MAYER | BROWN

MARCH 09, 2026

TRUMP ADMINISTRATION RELEASES CYBER STRATEGY FOR AMERICA AND RELATED EXECUTIVE ORDER ON COMBATTING CYBERCRIME

AUTHORS:

RAJESH DE, HOWARD W. WALTZMAN, ADAM S. HICKEY, STEPHEN LILLEY, JUSTIN HERRING, AARON FUTERMAN, HADASSAH G. DIAMENT

On March 6, 2026, the Trump Administration released President Donald Trump's Cyber Strategy for America (the "Cyber Strategy"), a seven-page framework outlining the President's vision for protecting American interests in cyberspace. The strategy signals significant shifts in federal cybersecurity policy, including a more aggressive cyber deterrence posture, a common-sense approach to cybersecurity regulation, expanded reliance on and cooperation with the private sector to respond to cybersecurity threats, and accelerated adoption of artificial intelligence and other emerging technologies for network defense.

In addition, in alignment with the Cyber Strategy, President Trump issued an Executive Order on Combatting Cybercrime, Fraud, and Predatory Schemes Against American Citizens, directing the federal government to take steps to combat transnational cybercrime through enhanced interagency coordination, public-private collaboration, and diplomacy.

This Legal Update summarizes the key priorities and policy pillars from the Cyber Strategy and the related Executive Order.

PRESIDENT TRUMP'S CYBER STRATEGY FOR AMERICA

The strategy positions cybersecurity as central to national security and frames American leadership in cyberspace as an extension of broader economic, technological, and military priorities. It also commits to "proactive, coordinated, and sustained action" rather than "partial measures and ambiguous strategies."

The strategy departs from key portions of the Biden Administration's 2023 National Cybersecurity Strategy, which emphasized, in part, mandatory compliance requirements for critical infrastructure and sought to shift liability toward software developers for insecure products. It also builds on the Trump Administration's June 2025 Cybersecurity Executive Order, which rescinded prescriptive federal IT mandates, while focusing on the modernization of federal information technology.

The Cyber Strategy is organized around six policy pillars that identify high-level strategic directions going forward:

Pillar 1: Shape Adversary Behavior. The first pillar puts additional emphasis on offensive cyber operations as a key tool of US policy, directing "the full suite of US government defensive and offensive cyber operations" and committing to "unleash the private sector by creating incentives" to disrupt adversary networks. The strategy also pledges to "uproot criminal infrastructure and deny financial exit and safe haven."

Pillar 2: Promote Common Sense Regulation. The strategy expresses the Administration's intent to "streamline cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally," stating that "[c]yber defense should not be reduced to a costly checklist[.]" This pillar also says that the Administration will "emphasize the right to privacy for Americans and American data."

Pillar 3: Modernize and Secure Federal Government Networks. The strategy calls for implementing "cybersecurity best practices, post-quantum cryptography, zero-trust architecture, and cloud transition," and the adoption of "AI-powered cybersecurity solutions to defend federal networks and deter intrusions at scale." It also calls for modernized procurement processes to "remove barriers to entry so that the government can buy and use the best technology."

Pillar 4: Secure Critical Infrastructure. Critical infrastructure—including the energy grid, financial and telecommunications systems, data centers, water utilities and hospitals—is identified as a top priority for hardening and supply chain security. The strategy calls for moving away from "adversary vendors and products" and promoting US technologies. The strategy refers to state, local, Tribal, and territorial authorities as a complement to, but not a substitute for, national cybersecurity efforts.

Pillar 5: Sustain Superiority in Critical and Emerging Technologies. The strategy pledges to build secure technologies that protect "user privacy from design to deployment," including explicit support for "the security of cryptocurrencies and blockchain technologies[]" and post-quantum cryptography and secure quantum computing. The Administration also commits to securing the full AI technology stack, from data centers to the models themselves, while prioritizing the deployment of agentic AI and cyber tools to autonomously detect and disrupt foreign threats. It also addresses countering "the spread of foreign AI platforms that censor, surveil, and mislead their users."

Pillar 6: Build Talent and Capacity. The strategy calls for eliminating roadblocks that prevent "industry, academia, government, and the military from aligning incentives and building a highly skilled cyber workforce[,]" instead envisioning a talent pipeline spanning "academia, vocational and technical schools, corporations, and venture capital."

EXECUTIVE ORDER ON COMBATTING CYBERCRIME

President Trump also issued an Executive Order on combatting cybercrime, which operationalizes key elements of the Cyber Strategy's first and fourth pillars. The Order establishes a whole-of-government effort to protect Americans from cyber-enabled fraud, ransomware, extortion, and related predatory schemes orchestrated by transnational criminal organizations. Key directives include:

- Creation of a coordination cell within the National Coordination Center to detect, disrupt, dismantle, and deter cyber-enabled criminal activity targeting US persons, businesses, and critical infrastructure.

- A 60-day interagency review of "relevant operational, technical, diplomatic, and regulatory frameworks" for combating transnational cybercrime, and an action plan within 120 days identifying responsible criminal networks and possible solutions to disrupt those networks.
- Leveraging technical capabilities, threat intelligence, and operational insights from commercial cybersecurity firms to enhance attribution and disruption of malicious actors.
- Diplomatic engagement with foreign governments for enforcement actions against transnational criminal organizations, with threatened consequences—including sanctions, visa restrictions, trade penalties, and expulsion of complicit officials—for countries that tolerate predatory activity.
- A recommendation within 90 days from the Department of Justice on establishing a Victim Restoration Program to provide restitution from seized or forfeited funds of cybercriminals.

LOOKING AHEAD

The Trump Administration has indicated that the Strategy "will guide action and resourcing through the follow-on policy vehicles[,]" suggesting that companies should anticipate additional executive orders, agency directives, and potential legislative proposals to operationalize the strategic pillars. Companies should continue to monitor key developments as the Trump Administration works to implement the cyber agenda reflected in the Strategy.

AUTHORS

PARTNER

RAJESH DE

WASHINGTON DC +1 202 263 3366

RDE@MAYERBROWN.COM

ASSOCIATE

HADASSAH G. DIAMENT

WASHINGTON DC +1 202 263 3260

HDIAMENT@MAYERBROWN.COM

ASSOCIATE

AARON FUTERMAN

WASHINGTON DC +1 202 263 3161

AFUTERMAN@MAYERBROWN.COM

PARTNER

JUSTIN HERRING

NEW YORK +1 212 506 2878

JHERRING@MAYERBROWN.COM

PARTNER

ADAM S. HICKEY

WASHINGTON DC +1 202 263 3024

NEW YORK

AHICKEY@MAYERBROWN.COM

PARTNER

STEPHEN LILLEY

WASHINGTON DC +1 202 263 3865

NORTHERN CALIFORNIA (PALO ALTO & SAN FRANCISCO)

SLILLEY@MAYERBROWN.COM

PARTNER

HOWARD W. WALTZMAN

WASHINGTON DC +1 202 263 3848

HWALTZMAN@MAYERBROWN.COM