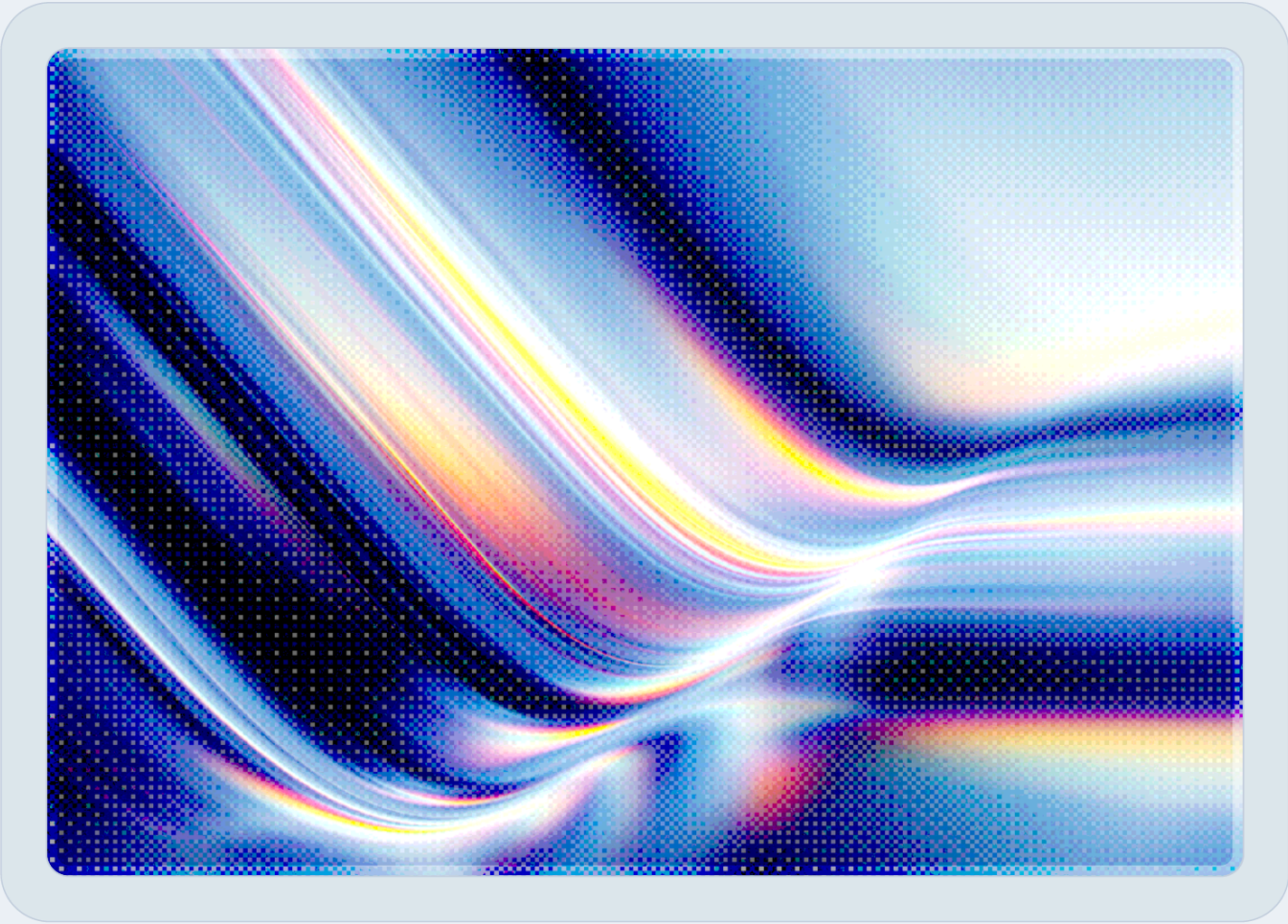
CSAI Foundation | Cloud Security Alliance

Cyber Privateers: Enterprise Risk After Trump's Offensive-Cyber Memo

2026-08-23

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

On August 12, 2026, President Trump signed a National Security Presidential Memorandum (NSPM), "Expanding Capabilities to Combat Transnational Cyber-Enabled Crime," directing the Department of Justice and Department of Homeland Security to stand up a program under which vetted private companies can conduct government-approved offensive cyber operations against foreign criminal groups [1][2][12]. The memo does not authorize independent "hack back" activity; every operation requires written, per-engagement approval from co-executive directors at DOJ and DHS, and participating firms must post a bond of at least $1 million that is forfeited for rule violations [1][3]. Legal analysts who have reviewed the memo's text note that it contains no indemnification provisions and leans on a 40-year-old Computer Fraud and Abuse Act exemption for government agents that has never been tested in court as applied to private contractors [4][5][6]. Enterprises face liability exposure whether or not they participate: prospective "Participating Companies" must weigh CFAA risk, foreign-law exposure, and insurance coverage gaps before signing on, while non-participating cloud providers, network operators, and critical infrastructure owners whose systems intersect with an approved operation currently have no clear legal protection of their own [5][6]. The Department of Justice and Department of Homeland Security have 60 days from the memo's signing — until roughly October 11, 2026 — to publish the operating procedures, vetting standards, and bonding details that will determine how much of this risk actually materializes [1][6].

