Insights, News & Events

WHITE HOUSE UNVEILS NEW CYBER STRATEGY TO REDUCE REGULATION AND GO ON THE OFFENSE AGAINST CYBERCRIMINALS

Insights
Mar 18, 2026

White House Unveils New Cyber Strategy to Reduce Regulation and Go On the Offense Against Cybercriminals

The White House recently published two documents to outline how the US plans to lead the world in cybersecurity while protecting Americans from cybercrime. Combined, the Cyber Strategy for America and the Executive Order on Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens released on March 6 outline the Administration's new approach to this important subject. What do businesses need to know about these latest publications and what should you be watching for in the future?

Offensive Strategy Outlined in Groundbreaking Document

Related People

Daniel Pepper, CIPP/US
Partner

303.218.3661

Jillian Seifrit, CIPP/US
Associate

610.230.6129

Historically, the national cybersecurity policy has been largely reactive: patching systems, issuing incident reports, and notifying affected individuals upon the event of a cyberattack. President Trump's Cyber Strategy for America focuses on offensive cyber operations to defect criminals before they ever have a chance to breach American networks.

The Strategy has six pillars for success.

1. Shape Adversary Behavior: The government will work with the private sector to identify and disrupt cyber criminals. This public-private coordination is intended to distribute the cost burden of cyber defense while hardening protections for individuals and enterprises alike.

2. Cut Red Tape: The Administration has made it clear that it favors less regulation in most aspects for US businesses – and cyber is no different. The Strategy emphasizes fewer compliance checklists and more streamlined regulatory frameworks, while acknowledging the continuing need to protect American's privacy.

3. Modernize Networks: This pillar emphasizes adoption of key technical controls: AI-powered threat detection, post-quantum cryptography, and zero-trust architecture.

4. Secure Critical Infrastructure: By promoting US technologies, the Administration wants to harden America's critical infrastructure including private companies.

5. Technology Superiority: Similarly to pillar 3, the Administration stresses the need to utilize AI to secure our networks. The Administration has made it clear that it wants the US to lead the world in AI technology, and it wants to use that tech when it comes to cybersecurity. Expect reduced compliance friction and increased government procurement demand for AI-based cybersecurity solutions.

6. Best Talent: The last pillar discusses the need for robust talent in this area and to recruit the next generation to utilize our advanced technologies.

The Executive Order Sets an Aim to Go After the Criminals

Meanwhile, the Executive Order sets out a robust plan to target Transnational Criminal Organizations (TCOs). It creates a new operational cell inside the National

Service Focus

Data Protection and Cybersecurity

Government Relations

Privacy and Cyber

Coordination Center (NCC) designed to prevent, disrupt, investigate, and dismantle the TCOs operations.

The Secretary of State, the Secretary of the Treasury, the Secretary of Defense, 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 (APHSA), are directed to review existing frameworks and identify necessary improvements by early May 2026. Also, they must deliver a full action plan proposing solutions for targeting TCOs by July 2026.

Further, the Secretary of State is directed to pressure foreign governments to crack down on TCOs operating within their country. If those countries ignore criminal activity, the Order threatens limitation of foreign assistance, targeted sanctions, visa restrictions, trade penalties, and expulsion from complicit officials.

What Happens to the Criminal's Money?

Within 90 days of the Order, the Attorney General must submit a proposal for a Victims Restoration Program funded directly from assets seized and forfeited from cyber criminals.

What to Watch Next

The Administration wants to lead the world with cybersecurity resilience with as little regulation as possible. Rather than mandating reporting obligations, the Administration is prioritizing innovation and incentive-based mechanisms to protect individuals and critical infrastructure.

If you operate in a highly regulated space, pay close attention to potential changing cyber reporting regulations that may ease the requirements. However, do not lose sight of the key takeaways from these two new releases – which is to protect American's privacy and American infrastructure.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, contact your Fisher Phillips attorney, the authors

of this Insight, or any attorney on our Data Protection and Cybersecurity Team.