Cooley

New Federal Program Deputizes Private Companies to 'Hack Back'

September 1, 2026

On August 12, 2026, President Donald Trump signed a memorandum titled "Expanding Capabilities to Combat Transnational Cyber-Enabled Crime" (memorandum). Historically, private companies have faced the imperative to defend themselves against cybercriminals while being legally barred from fighting back or "hacking back" – also known as active defense or active cyber response (ACR). The concept of ACR stems from a situation where participants in the program respond on behalf of victims of hacking by launching various offensive counterattacks against the hacker, with the intent of mitigating the effects of the attack. Business, scholars and politicians alike have debated this historical prohibition on "hacking back," arguing over the limits on the tools available to the private sector to defend itself when it holds the vast majority of the world's online infrastructure.

The memorandum directs the federal government to authorize vetted private companies to conduct offensive cyber operations, including surveillance and disruptive effects operations under federal oversight, against suspected foreign criminal hacking groups. For cybersecurity firms, threat intelligence providers and defense contractors, this memorandum potentially opens up new lines of activity and opportunity, but not without potential risk and exposure.

What the memorandum enables

The memorandum directs the National Coordination Center (NCC) to create and manage a program that would authorize certain preapproved "Participating Companies" to conduct cyber surveillance operations and cyber effects operations, under federal control and oversight, against foreign cyber-enabled transnational criminal organizations.

- A **cyber surveillance operation** means accessing another organization's computer systems or networks, without authorization from the owner or operator or by exceeding authorized access, primarily to passively collect information or intelligence, including information that could support a future cyber effects operation, with the intent to remain undetected.
- A **cyber effects operation** means an operation that actually manipulates, disrupts, denies, degrades or destroys another organization's information systems, networks or data, going beyond mere observation.

The program will be overseen jointly by the Department of Justice (DOJ) and the Department of Homeland Security (DHS), which must coordinate with each other to approve any operation, and every resulting action must be conducted on behalf of, and under the supervision of, these agencies.

The opportunity: a new kind of government relationship

For companies that provide offensive or clandestine cyber capabilities, this program provides a potential opportunity to become a partner to the US government. Participating companies would enter into contractual agreements with DOJ or DHS.

The memorandum also directs the government to build out the terms of this relationship over the coming months. By October 11, 2026, the program's executive directors must establish operating procedures, including minimum standards for participation covering technical proficiency, proven performance, facility security, personnel vetting, competence and reliability. In establishing these procedures and standards, the executive directions must ensure eligibility criteria that allows for participation by both large companies, which would provide capacity and volume, and smaller or more specialized companies, which would potentially be better suited to more discrete tasks.

The guardrails: federal oversight

The memorandum builds in several layers of federal oversight, including requiring:

- Individual approval of each operation by the program's executive directors.
- Participating Companies halt operations that stray outside of the approved scope and notify the NCC.
- Participating Companies to maintain a bond or escrow of at least $1 million, to be forfeited if the company falls out of compliance with its contractual agreement.
- Annual evaluation of Participating Companies for continued participation in the program.

The risk: residual liability

The harder question for any company considering this program is what happens when something goes wrong, and the memorandum signals that the government is also conscious of potential risks.

Authorized operations can have unexpected results

If a Participating Company discovers that an authorized operation has exceeded its approved parameters, such as by unintentionally targeting a US person, a US-based information system or a system controlled by a US person, it must immediately stop the operation, take steps to minimize the impact and notify the NCC, which then notifies the DOJ. Companies must also immediately report any imminent attack on US critical infrastructure they discover, or any reasonable belief that an approved operation may result in loss of life or serious injury, or rise to the level of use of force or armed attack under international law. The fact that the memorandum specifically anticipates and requires reporting on scenarios this serious is a signal of just how much can go sideways, even with rigorous vetting and federal sign-off.

