wiley

ALERT

# National Cybersecurity Strategy Outlines A New Era of Cybersecurity Regulation

March 2, 2023

On March 2, 2023, the White House Office of the National Cyber Director (ONCD) released the National Cybersecurity Strategy ("Strategy"). The Strategy outlines the Administration's priorities for cyber regulations and policy. This Strategy replaces the last National Cyber Strategy, released in 2018, but ONCD says it builds on several of its priorities. It sets out an ambitious goal: "a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences."

This Strategy promises an array of federal activity, some of which is already underway, some of which will need to be kickstarted by agencies, and some of which will need congressional action. This Strategy is being released amidst an array of federal agency activity, including implementation of new legislation, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022 [1], and possible major changes to the Framework for Improving Critical Infrastructure Cybersecurity managed by the National Institute for Standards and Technology (NIST).

**Overview of the National Cybersecurity Strategy**

In the Strategy, the Administration moves away from long-standing policy promoting voluntary adoption of cybersecurity risk management, to promoting cybersecurity regulatory standards. Entities that hold "concentrated risk" are a priority for enhancing requirements and capabilities. The Strategy encourages federal and state regulators to step in where they perceive gaps.

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law


## Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology

The Strategy is organized along five pillars: (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; (5) Forge International Partnerships to Pursue Shared Goals. Each of the pillars has subordinate "strategic objectives" that describe goals or a desired end state.

*Pillar One: Defend Critical Infrastructure*

The Administration says that it aims to develop a more effective model of "collaborative defense" by "equitably distributing" risk and responsibility, and establishing "foundational" levels of security and resilience. This pillar has several calls for direct regulation, some of which the Administration recognizes need legislation.

- Strategic objective 1.1: Establish cybersecurity requirements to support national security and public safety.
    - The Administration will seek mandatory requirements for cybersecurity for critical infrastructure owners and operators, and cites existing and developing regulations for pipelines, rail, aviation, and water as models.
    - Mandatory cybersecurity requirements will be imposed via a combination of federal and state regulation, but will vary by sector. These will be informed by the CISA Cross-Sector Cybersecurity Performance Goals and the NIST Cybersecurity Framework.
    - The Administration also hopes to harmonize regulations and de-conflict incident reporting requirements.
    - The Strategy notes that some critical infrastructure sectors have limited resources to adopt enhanced cybersecurity capabilities, and encourages regulators to keep those limitations in mind. It offers no specific guidance or proposals, however, for enhancing those resources.
- Strategic objective 1.2: Scale public-private collaboration.
    - DHS CISA will have the coordinating role for critical infrastructure security and resilience.
    - Existing "sector risk management agencies" will continue to have the primary roles in coordinating with industry stakeholders.
    - CISA and the sector risk management agencies are encouraged to improve and better target collaboration with the private sector, and to move towards real-time, actionable, and multi-directional cyber threat information sharing.
- Strategic objective 1.3: Integrate Federal cybersecurity centers.
    - The federal government will seek to better coordinate among its several cybersecurity centers, with the goal of supporting rapid intelligence sharing with critical infrastructure described in objective 1.2.
- Strategic objective 1.4: Update Federal incident response plans and policies.
    - The federal government will provide clear guidance for how private sector partners can get help from the government during an incident.

    - The forthcoming incident reporting rules created by CIRCIA will support incident response activities.
    - The recently established Cyber Safety Review Board will ensure that lessons learned help improve national cybersecurity posture.
- Strategic objective 1.5: Modernize Federal defenses.
    - The federal government will continue its efforts to modernize its own networks and move towards a zero trust architecture, as outlined in Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
    - It will also coordinate investments to enhance cybersecurity on federal civilian and national security networks.

*Pillar Two: Disrupt and Dismantle Threat Actors*

This portion of the Strategy highlights ongoing efforts, including the FBI-led National Cyber Investigative Joint Task Force and the multinational Counter Ransomware Initiative. Some proposals contained in this pillar may need additional legal support and authorities to facilitate and protect shared information and activities.

