Skadden

Cybersecurity and Data Privacy Update

March 13, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

320 S. Canal St.
Chicago, IL 60606
312.407.0700

Trump Administration Releases Cyber Strategy

Executive Summary

- **What's new:** The Trump administration released its national cyber policy blueprint, signaling a shift toward a more proactive, offense-oriented approach in cyberspace and increased private sector engagement.
- **Why it matters:** The U.S. cyber strategy's vision for incentivizing private entities to identify and disrupt adversary networks will likely require legal and regulatory changes, impacting companies operating in cybersecurity and critical infrastructure sectors.
- **What to do next:** Companies should consider closely monitoring developments to track how the administration plans to enact incentives and follow-on changes to cybersecurity compliance frameworks, legal rules and procurement processes.

On March 6, 2026, the Trump administration unveiled its national cyber policy blueprint, "President Trump's Cyber Strategy for America" (the U.S. Cyber Strategy). The U.S. Cyber Strategy functions as a high-level statement of intent rather than a detailed policy framework, but it offers meaningful signals about the future direction of the administration's actions regarding cybersecurity. Broadly, the U.S. Cyber Strategy suggests a shift toward a more proactive, offense-oriented approach in cyberspace, complemented by reducing the burdens imposed by cybersecurity compliance frameworks and increasing public-private coordination to protect American networks and technology.

The U.S. Cyber Strategy is structured around six "Pillars of Action" that identify high-level objectives to guide its implementation. Below we describe in detail the priorities and significance of the U.S. Cyber Strategy, and the impacts we expect it will have on companies in this space.

Background and Strategic Context

The U.S. Cyber Strategy is animated by the Trump administration's "America First" framework and seeks to position the U.S. as the preeminent power in cyberspace. The White House argues that cyber criminals and adversaries pose a cross-cutting threat to the country's citizens and businesses, and its global competitiveness. In response, the administration frames its approach as mobilizing all available tools of national power, including those outside the traditional cybersecurity domain, to actively counter adversaries, harden defenses and promote American innovation.

Trump Administration Releases Cyber Strategy

The Six Policy Pillars

Pillar I: Shape Adversary Behavior. The U.S. Cyber Strategy outlines that the U.S. will "deploy the full suite of U.S. government defensive and offensive cyber operations." The centrality of offensive operations in shaping adversary behavior is consistent with the "Defend Forward" concept presented in the Department of Defense Cyber Strategy from the first Trump administration. The goal of this offense-focused approach is to defeat and deter cyber adversaries before they breach American networks, not merely to respond to incidents after they occur.

Notably, the U.S. Cyber Strategy envisions a role for the private sector in offensive operations. The Trump administration says that it wants to create incentives for companies to "identify and disrupt adversary networks and scale our national capabilities." This ambiguous language leaves an open question of what role the Trump administration expects the private sector to fulfill. For example, despite advocating for greater private sector engagement, the U.S. Cyber Strategy does not explicitly call for legislative changes to enable private companies to "hack back" against adversaries in cyberspace. Authorizing private sector entities to engage in offensive cyber operations raises longstanding legal and policy questions. The Computer Fraud and Abuse Act (CFAA) generally prohibits unauthorized access to computer systems and provides for both criminal and civil penalties.[1] Many U.S. states and non-U.S. jurisdictions have enacted similar legal frameworks.

Any attempt to more directly involve the private sector in offensive cyber actions will likely require further legal and regulatory changes before it can be meaningfully implemented. Even if the administration were to issue new enforcement guidance redirecting prosecutions away from hack-back cases, the availability of civil penalties under the CFAA and its five-year statute of limitations would likely render such executive actions significantly less impactful. Technology companies should consider closely monitoring developments to track how the administration plans to enact such incentives.

Pillar II: Promote Common-Sense Regulation. The U.S. Cyber Strategy critiques the current landscape of cyber regulations as a "costly checklist" that weakens preparedness and response. It also commits to streamlining cyber regulations to reduce compliance costs and improve alignment between regulators and industry. This pillar reflects continuity with other actions the Trump administration has taken to limit the regulatory burden cybersecurity requirements impose, and even certain initiatives of the Biden administration. The U.S. Cyber Strategy seeks to empower the private sector with the "agility necessary to keep pace with rapidly evolving threats."

