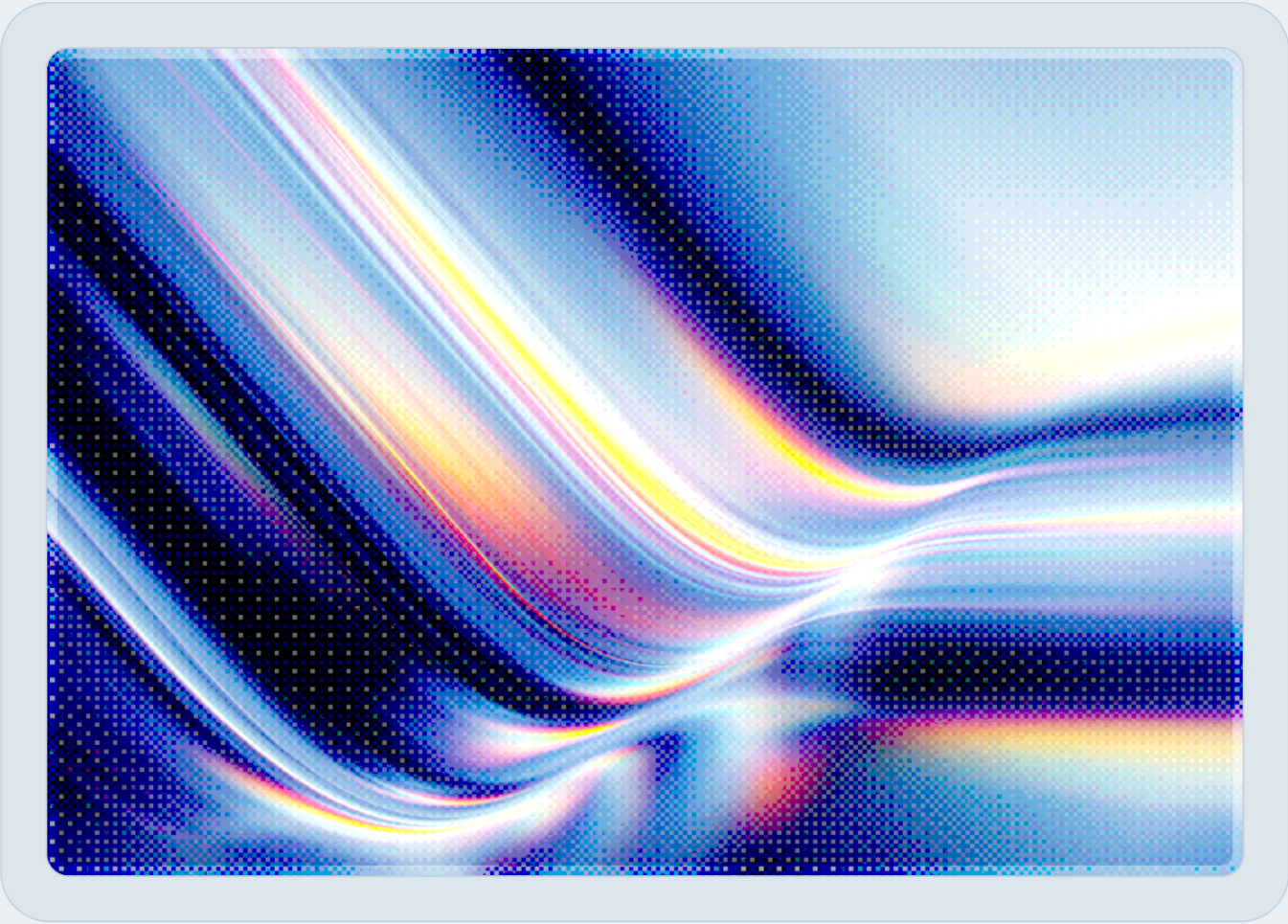
CSAI Foundation | Cloud Security Alliance