- Strategic objective 2.1: Integrate Federal disruption activities.
    - DOJ and other federal law enforcement agencies will continue to integrate domestic legal authorities with private industry and international allies to disrupt online criminal activity while DoD will "defend forward" by disrupting malicious activity before it impacts intended targets.
- Strategic objective 2.2: Enhance public-private operational collaboration to disrupt adversaries.
    - The Strategy notes that the private sector has a more comprehensive view of cyber threats than the federal government, and highlights examples of successful collaboration such as the 2021 Emotet botnet takedown.
    - To continue this success, the Administration encourages private sector companies to collaborate and take part in designated public-private collaboration hubs. "Nimble, temporary cells" would share information and work rapidly to disrupt adversaries. The federal government will look to support this collaboration model by removing barriers such as security requirements or records management policies.
- Strategic objective 2.3: Increase the speed and scale of intelligence sharing and victim notification.
    - This objective seeks to address an issue many companies have raised with the federal government: the lack of timely and valuable intelligence sharing.
    - The Strategy notes some examples of successful collaboration such as NSA's engagement with the defense industrial base, and the Joint Cyber Defense Collaborative. The Administration will look to expand these types of sharing initiatives to other sectors and tasks the sector risk management agencies with developing intelligence priorities for their sectors.
- Strategic objective 2.4: Prevent abuse of U.S.-based infrastructure.

    - The Strategy notes that malicious cyber actors frequently exploit U.S.-based cloud infrastructure, domain registrars, hosting and email providers and other digital services to carry out criminal activity or malign influence operations. The federal government will continue an effort under the authorities of Executive Order 13984, *Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities* (January 25, 2021), which establishes record-keeping requirements for U.S. Infrastructure as a Service (IaaS) providers to limit malicious cyber actors' use of those services.
- Strategic objective 2.5: Counter cybercrime, defeat ransomware.
    - Noting the impact ransomware has had on U.S. critical infrastructure, the Strategy highlights the existing Counter-Ransomware Initiative and points to international cooperation, law enforcement investigations, and anti-money laundering activities targeting cryptocurrency. The Administration again "strongly discourages" victims from paying ransom but notes that some may choose to pay.

*Pillar Three: Shape Market Forces to Drive Security and Resilience*

This portion of the Strategy outlines a vision to "incentivize industry to prioritize core economic and national security interests and recast responsibility for cyber risk management to stakeholders who manage concentrated risk and those best positioned to reduce risk." This pillar identifies objectives that include new regulations and will require legislation to make major suggested changes. Implementation of this pillar will rely on several existing workstreams and will impact private companies in several ways.

- Strategic objective 3.1: Hold the stewards of our data accountable.
    - The Strategy calls for national privacy legislation that would set limits on collection, use, transfer, and storing personal data, with heightened protections for sensitive data such as geolocation and health information. The legislation would also include requirements for protecting personal information that align with NIST standards and guidelines.
- Strategic objective 3.2: Drive the development of secure IoT devices.
    - The Administration will move forward with the cybersecurity labeling scheme for Internet of Things (IoT) devices, and will leverage federal procurement, among other tools, to promote IoT security.
- Strategic objective 3.3: Shift liability for insecure products and services.
    - The Administration will seek legislation establishing liability for software products and services. Such legislation would prohibit full disclaimers of liability by contract, and establish "higher standards of care for software in specific high-risk scenarios." The contemplated legislation will offer a safe harbor for developers that meet secure software development practices, such as the NIST Secure Software Development Framework.
    - The Administration will promote coordinated vulnerability disclosure practices.
    - Programs developing and promoting a software bill of materials (SBOM) will also continue, and an effort will be devoted to identifying and mitigating risks in widely used "unsupported" software (such as the Log4j vulnerability).

- Strategic objective 3.4: Use Federal grants and other incentives to build in cybersecurity.
  - The Strategy notes that several programs created and funded under laws such as the Bipartisan Infrastructure Law and the CHIPS Act offer funding for investments that may include cybersecurity.
- Strategic objective 3.5: Leverage Federal procurement to improve accountability.
  - Federal procurement policies will continue to implement the new clauses and policies created under EO 14028. The Strategy encourages agencies to test cybersecurity requirements through procurement that can lead to "novel and scalable approaches."
  - The Strategy notes that DOJ's Civil Cyber-Fraud Initiative uses the False Claims Act to pursue contractors who fail to meet their cybersecurity obligations.
- Strategic objective 3.6: Explore a federal cyber insurance backstop.
  - The assessment would focus on "catastrophic incidents," suggesting that structuring an economic recovery and aid package in advance through insurance could be more effective and faster than a response after such an event.

