WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

The U.S. National Cybersecurity Strategy: Key Takeaways

March 14, 2023

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Nicholas Chanin | Amelia Putnam

On March 2, 2023, the White House released its long-awaited National Cybersecurity Strategy ("the Strategy"), designed to recalibrate and focus the government's approach to securing national cyberspace.[1] Drafted by the Office of the National Cyber Director ("ONCD"), the Strategy is intended to direct the cybersecurity efforts of the Executive Branch and its agencies, and to guide future legislative and policymaking activities. The Strategy identifies a number of specific cybersecurity goals for both public- and private-sector entities, all designed to improve the United States' cybersecurity and strengthen the nation's response to evolving cybersecurity threats. For example, the Strategy proposes the establishment of cybersecurity regulations for critical infrastructure, but seeks to limit the potential burdens of such regulations by basing them on existing standards. In addition, the Strategy includes proposals to shift responsibility from end users of software and devices to the organizations that develop such software and devices. It also reiterates the Biden Administration's position that ransomware is "a threat to national security, public safety, and economic prosperity," and that businesses should not pay ransoms in an effort to "reduce the potential for profit" of ransomware schemes.[2]

The Strategy combines novel proposals with existing cybersecurity policies to set forth an approach that may significantly change the cybersecurity landscape. While some of these proposals may ultimately result in greater regulatory burdens, the Strategy itself does not make new law; many of its proposals would need to be either enacted by Congress or adopted

[1] *National Cybersecurity Strategy*, THE WHITE HOUSE (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[2] *Id.* at 17–18.

by the relevant regulators. But it does provide insight into how the Biden Administration views – and intends to approach – some of the key challenges and opportunities presented by these issues.

What's New? Novel Proposals Highlight New Thinking

The main takeaway from the Strategy is that the Administration is prepared to consider novel solutions that could disrupt the status quo in the cybersecurity and ancillary markets, including the market for software solutions. Where prior administrations primarily sought to arm private companies with information, this Administration sees significant benefits in active government participation through a variety of mechanisms.

- **Shifting Burdens, Shifting Liability:** Perhaps the most novel proposal in the Strategy is the proposed shift of responsibility (and liability) for cybersecurity from end users to software producers and providers. Currently, this is handled as a matter of contract law; individual entities and businesses, no matter how small, negotiate with the companies that provide the software, and the result is that many of these customers bear their own cybersecurity costs and risks. The Strategy urges a new approach: "Companies that make software must . . . be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers. Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes."[3] It is unclear how the Administration intends to effect such a change, but a shift in cyber responsibility and liability would fundamentally alter the software development industry.

- **Harmonized Regulations and Standards, More Efficient Communication:** Another potentially significant change from prior policy is the proposal to shift from a sector-by-sector cybersecurity approach to harmonized cybersecurity standards and more efficient communications across agencies and industries. In particular, "where Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms."[4] The Strategy acknowledges that such harmonization also may need to occur across international borders.[5] The Strategy directs the Cybersecurity and Infrastructure Security Agency ("CISA") to update the National Cyber Incident Response Plan so that any private-sector request for assistance from the federal government is disseminated to the appropriate agencies; as the Strategy says, the goal is to ensure "a call to one is a call to all."[6]

- **Proactive Approach to Combatting Cybercrime:** A significant portion of the Strategy is devoted to discussing a new, more aggressive approach to combatting threat actors.[7] Specifically, the Strategy describes that the federal government will "disrupt online criminal infrastructure and resources, from taking down notorious botnets to seizing

[3] *Id.* at 21.

[4] *Id.* at 9.

[5] *Id.*

[6] *Id.* at 12.

[7] *Id.* at 14.

cryptocurrency gleaned from ransomware and fraud campaigns"[8] and will also disseminate intelligence it gleans from these disruption campaigns and "notify victims when the government has information that an organization is being actively targeted or may already be compromised."[9] While this approach leans heavily on public-sector entities, particularly law enforcement and the intelligence community, the private sector also has a role, and stands to benefit from this shift. For victims of cybercrime, in particular, this new approach may enable much faster and less expensive remediation.

What's Not New? Continuity on Some Key Issues

Although it is framed as a new approach to the federal government's cyber strategy, the Strategy incorporates certain legacy ideas and approaches, including by "carr[ying] forward the foundational direction of Executive Order (EO) 14028 . . . National Security Memorandum (NSM) 5. . . NSM 8, and other executive actions."[10] For that reason, much of the Strategy represents incremental change rather than a revolutionary departure from prior approaches.

- **Maintains Sector-Specific Information Sharing:** As noted above, the Strategy directs federal agencies to harmonize regulations and cybersecurity standards, particularly for critical infrastructure. However, the Strategy retains existing information-sharing practices through Sectoral Risk Management Agencies ("SRMAs") that interface between CISA and the various critical infrastructure sectors.[11] While calling on all participants to improve and accelerate collaboration, the Strategy concludes that "this model will enable real-time, actionable, and multi-directional sharing to drive threat response at machine speed."[12]

- **Critical Infrastructure Cybersecurity Through Regulation:** The Strategy leans heavily on the idea that regulatory mandates can improve cybersecurity outcomes. Critical infrastructure businesses, particularly in the energy pipeline and transportation industries, should be familiar with the Biden Administration's conclusion that "the lack of mandatory requirements has resulted in inadequate . . . outcomes."[13] The stated goal of harmonizing regulations with existing standards and guidance is helpful – the Strategy makes clear its goal is regulations that are "operationally and commercially viable" – but it is just as clear that prescriptive regulations will continue to be a key feature of cybersecurity for critical infrastructure businesses.

[8] *Id.*
[9] *Id.* at 15.
[10] *Id.* at 6.
[11] *Id.* at 10.
[12] *Id.*
[13] *Id.* at 8.

Next Steps

The ONCD will work with the Office of Management and Budget to coordinate implementation of the Strategy. The agencies will annually report to the President, the Assistant to the President for National Security Affairs, and Congress about the effectiveness of the Strategy and any follow-on actions necessary to achieve cybersecurity goals. The ONCD also encourages other federal agencies, such as CISA, to increase their investment in cybersecurity, which could lead to additional regulations or rule-making proceedings led by other agencies.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel Alvarez	**Laura Jehl**	**Nicholas Chanin**	**Amelia Putnam**
202 303 1125	202 303 1056	202 303 1164	202 303 1089
dalvarez@willkie.com	ljehl@willkie.com	nchanin@willkie.com	aputnam@willkie.com

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in Brussels, Chicago, Frankfurt, Houston, London, Los Angeles, Milan, New York, Palo Alto, Paris, Rome, San Francisco and Washington. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.