Policy Backgrounder

Administration Allows Private Sector to Battle Foreign Cybercrime

The President issued a memorandum directing the Federal government to establish a framework for vetted US companies to support government-led cyber operations targeting foreign cyber-enabled transnational criminal organizations, including intelligence collection and disruptive activities. This Backgrounder explains the program and some associated risks for business.

Trusted Insights for What's Ahead®

- The program is limited to vetted contractors conducting individually approved operations under Federal supervision. The Departments of Justice (DOJ) and Homeland Security (DHS) would vet firms, approve missions in writing, and retain operational control.
- Approved companies would operate as Federal contractors under government supervision. They could conduct intelligence collection or disruptive operations against foreign cybercriminal organizations, with safeguards for foreign-government targets and US persons or systems.
- This builds on the Administration's broader push to scale Federal cyber capabilities through cooperation with industry. Some contractors working in the new program are likely contractors to major US businesses as well, raising concerns about potential retaliation against companies supporting US businesses in their cybersecurity efforts.
- The Memorandum does not establish a private "right to hack."
- DOJ and DHS have 60 days to define eligibility, mission approval, security, reporting, and oversight.

A Framework for Private Sector Offensive Cyber Operation

The President signed a Memorandum "Expanding Capabilities to Combat Transnational Cyber-Enabled Crime" opening the possibility of private companies potentially conducting sensitive operations on the government's behalf, raising questions about legal authority, contractor obligations, and the risks of using private firms in activities traditionally performed by Federal agencies.[1] The new program, which is voluntary, is limited to addressing foreign cyber-enabled transnational criminal organizations and excludes operations against organizations that are parts of foreign governments or wholly operated under their direction.

The program would effectively establish a government contractor model for offensive cyber operations. DOJ and DHS would vet firms, approve operations in writing, and maintain operational control. Participating companies could collect intelligence from foreign criminal networks or disrupt, degrade, manipulate, or destroy their systems and infrastructure.

The FBI has described the new memorandum as shifting away from the past ad hoc approach toward providing additional authority and capability to "empower" US industry in combating foreign cybercrime.[2] The Memorandum includes safeguards for mistaken contact with US persons or domestic systems, including requirements to stop or minimize an operation and notify the government, with additional legal authorization required for certain activities involving US persons or US-based systems.

The effort builds on a broader push to deepen government-industry cyber cooperation. A March Executive Order set up an operational cell within the National Coordination Center and called for greater use of commercial cybersecurity capabilities.[3] Supporters argue that cyberattacks are cheap to launch and expensive to defend against; using vetted commercial capabilities could help disrupt adversaries "at scale." Critics respond that using contractors in this way could blur the line between government and private cyber activity and add geopolitical risk.[4]

In addition, it remains unclear whether private contractors can conduct activities that Federal law otherwise restricts. The Computer Fraud and Abuse Act (CFAA) generally prohibits unauthorized computer access, while Section1030(f) exempts lawfully authorized investigative, protective, or intelligence activity of Federal agencies.[5] The Administration appears to be relying on the argument that contractors operating under Federal direction are carrying out a government operation, rather than exercising a new independent private "right to hack." Congress previously distinguished between public-private coordination and offensive operations by providing in the FY2022 National Defense Authorization Act that coordination with Cyber Command did not authorize private offensive cyber activity abroad.[6]

More broadly, the memorandum signals a potential change in the public-private division of responsibility for cybersecurity. While the Federal government has long relied on private expertise, this program would test whether companies can be incorporated directly into sensitive offensive missions traditionally conducted by law enforcement, military, and intelligence agencies.

The Administration sees the program as a way to address a capacity gap: US Cyber Command is primarily focused on threats from nation states and does not have the personnel to pursue the foreign cybercrime at scale, while private firms may offer greater specialized expertise and operational speed.

DOJ and DHS now have 60 days to establish eligibility, approval, reporting, security, and oversight requirements. Central questions in their framework will include attribution of the efforts, coordination with military and intelligence operations, assigning liability, exposure to violations of foreign law, and protections for participating firms and their personnel. Cybersecurity experts have warned that employees associated with offensive operations could face accusations or legal exposure abroad even when their actions are authorized by the US government.[7]

What This Means for CEOs

For most businesses, the memorandum does not offer a new cyber-defense option. A company hit by ransomware or another cyberattack is not newly authorized to penetrate or disrupt an attacker's systems. The program is limited to vetted contractors conducting individually approved operations under Federal supervision, which may also be contractors to private companies in their own provisions for cybersecurity. Companies that choose to participate in the program could also be contractors to private US businesses, making question of potential retaliation against participating firms a consideration for businesses in other industries.

For cybersecurity firms considering participation, the implications extend beyond technical capability to include questions of liability, indemnification, insurance, protection of employees, and potential retaliation. The memorandum also contemplates participation by smaller firms with specialized capabilities. The exact obligations will depend on the eventual contract structure, but cost-reimbursement contracts can require accounting systems capable of identifying and documenting contract costs, while Federal contracts impose information-security and subcontractor requirements.

About the Authors

David Young, President, The CEO Center, The Conference Board

John Gardner, Head of Public Policy & Research, The CEO Center, The Conference Board

Anthony Reyes, Senior Economic Policy Analyst, The CEO Center, The Conference Board

---

The Conference Board is the Member-driven think tank that delivers Trusted Insights for What's Ahead®. Founded in 1916. TCB.org | Learn about Membership

The CEO Center, founded in 1942 as the Committee for Economic Development, is the public policy center of The Conference Board. Members of The CEO Center are chief executive officers, key executives of leading US companies, and university Presidents. Collectively they represent 30+ industries, over 5 million employees, and more than $2T in annual revenues. The nonprofit, nonpartisan, business-led policy center delivers ***Reasoned Solutions in the Nation's Interest***™. **TCB.org/ceo-center**

Endnotes

[1] https://www.whitehouse.gov/presidential-actions/2026/08/expanding-capabilities-to-combat-transnational-cyber-enabled-crime/

[2] https://www.washingtonpost.com/national-security/2026/08/14/trump-signs-memo-authorizing-private-sector-launch-cyberattacks/

[3] https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens/

[4] https://www.washingtonpost.com/national-security/2026/08/14/trump-signs-memo-authorizing-private-sector-launch-cyberattacks/

[5] https://uscode.house.gov/view.xhtml?edition=prelim&req=granuleid%3AUSC-prelim-title18-section1030

[6] https://www.congress.gov/bill/117th-congress/senate-bill/1605/text

[7] https://techcrunch.com/2026/08/13/in-a-first-us-will-allow-some-private-firms-to-carry-out-cyberattacks/