Cyber Privateers: What the New Hack-Back Program Means for Enterprises

2026-08-14

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- On August 12, 2026, President Trump signed a National Security Presidential Memorandum (NSPM) directing the Homeland Security Task Force's National Coordination Center (NCC) to authorize vetted "Participating Companies" to conduct offensive cyber surveillance and effects operations against foreign transnational criminal organizations (TCOs), under federal direction, control, and authority [1][3].
- The program is, by most contemporaneous reporting, the first formal U.S. mechanism permitting private firms to conduct government-sanctioned hack-back operations [3][6], a departure from a decade of failed legislative attempts such as the Active Cyber Defense Certainty Act [11].
- Participating companies must be vetted, obtain written per-operation approval from DOJ and DHS officials, and are barred from actions that cause loss of life or rise to the level of "use of force" under international law; violations can trigger forfeiture of a required financial penalty bond [2][3][6].
- The NSPM rests on an interpretive reading of Computer Fraud and Abuse Act (CFAA) §1030(f) that has never been tested in court; if a court later rejects the theory that the statute's law-enforcement exception extends to private delegatees, participating firms could face retroactive civil and criminal exposure [7][9].
- Enterprises that are not themselves seeking to participate still face exposure: threat intelligence shared with government-linked programs may be repurposed for offensive operations, and misattributed targeting or retaliation against a participating firm's infrastructure could create collateral, cross-border incident response burdens for unrelated organizations [8].

Background

For nearly a decade, the debate over private-sector "hacking back" in the United States has been a legislative dead end. The Active Cyber Defense Certainty Act, first introduced by Representatives Tom Graves and Kyrsten Sinema in 2017, sought to amend the CFAA to let victim organizations pursue intruders beyond their own network boundaries, including to identify attackers, recover or destroy stolen data, and deploy "beaconing" technology to trace physical locations [11]. Graves and Representative

Josh Gottheimer reintroduced a similar version in the 116th Congress in 2019 [12]. Neither version advanced past committee, and mainstream security practitioners, including researchers at Rapid7 and civil society groups such as the Center for Democracy and Technology, warned, in their assessment, that the underlying technical problems, misattribution, shared and compromised infrastructure, and the risk of "victimizing the victim" when countermeasures are routed through innocent third parties such as hospitals, made legalized retaliation more dangerous than restrained defense [9][10].

The NSPM signed on August 12, 2026, sidesteps that legislative stalemate entirely. Rather than amending the CFAA through Congress, the memorandum directs the NCC, housed within the Homeland Security Task Force, to stand up a program under which DOJ and DHS jointly vet, contract with, and issue written per-operation approvals to private companies willing to conduct what the memorandum terms Cyber Surveillance Operations and Cyber Effects Operations against foreign TCOs [1][3][6]. The stated justification is scale: the administration's fact sheet cites the FBI Internet Crime Complaint Center's 2025 tally of $20.8 billion in reported losses to cyber-enabled fraud, ransomware, phishing, sextortion, and impersonation scams targeting Americans as evidence that existing law enforcement capacity cannot keep pace with transnational scam networks operating from jurisdictions such as parts of Southeast Asia that shelter forced-labor scam compounds [1][2].

Under the program's structure, the government retains formal command authority. Executive directors from DOJ and DHS must review every proposed operations package and issue written approval before a Participating Company acts, and firms must immediately halt any operation that exceeds its approved scope and report the deviation [1][3][6]. The memorandum explicitly excludes operations that could cause loss of life or that would constitute a "use of force" or "armed attack" under international law, and it requires companies to post a financial penalty, reported at a $1 million minimum, that can be forfeited for non-compliance [2][6]. The program is designed to be open to companies of varying size, not solely large federal contractors, and Homeland Security officials have framed vetting criteria around demonstrated technical proficiency rather than incumbency [2][3].

Reaction from the security and policy community has split along familiar lines. Cybersecurity veteran Chris Wysopal called the memorandum "a pretty big shift in US cyber policy," while noting it stops short of the fully unrestrained hack-back regime some earlier legislative proposals envisioned [3]. Others were sharper: former U.S. Cyber Command officer Andrew Schoka warned that the program risks producing "cyber privateers running around without any clear coordination or direction at the federal level," pointing out that deconfliction of offensive operations is already difficult among federal agencies alone, and that adding private firms with independent capability and speed compounds the problem [4]. Jason Kikta, former leader of the Cyber National Mission Force and now chief technology officer at Automox, was blunter still, describing the program as "a perpetual motion machine for billable threats" [2].

Representative Bennie Thompson, ranking member on the House Homeland Security Committee, said the oversight procedures remain unclear and argued that a program of this consequence warrants congressional authorization rather than reliance on a presidential memorandum alone [5].