Pillar III: Modernize and Secure Federal Government Networks. The administration commits to accelerating the modernization of federal information systems through the implementation of post-quantum cryptography, zero-trust architecture and cloud transition. AI-powered cybersecurity solutions are explicitly identified as a solution for defending federal networks. The U.S. Cyber Strategy also commits to creating competitive procurement processes and removing barriers to entry so the government can access the best available technology, signaling that the administration seeks to broaden the pool of vendors for cybersecurity work. This mirrors more general efforts by the Trump administration to support nontraditional defense contractors as part of its broader reindustrialization goals.

Pillar IV: Secure Critical Infrastructure. The U.S. Cyber Strategy prioritizes hardening the defenses of America's critical infrastructure, making specific reference to the energy grid, financial and telecommunication systems, data centers, water utilities, and hospitals. The U.S. Cyber Strategy promotes the use of U.S. technologies in critical infrastructure environments, reflecting longstanding national security concerns about the presence of adversary-origin technology in critical infrastructure systems. The anticipated release of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) final rule in May 2026 may provide an early indicator of how this pillar will be executed in practice. The details of this final rule, which was delayed from its original October 2025 publication date to incorporate industry feedback, will show how the Trump administration attempts to balance the tension between heightened security requirements in these high-risk sectors and its general objective of mitigating regulatory burdens.

Pillar V: Sustain Superiority in Critical and Emerging Technologies. The U.S. Cyber Strategy highlights the Trump administration's support for developing secure technologies that protect "user privacy from design to deployment," with explicit attention drawn to cryptocurrencies and blockchain technologies, post-quantum cryptography, and secure quantum computing. Building off its AI Action Plan, the Trump administration calls out the importance of securing the entire AI technology stack, including data centers, training data and AI models. The U.S. Cyber Strategy also emphasizes the deployment of agentic AI and AI-enabled cyber tools to autonomously detect and disrupt foreign threats.

Pillar VI: Build Talent and Capacity. The U.S. Cyber Strategy characterizes the cyber workforce as a strategic asset worthy of significant investment to bolster the other pillars. The U.S. Cyber Strategy envisions an accessible talent pipeline spanning academia, vocational schools, corporations and the military. It does not provide details on how such a pipeline will be developed or sustained.

[1] 18 U.S.C. § 1030.

Trump Administration Releases Cyber Strategy

Key Takeaways

- **The U.S. Cyber Strategy signals a proactive, offense-oriented shift in the U.S. cybersecurity posture.** The Trump administration's willingness to publicly champion the deployment of offensive cyber capabilities, including by raising the prospect of private sector engagement, reflects an ongoing evolution in how it intends to communicate, resource and prosecute its interests in the digital domain.
- **Private sector participation in offensive operations raises unresolved legal questions.** The U.S. Cyber Strategy's vision for incentivizing private entities to identify and disrupt adversary networks will likely require legal and regulatory changes before it can be implemented, and companies should consider monitoring closely how the administration moves to enact such incentives.
- **Deregulation is a central theme, but the details will matter.** The U.S. Cyber Strategy's commitment to reducing compliance burdens is consistent with the administration's broader deregulatory agenda, but its practical implications will depend on how these high-level priorities are implemented, including in high-risk critical infrastructure sectors.
- **AI and emerging technologies remain an administration focus.** Read alongside the White House's AI Action Plan, the U.S. Cyber Strategy makes clear that securing the full AI technology stack is a core national security priority and key component of strategic infrastructure. Stakeholders should anticipate continued federal government attention to this sector. The U.S. Cyber Strategy's explicit call for AI-powered cybersecurity solutions also functions as a clear demand signal for vendors that are positioned to provide these capabilities to the federal government.
- **The high-level nature of the U.S. Cyber Strategy means the scope of changes turns on follow-on implementation.** As a statement of broad intent rather than a detailed policy framework, the U.S. Cyber Strategy defers many of the decisions that will matter most to corporate stakeholders — including changes to cybersecurity compliance frameworks, legal rules regarding private sector involvement in offensive cyber actions, and procurement processes — to future implementing actions. The U.S. Cyber Strategy does not create any changes to legal obligations, but boards should consider closely monitoring follow-on developments for insight into the rules and opportunities the White House's cybersecurity agenda creates for companies operating in this space.

Contacts

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Lisa V. Zivkovic
Associate / New York
212.735.2887
lisa.zivkovic@skadden.com

Jake Dow
Associate / Washington, D.C.
202.371.7028
jake.dow@skadden.com