MARCH 13, 2023

Biden Administration Announces Updated National Cybersecurity Strategy

On March 2, 2023, the Biden Administration released an updated National Cybersecurity Strategy "to secure the full benefits of a safe and secure digital ecosystem for all Americans." The Strategy calls for stronger regulation of cybersecurity, more counter-hacking activity by law enforcement, and greater accountability for software manufacturers, in order to "realign incentives" to protect national security, public safety and economic prosperity.[1] Improved private-public collaboration is at the core of the Administration's vision for protecting critical infrastructure, although the Strategy aims to achieve that collaboration in part through increased regulation and by new legislation allowing software providers to be held liable for releasing products that are not secure by design. In an era of Congressional gridlock, aspects of the Administration's strategy that can be implemented by executive action alone are likely to draw the greatest focus. The updated strategy continues to carry out the Administration's goal of improving cybersecurity—including through actions of executive agencies—and takes the novel approach of shifting some of the liability for cybersecurity harms away from the users and consumers of technology products to the builders and sellers of these systems.

Key Takeaways

- The Strategy, if implemented, would create additional requirements and risks related to cybersecurity for manufacturers of technology products and software publishers. The Administration proposes to work with Congress and the private sector to develop legislation that prevents such companies "from fully disclaiming liability by contract, and to establish higher standards of care for software in specific high-risk scenarios," including by adopting safe harbor frameworks for companies that use secure methods. Additionally, the Strategy clarifies the Administration's support of emerging secure software development techniques and frameworks, as well as the mechanisms for identifying and mitigating risks software and supporting critical infrastructure.

[1] The White House, "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy," (Mar. 2, 2003), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

- More generally, the Strategy increases the likelihood of additional cybersecurity regulations beyond the critical sectors of the U.S. economy addressed by recent measures taken by the Biden Administration. The Administration makes clear in the updated strategy that it expects regulators beyond critical infrastructure sectors to exercise their authority, including by promulgating new rules and regulations, to improve cybersecurity of new information technology products and the data security protections in emerging innovations.

- The Strategy proposes to take additional steps to discourage the payment of ransomware, including by leveraging multinational efforts to disrupt ransomware gangs and pressure countries harboring bad actors, improving cyber defenses of targets and tightening limits on the use of virtual currencies that enable ransomware attacks, and developing new law enforcement tools to investigate and hold perpetrators of ransomware attacks accountable. Companies will need to take heed of these changes as they develop and adapt their incident response and ransomware policies and procedures, as well as when responding to potential ransomware attacks.

Summary of the Updated Strategy

The updated strategy is centered around two "fundamental shifts" in the federal government's approach to cybersecurity.[2]

- First, the Strategy seeks to "Rebalance Responsibility for the Defense of Cyberspace," acknowledging that the greatest responsibility for protecting critical infrastructure currently falls on users who may be ill-equipped to handle it. As the Strategy explains, a "single person's momentary lapse in judgment, use of an outdated password, or errant click on a suspicious link should not have national security consequences."[3]

- Second, the Strategy outlines the Administration's prioritization of realigning incentives for the private sector to invest in cybersecurity. The Strategy aims to foster private-public collaboration to achieve cybersecurity gains, to build a robust and diverse cyber workforce, and to embrace security and resilience by design, by focusing where new regulations will produce the greatest improvements in infrastructure resilience.[4]

In support of these two shifts, the Strategy is built on five pillars: defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces to drive security and resilience, investing in a resilient future and forging international partnerships to pursue shared goals.

- **Defending Critical Infrastructure.** The Strategy observes that "[n]ext-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and exposing some of our most essential systems to disruption."[5] To address these risks, the updated strategy outlines a multi-pronged approach to deploy existing federal power to protect the nation's 16 critical infrastructure sectors,[6] to scale up private-public collaboration (including by requiring mandatory notification to the government of covered incidents), and to support legislation for further mechanisms of accountability in these sectors. The Strategy acknowledges the costs of new cybersecurity regulations and seeks to implement "operationally and commercially viable" regulations to avoid crises and mitigate growing cybersecurity risks to critical infrastructure.[7] Agencies will be

---

2 National Cybersecurity Strategy, page 4.

3 National Cybersecurity Strategy, page 4.

4 National Cybersecurity Strategy, page 5.

5 National Cybersecurity Strategy, page 2.

6 See Cybersecurity & Infrastructure Security Agency, *Critical Infrastructure Sectors*, available at https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (accessed Mar. 9, 2023);

7 National Cybersecurity Strategy, page 8.

expected to exercise their existing authority in areas relevant to cybersecurity, and the Administration anticipates working with Congress to close any gaps in the government's regulatory authority.[8]

- **Disrupting and Dismantling Threat Actors.** The power of the Federal Government will be deployed to make cybercrime unprofitable and unsustainable, continuing the Administration's "all tools" approach to national security and cybersecurity threats.[9] In some respects, the updated strategy may signal a more assertive posture by clarifying that the U.S. will "use all instruments off national power to disrupt and dismantle threat actors whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities."[10] The Strategy also expands the concept of threat disruption to include the sharing of threat intelligence from the Federal Government to potential victims.[11] Under the updated strategy, all service providers must make reasonable efforts to secure their infrastructure against abuse.[12] Payment of ransoms to resolve cyberattacks is discouraged.[13]

- **Shaping Market Forces to Drive Security and Resilience.** The Strategy aims to eliminate any competitive advantage for organizations to underspend on cybersecurity. Because there is no overall federal requirement for organizations to take specific measures to secure their IT systems of data they store, some organizations create risk by failing to implement safeguards commensurate to the risks they face. The Strategy seeks to address these types of issues by, for example, calling for legislation for federal data privacy protection and for shifting liability onto software providers who fail to take reasonable precautions to secure their software. The Strategy also raises the possibility that the Federal government could put in place a federal cyber insurance backstop.

- **Investing in a Resilient Future.** The Strategy calls for federal and private investment in a number of efforts to improve data security in the private sector including, for example: encryption that is secure against quantum computing, securing the nation's clean energy infrastructure and digital personal identification.[14] For the Administration, infrastructure resiliency requires not just improved systems and technologies, but also an expanded and diverse cyber work force, which the Strategy aims to achieve through private-public partnerships, scholarships and training.

- **Forging International Partnerships to Pursue Shared Goals.** The Administration proposes to build coalitions with international partners to encourage responsible behavior online and to secure the global supply chain. Disrupting the operations of malicious actors based in foreign countries will require building our capacity to support our global partners when they find themselves under attack.[15]

We will continue to provide updates on developments in cyber policy.

* * *

8 National Cybersecurity Strategy, page 8.

9 Paul, Weiss Client Alert: *Deputy Attorney General Announces Creation of Disruptive Technology Strike Force*, (March. 3, 2023), available at https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/deputy-attorney-general-announces-creation-of-disruptive-technology-strike-force?id=46190.

10 National Cybersecurity Strategy, page 18.

11 National Cybersecurity Strategy, page 16.

12 National Cybersecurity Strategy, page 17.

13 National Cybersecurity Strategy, page 20.

14 National Cybersecurity Strategy, pages 25-27.

15 National Cybersecurity Strategy, pages 29-33.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associates Jordan Orosz and Cole Rabinowitz contributed to this Client Memorandum.