

# Cybersecurity and Data Privacy Update

March 23, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West  
New York, NY 10001  
212.735.3000

1440 New York Ave., NW  
Washington, DC 20005  
202.371.7000

320 S. Canal St.  
Chicago, IL 60606  
312.407.0700

## White House Announces Cybercrime Executive Order

### Executive Summary

- **What’s new:** On March 6, 2026, President Trump issued an executive order directing federal agencies to develop an action plan to more aggressively combat transnational criminal organizations engaged in cybercrime targeting Americans.
- **Why it matters:** The order is part of a growing push to enlist the private sector in both investigation and disruption of malicious cyber actors, and it instructs the Justice Department to develop a recommendation for a Victims Restoration Program that would use funds seized from threat actors to compensate victims of cybercrime.
- **What to do next:** Businesses should consider monitoring the implementation of the EO for greater clarity as to how the administration plans to integrate private sector engagement in government cyber actions and to assess whether a Victim Restoration Fund is established and, if so, what eligibility criteria apply to receive support.

On March 6, 2026, President Donald Trump signed Executive Order 14390 (the EO or Order), “Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens,” which directs federal agencies to develop plans to more aggressively combat cybercrime targeting the U.S. The order, released on the same day as the president’s Cyber Strategy for America, is further indication that the Trump administration intends to broaden the role of the private sector in the government’s offense-oriented approach to cyber threats.

The EO identifies a broad range of threats, including “ransomware and malware, phishing, financial fraud, ‘sextortion’ and other extortion schemes, impersonation, and more,” which the government intends to counter with “law enforcement, diplomacy, and potential offensive actions.” The Order calls for a coordinated, multiagency approach to enhance victim support, disrupt the transnational criminal organizations (TCOs) that often carry out cybercrimes, and increase international pressure on foreign jurisdictions that harbor cybercriminals.

### Key Points in the EO

**Action plan.** The core of the EO is a directive to the secretaries of state, treasury, war<sup>1</sup> and homeland security, as well as the attorney general, in consultation with the Office

<sup>1</sup> Congress has not yet acted on the administration’s change of the Department of Defense to the Department of War.

# White House Announces Cybercrime Executive Order

---

of the National Cyber Director (together, Relevant Federal Authorities), to develop an action plan that “proposes solutions to prevent, disrupt, investigate, and dismantle these TCOs.”

By May 5, 2026 (60 days from the date of issue), the Order directs the Relevant Federal Authorities to review existing regulatory frameworks and assess how each may be improved to combat TCOs engaged in cyber-enabled crime. Based on this review, the Relevant Federal Authorities are directed to submit an action plan to the president by July 4, 2026 (120 days from the date of issue). The action plan will provide for the establishment of a new “operational cell” within the Homeland Security Task Force National Coordination Center (NCC Operational Cell), a joint Federal Bureau of Investigation and Department of Homeland Security entity authorized by EO 14159 (“[Protecting the American People Against Invasion](#)”) for coordination among law enforcement, defense and intelligence community efforts to combat a range of threats, including TCOs.

**NCC Operational Cell.** The Order designates the NCC Operational Cell with responsibility for coordinating efforts to “detect, disrupt, dismantle, and deter — including by involving the private sector as appropriate” foreign TCOs and associated networks that target the U.S. The EO also requires that the action plan and the NCC Operational Cell include mechanisms to improve information sharing, operational coordination and rapid response activities across the federal government in alignment with existing law enforcement frameworks to counter foreign cyber threats. The Order further directs the secretary of homeland security, through the director of the Cybersecurity and Infrastructure Security Agency, to partner with the NCC Operational Cell to support state, local, tribal and territorial partners with “training, technical assistance, and resilience building” to expand defensive capacity, share threat intelligence and harden critical infrastructure systems against exploitation by TCOs “to the maximum extent permitted by law.”

**Private sector offense.** The EO’s action plan directs the attorney general and the secretary of homeland security, with support from the secretary of war, to describe how they will use the technical capabilities, threat intelligence and operational insights of commercial cybersecurity firms and other nonfederal entities, “consistent with applicable law,” to “enhance attribution, tracking, and disruption” of malicious threat actors and their enabling infrastructure. While the details remain limited, this element is noteworthy in explicitly calling for private actors to support “disruption” activities against malicious actors and their infrastructure.

**Victim Restoration Program.** By June 4, 2026 (90 days from the date of issue), the Order requires the attorney general to submit a recommendation to the president regarding the establishment of a Victims Restoration Program designed to provide victims of “cyber-enabled fraud schemes” with restoration or remission from funds “clawed back, forfeited, or seized” from cybercrime TCOs.

**International engagement.** The Order directs the secretary of state, in coordination with the NCC Operational Cell and U.S. allies and partners, to engage foreign governments to “demand enforcement actions” against TCOs operating within their borders and greater cooperation with U.S. law enforcement. The EO contemplates a range of consequences for nations that tolerate TCO activity, including limitations on foreign assistance, targeted sanctions, visa restrictions, trade penalties, and expulsion of foreign officials and diplomats.

## Looking Ahead

Along with the concurrently released Cyber Strategy, the EO signals that the Trump administration plans to take a more offensive-oriented approach to cybersecurity in general and cybercrime in particular, including by exploring ways to leverage private sector support in disruption actions. While the Order reflects a significant policy shift with respect to private sector engagement, details remain scarce and, as the EO notes, such operations must be “consistent with applicable law.” As noted in [our recent guidance](#) on the administration’s Cyber Strategy, latitude for private sector offense is constrained by statutes such as the Computer Fraud and Abuse Act, which broadly outlaws private sector network intrusions.

More generally, government plans for increasing private sector engagement may pressure businesses to share additional information with the government regarding their networks and operations if such data can support the administration’s law enforcement goals. Businesses may want to review third-party data sharing agreements to better understand when their information may be shared in response to government requests.

Businesses should consider monitoring the implementation of the EO, which may provide additional opportunities for government contracting and collaboration; potential access to victim support funds should the Justice Department set up a Victim Restoration Program; and, perhaps sometime soon, novel options for private sector engagement in response to a breach.

# White House Announces Cybercrime Executive Order

---

## Contacts

### **David A. Simon**

Partner / Washington, D.C.  
202.371.7120  
david.simon@skadden.com

### **Joshua Silverstein**

Counsel / Washington, D.C.  
202.371.7148  
joshua.silverstein@skadden.com

### **Matthew Urfirer**

Associate / Washington, D.C.  
202.371.7039  
matthew.urfirer@skadden.com

### **William E. Ridgway**

Partner / Chicago  
312.407.0449  
william.ridgway@skadden.com