*Pillar Four: Invest in a Resilient Future*

The Administration says that it plans to maintain the U.S. leading role as an innovator in next-generation technologies and infrastructure. The Strategy here calls for several new regulatory mandates, but also calls for substantial government spending in R&D in new and future technology. This investment focuses on computing, biotech, and clean energy, among other areas, demonstrating a sense of the Administration's priorities.

- Strategic objective 4.1: Secure the technical foundation of the internet.
  - The Strategy calls for addressing "pervasive concerns" such as Border Gateway Protocol vulnerabilities, unencrypted Domain Name System requests and slow adoption of IPv6. These issues will be addressed through "close collaboration" between the government and private sector.
  - The federal government will ensure that its own networks implement these security measures.
  - The U.S. will support Standards Development Organizations to ensure that the internet remains open, free, global, interoperable, reliable, and secure.
- Strategic objective 4.2: Reinvigorate federal research and development for cybersecurity. This effort will focus on three priority "families" of technologies:
  - Computing, including microelectronics, quantum systems, and artificial intelligence;
  - Biotechnologies and manufacturing; and
  - Clean energy.
- Strategic objective 4.3: Prepare for our post-quantum future.
  - Highlighting federal efforts, the Strategy encourages the private sector to prepare to implement quantum-resistant cryptography.

- Strategic objective 4.4: Secure our clean energy future.
    - The Administration will look to add cybersecurity requirements proactively into new technologies, such as electric vehicle chargers, zero-emissions fueling infrastructure, zero-emissions transit and school buses, and distributed energy resources.
- Strategic objective 4.5: Support development of a digital identity ecosystem.
    - Noting that the lack of secure digital identifies leads to fraud and can slow citizen access to government resources and funding, including in disaster response, the Administration plans to build on NIST's ongoing work to develop secure digital credentials, attribute and credential validation services, and updating standards, among others.
    - The Strategy encourages states rolling out mobile drivers' licenses to incorporate privacy and security.
- Strategic objective 4.6: Develop a national Strategy to strengthen our cyber workforce.
    - The Administration will seek to expand the number of cybersecurity workers, increase the diversity of the workforce, and expand access to training and career pathways.

*Pillar Five: Forge International Partnerships to Pursue Shared Goals*

The Strategy emphasizes that cybersecurity will be pursued on the international front by working with allies and international forums to develop cohesive cybersecurity efforts for cybercrime and global supply chains. This pillar revisits important coalition work around the world and restates the vital role that standards play. It also draws on lessons learned from recent geopolitical trends.

- Strategic objective 5.1: Build coalitions to counter threats to our digital ecosystem.
    - Noting multiple ongoing international partnerships and engagements, the Strategy calls for advancing these efforts with like-minded countries on issues such as threat information sharing, secure-by-design principles, and incorporating private sector and civil society groups.
- Strategic objective 5.2: Strengthen international partner capacity.
    - The Departments of Justice and Defense will continue to build and expand their respective law enforcement and military partnerships, respectively, while the State Department will prioritize aid to build cybersecurity capacity across the globe.
- Strategic objective 5.3: Expand U.S. ability to assist allies and partners.
    - The Administration continues a commitment to support allies and partners when victims of a significant cyberattack, and highlights a NATO initiative on virtual cybersecurity incident response support.
- Strategic objective 5:4: Build coalitions to reinforce global norms of responsible state behavior.
    - The Strategy calls for the U.S. to continue work to reshape and secure the global supply chain for ICT products and services.

- The Administration will promote the global deployment of 5G, and support Open RAN through the NTIA Public Wireless Supply Chain Innovation Fund.
- The U.S. will work with partners and allies to identify and implement best practices in cross-border supply chain management.

[1] P.L. No: 117-103 (March 15, 2022).

***

Wiley's Privacy, Cyber & Data Governance Team has helped companies of all sizes from various sectors proactively address risks and address compliance with new cybersecurity laws and requirements. Our team has been actively involved in almost every proceeding that is referenced in the Strategy, and is advising clients on the likely results of new legislation, revisions to core NIST documents, and agency regulatory and oversight activities. Please reach out to any of the authors with questions.