CLIENT ALERT | March 10, 2026

President Trump's Cyber Strategy and Executive Order Combating Cybercrime: Key Takeaways

The executive actions emphasize public-private partnerships, enhanced information sharing, and leveraging commercial cybersecurity capabilities.

On March 6, 2026, President Trump signed an executive order titled "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens" (the Order) that directs an interagency coalition to improve existing policy frameworks to address cyber threats and target transnational criminal organizations. The White House also published the long-anticipated Cyber Strategy for America (the Cyber Strategy), which sets out six high-level pillars that will guide the administration's approach to cyber policy. Moreover, on March 9, 2026, National Cyber Director Sean Cairncross offered additional remarks concerning both the Order and the Cyber Strategy, including potential revisions to incident reporting rules.

This Client Alert identifies the key provisions of the Order and Cyber Strategy and provides initial considerations for those in the private sector.

Overview

The Order addresses a range of cyber-enabled criminal activity, including ransomware, malware, phishing, financial fraud, and extortion and impersonation schemes. The Order identifies transnational criminal organizations as the primary actors behind these schemes, noting that foreign regimes often provide "willing or tacit state support" to cybercrime.

Key Provisions

- **Interagency Review and Action Plan:** The Order directs 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, to conduct a review of existing operational, technical, diplomatic, and regulatory frameworks within 60 days, and to submit an action plan within 120 days to the president that identifies responsible transnational criminal organizations and proposes solutions to "prevent, disrupt, investigate, and dismantle them."

- **National Coordination Center Operational Cell:** The Order requires the establishment of an "operational cell" within the National Coordination Center (NCC) that will be responsible for coordinating federal efforts to "detect, disrupt, dismantle, and deter" cyber-enabled transnational

criminal activity that targets United States persons, businesses, critical infrastructure, and public services.

  - The operational cell is mandated to improve information sharing, operational coordination, and rapid response across the federal government to address cyber-enabled threats originating from foreign jurisdictions. Notably, beyond coordination within the government, the operational cell is directed to involve the private sector as appropriate in its efforts to combat transnational criminal organizations.

  - The operational cell is also directed to partner with the Secretary of Homeland Security in his capacity as Director of the Cybersecurity and Infrastructure Security Agency (CISA) to provide training, technical assistance, and resilience building to support state, local, tribal, and territorial (SLTT) partners, including to expand defensive capacity, share threat intelligence, and harden SLTT partners' critical infrastructure systems against cybercrime exploitation by transnational criminal organizations.

- **Prosecution Priorities:** The Order directs the Attorney General to continue prioritizing prosecutions of defendants engaged in cyber-enabled fraud (such as "scam centers" and sextortion schemes) and to pursue the most serious offenses.

- **Victim Restoration Program:** The Order directs the Attorney General to submit a recommendation within 90 days regarding the establishment of a Victims Restoration Program, intended to provide restoration or remission to victims of cyber-enabled fraud schemes from the funds clawed back, forfeited, or seized from the transnational criminal organizations that perpetrated such schemes.

- **International Engagement:** The Secretary of State is directed to engage with foreign governments to demand more robust cooperation with US law enforcement, including enforcement actions against transnational criminal organizations operating within their borders. The Order provides that the Secretary of State "shall take all necessary and appropriate steps" to ensure that foreign governments that "tolerate" predatory activity face consequences "consistent with United States law and policy," such as limits on foreign assistance, targeted sanctions, visa restrictions, trade penalties, and, where appropriate, expulsion of foreign officials and diplomats complicit in such cyber schemes.

Released on the same day, President Trump's Cyber Strategy for America calls for coordination across the federal government and the private sector to invest technologies and facilitate offensive and defensive cyber missions. The Cyber Strategy consists of six pillars but provides little detail. Instead, the Cyber Strategy sets out general objectives for combatting cyber threats and building a robust infrastructure and workforce to combat international cyber threats.

Of particular importance to the private sector, the Cyber Strategy cautions against over-regulation and states that cyber defense "should not be reduced to a costly checklist that delays preparedness, action, and response." Though not specifying how it would undertake this exercise, the administration highlights that it will be focused on streamlining cyber regulations "to reduce compliance burdens, address liability, and better align regulators and industry globally." As part of those efforts to streamline cyber regulations, Director Cairncross stated that the administration aims to "make sure that information flow is working well, that incident reporting makes sense to the industry, [and] that it's not overly burdensome."

In particular, Director Cairncross stated that the White House seeks to ensure that the "SEC disclosure rule makes sense for industry" and that the White House would review pending disclosure requirements created by CISA under the Cyber Incident Reporting for Critical Infrastructure Act to ensure that they "meet[] congressional intent."

Initial Takeaways

The Order does not impose direct obligations on private entities. It does, however, emphasize public-private partnerships, enhanced information sharing, and leveraging commercial cybersecurity capabilities. These efforts suggest that businesses — particularly those in the cybersecurity and technology sectors — may see increased engagement from federal agencies in the coming months. Moreover, other private sector entities experiencing cybersecurity incidents may experience greater levels of federal engagement, especially with regard to requests for indicators of compromise or threat actor tactics, techniques, and procedures.

Businesses should consider:

- Monitoring the development of the interagency action plan and the NCC operational cell, as well as any forthcoming guidance on information-sharing mechanisms
- Assessing current threat intelligence capabilities and incident response procedures in anticipation of potential federal outreach
- Reviewing contracts and policies related to information sharing with government entities, particularly for cybersecurity and technology companies
- Evaluating exposure to cyber-enabled fraud and considering whether heightened engagement with federal law enforcement is warranted
- Remaining informed concerning forthcoming regulations, guidance, or voluntary frameworks that may emerge from the interagency action plan or efforts to streamline cyber regulations, especially potential revisions to the SEC's 2023 incident disclosure rule or other disclosure rules such as the pending CISA rules

- Remaining mindful of administration requests of the private sector, given comments from Director Cairncross that private sector CEOs are expected to "dedicate some real resources"

Latham & Watkins will continue to monitor developments related to the Order and Cyber Strategy, in particular the administration's efforts to stand up the operational cell and streamline cybersecurity regulations, including the SEC's cybersecurity disclosure requirements.

The authors would like to thank Andreas Pavlou for his contribution to this Client Alert.

Contacts

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Marissa R. Boynton
marissa.boynton@lw.com
+1.202.637.3307
Washington, D.C.

Antony (Tony) Kim
antony.kim@lw.com
+1.202.637.3394
Washington, D.C.

Clayton Northouse
clayton.northouse@lw.com
+1.202.637.3371
Washington, D.C.

Michael H. Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

Serrin Turner
serrin.turner@lw.com
+1.212.906.1330
New York