Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

The Trump Administration's Cyber Strategy

March 11, 2026

On March 6, 2026, the White House released *President Trump's Cyber Strategy for America* (the strategy). The document builds upon earlier cyber-related actions and describe the Administration's policies and postures on cybersecurity. This Insight describes these documents and provides context for Congress.

The Cyber Strategy

The Administration's Cyber Strategy includes six pillars—each of which mirrors previous governmental policies toward improving cybersecurity. The pillars are cross-cutting and would involve a variety of federal agencies (e.g., Department of Defense, Department of Justice, and Department of Homeland Security) as well as the private sector.

1. **Shape Adversary Behavior—**The Administration asserts goals related to using all instruments of U.S. power (e.g., instruments of national power and the private sector) to identify, disrupt, and overcome adversaries. The goal of shaping behavior appears focused on combatting malicious activity in cyberspace. This mirrors the "layered cyber deterrence" strategy outlined by the congressionally-established Cyberspace Solarium Commission.
2. **Promote Common Sense Regulation—**The Administration would like to streamline cybersecurity regulations. Regulatory burden has been an oft-discussed cyber issue across previous Administrations. The Biden Administration sought public comment on the issue.
3. **Modernize and Secure Federal Government Networks—**The Administration would like to accelerate the deployment of post-quantum cryptography, artificial intelligence (AI)-enabled cybersecurity tools on federal networks, and improve procurement of modern cybersecurity tools. The Administration would also like to increase threat-hunt operations for federal agencies.
4. **Secure Critical Infrastructure—**The Administration highlights energy, financial services, telecommunications, data centers (part of the information technology sector), water utilities, healthcare, and operational technology (broadly) as sectors it should

Congressional Research Service
https://crsreports.congress.gov
IN12667

prioritize identifying and protecting assets. The Administration also wants to advance supply chain security, a repeated goal from the first Trump Administration.

5. **Sustain Superiority in Critical and Emerging Technologies**—Quantum computing, cryptocurrencies, blockchain, and AI are highlighted as technologies paramount to American innovation. The Administration also seeks to use diplomacy as a tool in this pillar to encourage other nations to adopt American AI policies and technologies. The previous Administration's strategy also discussed the importance of emerging technologies.
6. **Build Talent and Capacity**—The Administration considers the cyber workforce a strategic national asset, and wants to help build out a talent pipeline. The previous Administration also sought to address cyber education and workforce challenges through national, strategic initiatives.

The National Cyber Director said that this strategy would be accompanied by an action plan. That plan does not appear to have been released along with this strategy. The action plan itself may reveal differences and nuance between the Trump Administration's cyber strategy and those of previous Administrations.

Considerations for Congress

The strategy provides high-level policy outlines of the Administration's cybersecurity objectives. How these objectives are accomplished and what effects these documents might have on agency budget requests and priorities remain to be seen. While Congress awaits greater detail (e.g., in a plan or through executive orders), it may choose to consider the implications of current policy and how this may be encouraging or discouraging the Administration's goals.

Cyber Workforce

The strategy calls the cyber workforce a "strategic asset." Congress has taken interest in the nation's cybersecurity workforce in the past—enacting laws related to scholarships, recruitment and retention, and compensation of cyber-skilled federal employees. Congress has also investigated the pipeline of workers available for cybersecurity jobs across the country and within the armed services. Congress may choose to conduct oversight on existing cyber workforce growth initiatives, or expand workforce considerations to include the role of immigration, AI and automation, and reducing barriers for workers to have their careers include both government and the private sector work.

Federal Network Security

The Administration is seeking to advance zero-trust architecture, post-quantum cryptography, cloud computing, and AI to improve federal network security. However, the Trump Administration rescinded some of the Biden Administration's previous efforts to achieve these same outcomes. The extent to which the Trump Administration's efforts will be evolutionary, complementary, or antithetical to previous efforts, or substitute for them, remains to be seen.

Most of Congress's concerns around federal network security focus on authorities and resources. For instance, such issues were addressed when Congress updated the main federal information technology security law (the Federal Information Security Modernization Act of 2014, or FISMA) in 2014. There have been recent attempts to update it. Additionally, the Administration may identify authority and gaps in resources that it requests Congress to address. For instance, multiple Administrations have surfaced the

issues of costs associated with maintaining legacy systems and purchasing cybersecurity tools as a source of risk for federal agencies.

Private Sector Engagement

The strategy seeks to incentivize the private sector to find and disrupt adversarial networks. This is akin to the "hack-back"debate Congress has engaged in for a number of years. It has been difficult to advance the debate, because there are many outstanding questions:

- Will private companies be vetted to conduct offensive activities, and if so, how?
- How will adversary targets be identified and approved?
- What capabilities can be used against adversaries?
- What, if any, liability protections will the private sector be afforded?
- What is the role of insurance for hack-back companies? and
- What risks would the company and nation be exposed to under such a system?

The previous cyber strategy also sought to engage the private sector, but to collaborate on combatting malicious actors and building more secure products. This strategy suggests that the private sector will directly and independently engage malicious cyber actors.

Offensive Activities

The strategy suggests a more aggressive posture from the United States government pertaining to the actions it may take against adversaries. The past four Administrations have issued sanctions and indictments in response to cyberattacks. Congress has authorized the Department of Defense (now "using a secondary Department of War designation," under Executive Order 14347 dated September 5, 2025) to engage nation-state adversaries and Mexican TCOs in cyberspace. It is unclear if the Trump Administration will request new authorities or resources to engage in amplified cyber-offensive activities.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer

as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.