Anti-hacking laws at home and abroad

The Computer Fraud and Abuse Act (CFAA) is an avenue for exposure, as it bars cyber activity undertaken without authorization or that exceeds authorized access – the very activity this memorandum enables. Anyone who suffers damage or loss from a violation of the CFAA may sue the violator for damages and equitable relief.

It is unclear whether this private right of action would survive against a defendant acting as a Participating Company under the program. The memorandum references compliance with the CFAA, alluding to an exemption for "any lawfully authorized investigative, protective or intelligence activity of a law enforcement agency of the United States [and certain other government entities]."[1] But it's unclear the extent to which the exemption can apply to the actions of private entities undertaken on behalf of the government. This uncertainty means that a Participating Company could find itself exposed to a civil suit from whoever was harmed, having to litigate the exemption's scope.

Foreign law adds another layer that the memorandum does not seek to address or resolve. These operations are meant to target servers, networks and infrastructure located outside the United States, and most countries have their own computer crime statutes that make unauthorized access to a computer system a domestic offense wherever it originates. A US government contract does not extend to a foreign hacking law and does not confer immunity from prosecution or civil suit in that country. A Participating Company conducting an approved operation against infrastructure or targets sitting in a foreign jurisdiction could still face criminal or civil exposure under that jurisdiction's own laws.

No new swords or shields

Federal oversight also does not mean federal immunity for a company that steps outside the lines. The memorandum expressly caveats that it does not create any right or benefit, procedural or substantive, that any party can enforce against the United States or its officers and employees. That language lays out the government's position that a Participating Company cannot point to this memorandum as a federal government indemnity for claims brought against the company, and a private party harmed by an operation gone wrong has no new claim against the government created by this memorandum.

Who else should be paying attention

This is not only a story for companies that might apply to the program. Cloud and hosting providers, internet service providers and critical infrastructure operators have reason to watch closely too, because these operations could touch their infrastructure without warning. A hosting provider or network operator whose infrastructure sits between a Participating Company and its intended target may lack visibility into an authorized operation running through its systems until something breaks.

The program also contemplates Participating Companies entering into commercial agreements with other private sector entities to receive threat intelligence in support of their cyber operations. Managed security service providers and incident response firms should also take note, even if they never seek Participating Company status themselves. However, such entities also run the risk of identifying operations by Participating Companies when responding to incidents at foreign entities, which may present conflicts of interest between their incident response and threat intelligence services.

Before entering into any threat intelligence sharing arrangement with a Participating Company, a company should understand exactly how its data and its name could end up feeding into a federally authorized cyber operation, and what obligations or exposure that creates for the company supplying the intelligence, not just the company acting on it.

Looking ahead

The program's operating procedures are not due until October, so the details of eligibility, vetting and contract terms are still being written. But companies in the defense industrial base, cybersecurity, and cyber operations, threat intelligence and managed security spaces should start thinking now about:

- Whether becoming a Participating Company, or a commercial data partner to one, fits the company's risk tolerance and business strategy.
- What contractual protections, insurance and indemnification the company would need before agreeing to conduct operations under this kind of federal authorization.
- Developing a legal strategy and assessing potential exposure under the CFAA and other anti-hacking laws (including outside of the US).
- Preparedness for inadvertent or intentional retaliation or escalation from targets of cyber operations conducted under the program.
- Whether the company's infrastructure or client base could be swept into someone else's authorized operation, even without any direct involvement in the program.

This memorandum marks a shift in how the government defines the private sector's role in the fight against cybercrime. Companies in this space have an opportunity to contribute to the disruption of cyber-enabled transnational criminal organizations, but the legal exposure runs alongside the opportunity, not behind it. If you have questions about whether your company should participate in this program, how to structure a commercial data-sharing arrangement tied to it or how to manage the liability that comes with operating in this space, please contact the Cooley cyber/data/privacy practice.

Notes

1. 18 USC § 1030(f).

assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Emma Plankey Boston	eplankey@cooley.com +1 617 937 1349
Mari Dugas New York	mdugas@cooley.com +1 202 740 0747