KPMG

Regulatory Alert

Regulatory Insights

March 2026

Cybersecurity: New Cyber Strategy; Cybercrime Executive Order

---

KPMG Regulatory Insights:

Cyber Strategy:
Policies and priorities intended to support American leadership in the digital world in areas such as "finance, innovation and emerging technology, military power, and manufacturing."

Combating Cybercrime:
Directive to harden financial and digital systems against cyber threats, support victims, and counter attacks through "law enforcement, diplomacy, and potential offensive actions."

Aligning Goals:
Key features include government coordination (across federal agencies and between federal and state/local authorities), public-private collaboration (to expand innovation and scale), and engagement with foreign governments (including a focus on enforcement actions and potential for other consequences, where appropriate.)

Looking Ahead:
Organizations will need strong cybersecurity programs consistent with existing frameworks (e.g., NIST, ISO 27001) to respond to evolving cybercrime risk, including impacts to critical infrastructure, and given the expectation of an increase in public-private collaboration.

The Administration has released its "Cyber Strategy for America" (Cyber Strategy) and issued an Executive Order, entitled "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens". Together, these actions outline the Administration's intended approach to cybersecurity, aligning high-level strategic policies and priorities with near-term operational directives.

The Cyber Strategy provides overarching policy architecture, while the Executive Order establishes immediate priorities for interagency coordination, enforcement, and international cooperation.

Cyber Strategy

The Cyber Strategy articulates the Administration's long-term direction for federal cybersecurity policy. It frames cybersecurity as integral to national security and economic competitiveness and emphasizes coordinated action across federal agencies and the private sector. The strategy is organized around six policy pillars that collectively address deterrence, regulatory approach, network security, infrastructure resilience, technological leadership, and workforce development. The pillars are outlined on the following page.

Strategy Policy Pillar	Details
Shape Adversary Behavior	— Emphasize deterrence through the full range of U.S. government cyber capabilities (offensive and defensive) — Incentivize private-sector identification and disruption of malicious actors and adversary networks to scale national capabilities
Promote "Common Sense" Regulation	— Streamline data and cybersecurity regulations with alignment across regulators and industries — Focus on liability and privacy protection
Modernize and Secure Federal Government Networks	— Implement cybersecurity best practices, zero-trust architectures, post-quantum cryptography, and cloud transition — Adopt AI-enabled security tools, and reform procurement to facilitate access to advanced technologies — Elevate cyber in public and private leadership
Secure Critical Infrastructure	— Identify, prioritize, and harden critical infrastructure and related supply chains for defense and adjacent vendors, companies, networks, and services — Key sectors include: - Energy - Financial services - Telecommunications - Data centers - Water utilities - Healthcare — Promote and employ US technologies; reduce reliance on adversary-linked vendors — State, local, Tribal, and territorial (SLTT) authorities to complement, not substitute for, national cybersecurity efforts
Sustain Superiority in Critical and Emerging Technologies	— Emphasize critical emerging technologies, including: - AI (including data centers, AI-enabled cyber tools) - Quantum computing technologies - Cryptography (including quantum cryptography) - Digital asset infrastructure (including blockchain) — Promote security-by-design principles across emerging technologies (including generative AI and agentic AI)
Build Talent and Capacity	— Reconcile cyber-related education and training to promote a talent pipeline across academia, technical/vocational schools, corporations, and venture capital — Align incentives across industry, academia, government, and the military to develop a stronger and more integrated cybersecurity workforce pipeline (across industries and occupations)

Executive Order on Combating Cybercrime

The Executive Order focuses on near-term operational measures to counter cyber-enabled fraud, ransomware, extortion, and related predatory schemes, particularly those conducted by transnational criminal organizations (TCOs). It emphasizes coordination across federal agencies, engagement with the private sector, and use of diplomatic and enforcement tools.

Executive Order Key Areas	Details
Interagency coordination	**Directs:** — Establishment of a coordination cell within the National Coordination Center (NCC) — Detection, disruption, dismantlement, and deterrence of cyber-enabled criminal activity targeting U.S. persons, businesses, and critical infrastructure
Strategic review and action planning	**Initial efforts include:** — 60-day review of operational, technical, diplomatic, and regulatory tools for combating transnational cybercrime — 120-day action plan identifying responsible criminal networks and potential disruption measures
Public-private collaboration	**Encourages:** — Use of threat intelligence, technical capabilities, and operational insights from commercial cybersecurity firms as support for attribution and disruption of malicious actors
Enforcement and restitution	**Demands:** — Diplomatic engagement with foreign governments to pursue enforcement actions against cybercriminal organizations — Department of Justice recommendations on establishing a Victim Restoration Program to return seized or forfeited funds to victims

Agency responsibilities to implement the Executive Order are assigned as follows:

Agency/Official	Responsibility	Deadline
Interagency: — **Secretary of State** — **Secretary of the Treasury** — **Secretary of War** — **Attorney General** — **Secretary of Homeland Security** In consultation with the Office of the National Cyber Director and the Assistant to the President and Homeland Security Adviser (APHSA):	Combat TCOs through review of, and identification of improvements to, existing operational, technical, diplomatic, and regulatory frameworks	60 days
	Submit an action plan: — Identifying TCOs responsible for scam centers and cybercrime — Proposing solutions to prevent, disrupt, investigate, and dismantle these organizations — Providing for the creation of an operational cell within the NCC to coordinate federal efforts — Describing engagement with public companies/resources	120 days
Attorney General	Prioritize prosecutions of cyber-enabled fraud	Ongoing
	Recommend through APHSA a Victim Restoration Program for cybercrime, fraud, and predatory schemes	90 days
Secretary of Homeland Security	Acting through CISA in partnership with NCC, support SLTT (state, local, Tribal and territorial government) partners with training, technical assistance, and resilience building	Ongoing
Secretary of State	Engage foreign governments	Ongoing
	Apply consequences for non-cooperation, including: — Foreign assistance limitations — Targeted sanctions — Visa restrictions — Trade penalties — Where appropriate, expulsion from the U.S. of foreign officials and diplomats complicit in cyber-enabled schemes	Ongoing

For more information, please contact Michael Isensee or Matt Miller.

Contact

Laura Byerly
Managing Director
Regulatory Insights
lbyerly@kpmg.com

Brian Hart
Principal
Risk, Regulatory and Compliance
bhart@kpmg.com