Security Analysis

The NSPM's legal architecture is arguably its most fragile feature: it rests on an untested legal theory rather than a statutory change. Rather than amending the CFAA through Congress, the memorandum relies on an interpretive argument that §1030(f), which exempts "lawfully authorized investigative, protective, or intelligence activity" of a government agency from the statute's prohibitions, can be extended to private companies acting as delegated agents of DOJ and DHS under the program's written approvals [7][9]. That theory has never been adjudicated. If a court later declines to read §1030(f) as covering private delegatees, in litigation brought by a misattributed target, a foreign government, or a defendant in an unrelated criminal matter, participating companies could find that their per-operation government approval provided no durable legal shield, exposing them to the same civil and criminal CFAA penalties the program was designed to route around [7][9]. Because the interpretive theory is novel and untested, firms that acted under it during the program's early phase could face retroactive exposure even after having followed every procedural requirement the NCC laid out.

Attribution is the technical problem that critics have consistently pointed to as the reason prior hack-back proposals failed, and nothing in the NSPM's structure resolves it directly [9][10]. Transnational scam and ransomware infrastructure is frequently hosted on compromised servers belonging to unrelated third parties, including hospitals, small businesses, and cloud tenants who have no connection to the criminal operation routed through their systems [9]. Pareekh Jain of Pareekh Consulting noted that avoiding collateral damage under these conditions is extremely difficult precisely because criminal groups deliberately obscure their infrastructure within legitimate networks [8]. A disruptive "cyber effects operation" that misidentifies a target, or that degrades shared infrastructure incidental to a legitimate target, could cause harm to organizations that were never party to the underlying criminal scheme and that have no visibility into, or recourse against, the operation that affected them. Unlike government agencies conducting similar operations, participating private companies carry none of the sovereign immunity or diplomatic protections that historically constrained the consequences of state-directed offensive action, which means retaliation against a participating firm's own infrastructure, or against its employees, is a live risk with no clear mitigation built into the program [4][8].

For the broader enterprise population that will not seek to become Participating Companies, the more immediate exposure runs through data and infrastructure they already control. CISOs and threat intelligence teams that share indicators, telemetry, or incident data with government-linked information-

sharing channels should recognize that this data may now feed into proposals for offensive operations rather than remaining purely defensive, a shift Counterpoint Research's Neil Shah flagged directly, cautioning that "enterprise CISOs should be careful before feeding telemetry into these programs" [8]. Existing data-sharing agreements, customer contracts, and privacy commitments were typically negotiated against the assumption that shared threat data would be used defensively; enterprises should not assume those agreements implicitly cover contribution to attributable offensive action. There is also a second-order market effect worth watching: Jonathan Ong of Omdia has questioned whether large, brand-sensitive vendors will participate at all, given the reputational exposure relative to the commercial upside of privileged threat access [8]. If that reluctance holds, participation could skew toward smaller firms with fewer resources to absorb the associated liability and oversight burden, a possibility CSA raises here as an extrapolation from Ong's point rather than as something he stated directly.

Recommendations

Immediate Actions

Enterprises should treat this as a governance and contract-review event, not a technical one. Legal and privacy teams should audit existing threat-intelligence sharing agreements, ISAC/ISAO memberships, and vendor data-sharing clauses to determine whether shared telemetry could legally be repurposed by a recipient organization for offensive operations under the new program, and should amend agreements where that use was not contemplated. Security leadership should inventory any existing vendor relationships with companies known to be pursuing NCC vetting, since a vendor's participation in offensive operations introduces a new category of third-party and reputational risk that standard vendor risk assessments do not currently capture.

Short-Term Mitigations

Organizations should update incident response and business continuity plans to account for the possibility of retaliatory or collateral cyber activity connected to a Participating Company's operations, even where the organization itself has no relationship to the program. This includes reviewing whether shared or leased infrastructure, cloud tenancy, or upstream service providers could be incidentally implicated in either side of a future offensive-defensive exchange. Enterprises should also monitor NCC vetting criteria and reporting requirements as they are published, since the scope of "Cyber Surveillance Operations" and "Cyber Effects Operations" remains loosely defined in public materials and will likely be clarified through implementing guidance over the coming months [1][6].

