs**, as directed under Executive Order 14028, "Improving the Nation's Cybersecurity." The Strategy plans that through the expansion of IoT security labels, consumers will be able to compare the cybersecurity protections offered by different IoT products, thus creating a market incentive for greater security across the entire IoT ecosystem.

- **Shift Liability for Insecure Software Products and Services** – The Administration will work with Congress and the private sector to develop legislation establishing liability for insecure software products and services. The Strategy emphasizes the need for such legislation to "prevent manufacturers and software publishers with

market power from fully disclaiming liability by contract, and to establish higher standards of care for software in specific high-risk scenarios." The Strategy also recognizes the need for an "adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services." The Strategy states that this safe harbor will draw from current best practices for secure software development, such as the **NIST Secure Software Development Framework**. To further incentivize the adoption of secure software development practices, the plan encourages coordinated vulnerability disclosure across all technology types and sectors; promotes the further development of a Software Bill of Materials ("SBOMs"); and plans for the development of a process for identifying and mitigating the risk presented by unsupported software that is widely used or supports critical infrastructure.

- **Use Federal Grants and Other Incentives to Build in Security** – The federal government will collaborate with state and local entities, the private sector, and other partners to balance cybersecurity requirements for applicants with technical assistance and other forms of support.

- **Leverage Federal Procurement to Improve Accountability** – The Civil Cyber-Fraud Initiative ("CCFI") uses DOJ authorities under the False Claims Act to pursue civil actions against government grantees and contractors who fail to meet cybersecurity obligations. The Strategy states that CCFI "will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cyber incidents and breaches."

- **Explore a Federal Cyber Insurance Backstop** – The Strategy calls on the federal government to have a pre-planned response for potential catastrophic events. The Administration will assess the need for, and possible structures of, a federal insurance mechanism that would support the existing cyber-risk insurance market and form part of the federal government response to catastrophic cyber events.

Pillar Four: Invest in a Resilient Future

The Strategy emphasizes the need to marshal public and private investments in cybersecurity, aiming to "leverage strategic public investments in innovation, R&D, and education to drive" cybersecurity investment, including through multiple funding sources. As part of these investments, the Strategy aims to "ensure that resilience is not a discretionary element of new technical capabilities but a commercially viable element of the innovation and deployment process." To this end, the Strategy outlines six strategic objectives:

- **Secure the Technical Foundation of the Internet** – The Strategy states that the government must take steps to mitigate the most pervasive concerns of the internet's foundation, such as "Border Gateway Protocol vulnerabilities, unencrypted Domain Name System requests, and the slow adoption of IPv6." The Strategy similarly prioritizes preserving and extending the open, global internet by engaging in standards development processes, such as through non-governmental Standards Developing Organizations, to instill shared values and "ensure that technical standards produce technologies that are more secure and resilient."

- **Reinvigorate Federal Research and Development for Cybersecurity** – The Strategy directs the research, development, and demonstration ("RD&D") community "to proactively prevent and mitigate cybersecurity risks in existing and next generation technologies." Specifically, the Strategy notes that these RD&D investments will focus on securing: (1) computing-related technologies, (2) biotechnologies and biomanufacturing, and (3) clean energy technologies.

- **Prepare for our Post-Quantum Future** – The Strategy recognizes that quantum computing has the possibility of "break[ing] some of the most ubiquitous encryption standards employed today…." As a result, the Strategy prioritizes "the transition of vulnerable public networks and systems to quantum-resistant cryptography-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks." The Strategy also notes that "the private sector should follow the government's model" in preparing for post-quantum cryptography.

- **Secure our Clean Energy Future** – The Strategy aims to proactively build-in cybersecurity to new energy infrastructure "through implementation of the

Congressionally-directed National Cyber-Informed Engineering Strategy." The Strategy notes that the Department of Energy will "continue to promote cybersecurity for electric distribution and distributed energy resources in partnership with industry, States, Federal regulators, Congress, and other agencies."

- **Support Development of a Digital Identity Ecosystem** – The federal government will encourage and enable investments in "strong, verifiable digital identify solutions," including by "strengthening the security of digital credentials, providing attribute and credential validation services, conducting foundational research, updating standards, guidelines, and governance processes," and developing digital identify platforms.

- **Develop a National Strategy to Strengthen Our Cyber Workforce** – The Strategy prioritizes efforts at filling vacancies in cybersecurity positions nationwide, in both the public and private sectors.

Pillar Five: Forge International Partnerships to Pursue Shared Goals

The Strategy emphasizes that "[t]o counter common threats, preserve and reinforce global internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community."

In terms of forging international partnerships, the Strategy highlights five strategic objectives:

- **Build Coalitions to Counter Threats to Our Digital Ecosystem** – The Strategy stresses the need to build international partnerships to share cyber threat information, exchange model cybersecurity practices, compare sector-specific expertise, drive secure-by-design principles, and coordinate policy and incident response activities.

- **Strengthen International Partner Capacity** – The Strategy aims to strengthen the capacity of like-minded states by marshalling "expertise across agencies, the public and private sectors, and among advanced regional partners."

- **Expand U.S. Ability to Assist Allies and Partners** – The federal government aims to "establish policies for determining when it is in the national interest to provide" incident response support to allies and partners.

- **Build Coalitions to Reinforce Global Norms of Responsible State Behavior** – The Strategy states that the United States will work with allies and partners "to pair statements of condemnation with the imposition of meaningful consequences" for states that violate responsible state behavior through the use of all tools of statecraft, such as diplomacy, economics, law enforcement operations, legal sanctions, and others.

- **Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services** – The Strategy emphasizes the need to work with allies and partners "to identify and implement best practices in cross-border supply chain risk management and work to shift supply chains to flow through partner countries and trusted vendors." The Strategy acknowledges that this objective "will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more secure, resilient, and trustworthy."

Looking Ahead. The publication of the National Cybersecurity Strategy signals the beginning of the next phase of the Administration's efforts to implement its approach to enhanced cyber regulation. As set out in the Strategy, the Office of the National Cyber Director "will work with interagency partners to develop and publish an implementation plan to set out the federal lines of effort necessary to implement this Strategy." Given the broad reach of the Strategy, implementation may include the promulgation of new regulations, as well as new legislative proposals, codifying the Strategy's objectives.

Shift Towards Regulation. The National Cybersecurity Strategy signals a shift towards a more regulatory-focused cybersecurity approach. The Strategy aims to leverage new legislation and regulation to compel various businesses and industries to improve their own cybersecurity, as well as the collective security of the internet and the cyber supply chain. On the whole, the Strategy follows upon – and reaffirms – efforts by the administration and various federal agencies over the past few years to enact more robust cybersecurity requirements. For example, the Strategy cites to the Administration's

ongoing efforts to implement the provisions of its Executive Order on **Improving the Nation's Cybersecurity** and the efforts of federal regulators to enact more robust cybersecurity requirements, like the **enhanced cybersecurity requirements for the rail and air sectors** imposed by TSA.