wiley

ALERT

# New National Cyber Strategy and EO Lays Out a Path for Combating Cybercrime and Promoting Innovation

March 11, 2026

On March 6, 2026, the White House unveiled *President Trump's Cyber Strategy for America*. The Cyber Strategy outlines the Administration's priorities for ensuring that America remains unrivaled in cyberspace," grouped together under six "Pillars of Action." Acknowledging the "growing number and severity of cyber threats," the new Cyber Strategy notably focuses "disrupting adversaries' cyber campaigns" and "creating incentives [for the private sector] to identify and disrupt adversary networks." Additionally, key themes throughout the Cyber Strategy include promoting coordination between the government and the private sector, implementing efforts to make American networks more defensible and resilient, and removing ineffective regulations to promote innovation. In conjunction with the release of the Cyber Strategy, the President also signed an Executive Order (March 6 EO) on combating cybercrime and fraud and released an associated Fact Sheet. The March 6 EO directs federal law enforcement agencies to develop tools to better combat transnational criminal organizations responsible for cyber scams and fraud. These developments are an extension of President Trump's "America First" agenda into cyberspace and also support the National Security Strategy.

Below, we provide a summary of the Cyber Strategy and the March 6 EO. While the Cyber Strategy is high-level at this stage, additional Executive Orders are expected that will fill out the details under the six Pillars of Action.

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law


## Practice Areas

AI Executive Order
Artificial Intelligence (AI)
Emerging Technologies
Government Contracts
Government Contracts
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology
Trump Administration Resource Center

### *The Cyber Strategy*

The Cyber Strategy outlines six Pillars of Action, which are intended to guide implementation, resourcing, and measures for success through "follow on policy vehicles." The six pillars are as follows:

1. ***Shape Adversary Behavior.*** This pillar declares the Administration will deploy its "full suite of U.S. government defensive and offensive cyber operations" to fend off adversaries in cyberspace. In addition to government action, this pillar discusses "unleash[ing] the private sector by creating incentives to identify and disrupt adversary networks and scale our national capabilities." Chief among the goals of this pillar are to "detect, confront, and defeat cyber adversaries before they breach our networks and systems." The pillar frames deterrence as creating risk and consequences for adversaries and eroding their capacity and capability. It also states that the costs and responsibility for defending cyberspace should be shared between the U.S. and its allies.
2. ***Promote Common Sense Regulation.*** This pillar articulates the Administration's goal to "streamline cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally," which the Cyber Strategy declares as a better approach than imposing "costly checklist[s]." This will include "data and cybersecurity regulations to ensure the private sector has the agility … to keep pace with … evolving threats," while protecting "the right to privacy for Americans and American data."
3. ***Modernize and Secure Federal Government Networks.*** To advance federal information system modernization and resilience, this pillar focuses on implementing "cybersecurity best practices, post-quantum cryptography, zero-trust architecture, and cloud transition" with respect to federal information systems. The pillar also emphasizes several priorities to modernize and secure federal networks, including: raising the importance of cyber in government leadership and the boardroom; using the best technologies and teams; testing and hunting for threat actors on federal networks; prioritizing the security and resilience of National Security Systems; adopting AI-powered cyber solutions; modernizing competitive procurement processes; and removing barriers to buying the best technologies.
4. ***Secure Critical Infrastructure.*** This pillar states that "[w]e will identify, prioritize, and harden America's critical infrastructure and secure its supply chains, including defense critical infrastructure and adjacent vendors, private companies, networks, and services—such as the energy grid, financial and telecommunication systems, data centers, water utilities, and hospitals – securing information and operational technology supply chains." It also discusses efforts to secure the IT and operational technology supply chains while moving away from "adversary" country vendors. Of note, the pillar emphasizes that state, local, Tribal, and territorial authorities should be a "complement to – not substitute for – national cybersecurity efforts."
5. **Sustain Superiority in Critical and Emerging Technologies.** This pillar discusses building technology tools and supply chains in the United States that are secure "from design to deployment," including "supporting the security of cryptocurrencies and blockchain technologies" and promoting post-quantum cryptography and secure quantum systems. This pillar emphasizes the need to secure the U.S. AI tech stack, and points to securing networks through use of agentic AI. It also highlights cyber

diplomacy focused on ensuring AI around the globe is secure and not used to "censor, surveil, and mislead."

6. ***Build Talent and Capacity.*** The final pillar of the Cyber Strategy focuses on efforts to educate and train cybersecurity personnel and champion U.S. economic growth. This pillar notes the need for a "pragmatic and accessible" pipeline that draws on existing resources in academia, industry, and venture capital.

***The March 6 EO***

The March 6 EO, entitled *Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens*, establishes a process and timeline for the Administration to conduct a comprehensive review to determine what "operational, technical, diplomatic, and regulatory" tools could be improved to combat transnational criminal organizations (TCOs) engaged in cyber-enabled crime and predatory schemes.

The March 6 EO states: "It is the policy of the United States to protect Americans from, and harden our financial and digital systems against, these threats [from TCOs]. The United States shall counter attacks on Americans with a commensurate response that includes law enforcement, diplomacy, and potential offensive actions. It is further the policy of the United States to provide support to victims of these crimes, expand public alerts, and prioritize protection for those most at risk to end the exploitation and victimization of Americans."

The March 6 EO requires the Secretary of State, the Secretary of the Treasury, the Secretary of War, the Attorney General, and the Secretary of Homeland Security, in consultation with the Office of the National Cyber Director, and in coordination with the Assistant to the President and Homeland Security Advisor to: (1) "review the relevant operational, technical, diplomatic, and regulatory frameworks in place to determine how each can be improved to best combat TCOs engaged in cyber-enabled crime and similar predatory schemes against Americans," and (2) formulate and submit to the President an action plan "that identifies the TCOs responsible for scam centers and cybercrime and proposes solutions to prevent, disrupt, investigate, and dismantle these TCOs."

In conjunction, the March 6 EO directs that there will be a dedicated "operational cell within the National Coordination Center (NCC) ... which will be responsible for coordinating federal efforts to detect, disrupt, dismantle, and deter – including by involving the private sector as appropriate – cyber-enabled criminal activity conducted by foreign TCOs and associated networks that target United States persons, businesses, critical infrastructure, or public services." The action plan and NCC operational cell are required to "include mechanisms to improve information sharing, operational coordination, and rapid response across the Federal Government." These activities are required to align with existing law enforcement efforts against foreign cyber-enabled threats.

Additionally, the March 6 EO directs the following actions:

- The Attorney General shall continue to prioritize prosecutions of cyber-enabled fraud and scam schemes.

- The Secretary of Homeland Security shall partner with the NCC to provide training, technical assistance, and resilience building against cyber threats for state and local partners.
- The Attorney General shall submit a recommendation regarding the establishment of a Victims Restoration Program to return seized or forfeited funds from fraudsters directly to victims.
- The Secretary of State shall engage with foreign governments regarding demands to take enforcement action against TCOs and impose consequences on countries that tolerate these schemes.

***

These latest cyber policy developments from the White House will set in motion new lines of effort across the federal government, with impacts on the private sector, including but not limited to federal contractors.

Wiley's cross-disciplinary Privacy, Cyber & Data Governance, National Security, International Trade, Strategic Competition & Supply Chain, and Government Contracts teams have significant experience advising clients on all aspects of regulatory and policy strategies and compliance. We engage with key government stakeholders in these dynamic areas and can guide companies interested in exploring the impacts and opportunities created by the Cyber Strategy and EO.