Strategic Considerations

Boards and risk committees should recognize that this program introduces a durable, structural shift in the U.S. cyber policy environment rather than a one-time event. Enterprises operating internationally should evaluate whether the program's cross-border implications, particularly the risk that a foreign government could conflate a Participating Company's operation with tacit U.S. government action against it, create new geopolitical risk factors relevant to operations, personnel, or data residency in affected regions. Given that the underlying legal theory is untested, organizations with existing relationships to companies pursuing NCC status should also plan for the possibility that congressional or judicial action could unwind or substantially narrow the program, and should avoid structuring long-term commercial dependencies on the assumption that its current legal footing is stable.

CSA Resource Alignment

This event sits at the intersection of national cyber policy shifts and enterprise governance, an intersection CSA has tracked closely through its rapid-response analyses of the current administration's cybersecurity executive actions. CSA's review of the June 2026 AI cybersecurity executive order flagged a governance pattern that applies directly here: voluntary federal frameworks that lack reusable, independently assessable controls and a repeatable audit method tend to leave enterprises interpreting ambiguous, discretionary guidance largely on their own, with alignment across the ecosystem, rather than sheer capacity, emerging as the decisive challenge [13]. The hack-back program raises a comparable governance problem. It, too, rests on a non-legislative federal posture, discretionary vetting, and per-operation approval rather than settled statute, and it carries direct implications for how enterprises structure data-sharing agreements and manage third-party risk.

The offense/defense capability imbalance underlying this policy shift has also been quantified directly, if not by CSA itself. The UK's AI Security Institute (AISI) has found that AI models' cyber task-completion capability has been doubling roughly every 4.7 months since late 2024, a pace that outstrips typical enterprise patch and remediation cycles [14]. The same asymmetry underlies the administration's stated rationale for this program: that traditional law enforcement cannot keep pace with technically sophisticated, fast-moving transnational criminal infrastructure. Enterprises should read the two developments together: private offensive authorization is, in part, a policy response to a capability gap that independent researchers have already measured.

Finally, the governance questions raised by this program, third-party risk from vendors pursuing government authorization, data-sharing agreements that may be repurposed beyond their original defensive intent, and incident response planning for retaliatory or collateral cyber activity, map onto

several control domains within the AI Controls Matrix (AICM) v1.1 covering supply chain and third-party risk, incident response, and identity and access management, even though this specific program is not itself an AI-driven initiative [15]. Enterprises reassessing vendor and data-sharing governance in light of this NSPM can apply the same AICM-aligned controls process CSA recommends for AI supply chain risk to evaluate exposure introduced by vendors participating in government-sanctioned offensive cyber programs.

References

[1] The White House. "Fact Sheet: President Donald J. Trump Expands Capabilities to Combat Transnational Cyber-Enabled Crime." The White House, August 12, 2026.

[2] BleepingComputer. "White House Taps Security Firms for Offensive Hack-Back Operations." BleepingComputer, August 2026.

[3] CyberScoop. "Trump Turns to Private Sector in Offensive Hacking Operations Memo." CyberScoop, August 13, 2026.

[4] CNN. "'Cyber Privateers': Trump Issues Order Allowing US Companies to Hack Overseas Groups Under Certain Conditions." CNN Politics, August 13, 2026.

[5] The Record from Recorded Future News. "Trump Taps Cyber Firms to Go on Offensive Against Criminals." The Record, August 2026.

[6] The Register. "Trump Wants to Grant Private Cyber Firms a License to Hack Back." The Register, August 13, 2026.

[7] Tech Times. "Trump Authorizes Private Firms to Hack Foreign Criminals; Legal Basis Untested by Courts." Tech Times, August 13, 2026.

[8] CSO Online. "Trump Administration Opens Door to Private-Sector Cyber Offensives." CSO Online, August 2026.

[9] Center for Democracy and Technology. "Private Sector Hack-Backs and the Law of Unintended Consequences." CDT, 2026.

[10] Rapid7. "Cyber Hack Back Is Still Wack." Rapid7 Blog, August 2021.

[11] Just Security. "Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act." Just Security, November 2017.

[12] Library of Congress. "H.R.3270 - Active Cyber Defense Certainty Act, 116th Congress (2019-2020)." Congress.gov, 2019.

[13] Cloud Security Alliance. "The Presidential AI Executive Order and Industry Alignment." CSA AI Safety Initiative, June 2026.

[14] AI Security Institute (AISI), UK Department for Science, Innovation and Technology. "How Fast Is Autonomous AI Cyber Capability Advancing?." AISI, February 2026.

[15] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, 2026.