Background

The NSPM arrives against a backdrop of rising, well-documented losses from cyber-enabled fraud rather than the inflated headline figures that have circulated in other policy debates. The White House's own justification for the memo cites $20.8 billion in cyber-enabled crime losses reported by Americans in 2025, up from roughly $12.5 billion when a related executive order was signed earlier in the year, with ransomware, phishing, financial fraud, sextortion, and impersonation scams named as the primary drivers [7][2]. That trajectory — a roughly two-thirds increase in reported losses in a single year — is the administration's core argument for why existing law enforcement capacity, concentrated in the FBI and a handful of federal partners, cannot keep pace with transnational criminal groups operating from jurisdictions where extradition and mutual legal assistance are difficult or unavailable [2][8].

The memo directs the National Coordination Center (NCC) to build a formal program, jointly overseen by DOJ- and DHS-appointed Program Executive Directors, that can contract with "vetted United States companies" to conduct two categories of activity against foreign Cyber-Enabled Transnational Criminal Organizations (CE-TCOs) [1][9]. Cyber Surveillance Operations are aimed at covertly collecting intelligence on a target group's infrastructure and operations, including "manipulation or temporary disruption" incidental to that collection, provided it is not intended to produce physical effects [9]. Cyber Effects Operations go further, authorizing manipulation, disruption, denial, degradation, or destruction of an adversary's systems or the information on them [9]. Both categories are explicitly bounded: the memo prohibits any operation that would cause loss of life, serious injury, or an outcome that would constitute an armed attack under international law, and it requires companies to halt immediately and notify the government if an operation inadvertently touches a U.S. person or system [1][3].

Other coverage has framed this as a revival of eighteenth-century "letters of marque and reprisal," a comparison that makes for a memorable headline but understates the degree of federal control the memo actually imposes. Privateers operating under historical letters of marque are generally understood to have held substantial independence once commissioned; this program does the opposite, requiring standing government control, written pre-approval of each operation, and continuous deconfliction with the State Department, Treasury, the Defense Department, DOJ, and the intelligence community before and during execution [3][6]. Chris Wysopal, co-founder of Veracode, described it as "a pretty big shift in U.S. cyber policy" that nonetheless "stops short" of the broader, unsupervised hack-back proposals that have circulated in Congress for years, including legislation invoking the constitutional letters-of-marque power directly [1]. That distinction matters for enterprise risk: this is a government-directed contracting program with extensive federal control, not a green light for companies to retaliate against attackers on their own initiative, and organizations that conflate the two may misjudge both their exposure and their options.

Security Analysis

The central legal uncertainty in the memo is one of statutory authority applied in a novel way. The NSPM frames all authorized activity as occurring "as part of lawful investigatory, protective, or intelligence operations carried out by Federal law enforcement," language drawn from 18 U.S.C. § 1030(f), the Computer Fraud and Abuse Act's carve-out for government agents [4][6]. That exemption has existed since the CFAA's original passage but has never been interpreted by an appellate court to extend liability protection to a private company acting as a government contractor rather than a government employee [4]. Wiley's analysis of the memo text found that Section 2's delegation of approval authority to the Program Executive Directors leaves ambiguous whether a Participating Company itself executes an operation or merely supports one that is technically conducted by government personnel — a distinction

that materially affects liability exposure in ways the memo does not resolve [6]. Wiley's alert goes on to advise that companies should carefully consider whether their participation agreements adequately address indemnification, a recommendation consistent with the memo's published text containing no indemnification provisions of its own; that gap would leave companies acting, in effect, as government agents without any contractual promise that the government will defend them or assume liability if an operation is later challenged [6].

That gap compounds a set of overlapping exposure categories that enterprise legal and risk teams will need to evaluate independently of whether the underlying operation was properly authorized. Attorney Lyn Brown, quoted in coverage of the memo, said the forthcoming contractual agreements between DOJ, DHS, and participating firms will be "key," and that firms will likely seek "liability protection or indemnification" as a condition of participation — protection the memo's text does not currently promise [3]. Tonya Ugoretz, a former FBI and DHS cyber official, said CFAA exposure "will be front and center as companies decide whether and how much they want to participate" [3]. Beyond U.S. federal law, operations against foreign infrastructure risk running afoul of the target country's own computer-crime statutes — the U.K.'s Computer Misuse Act and comparable statutes elsewhere do not recognize a U.S. government-contractor exemption — which means a company's legal exposure does not stop at the U.S. border even when it is operating exactly as instructed by its NCC contract [4].

Insurance is a second, related gap, and one this note infers from first principles rather than from law-firm commentary: standard cyber liability and technology errors-and-omissions policies are underwritten around the assumption that the policyholder is a victim of an attack, not an active participant in offensive operations, and existing coverage is unlikely to extend to government-directed offensive activity absent a specific endorsement. This concern echoes a broader dynamic CSA has already documented in the 2026 cyber insurance market: carriers have moved decisively away from ambiguous, "silent" coverage of AI- and technology-related exposures toward express inclusion or express exclusion, and a company entering this program without first confirming how its carrier treats government-contracted offensive cyber activity risks discovering a coverage gap only after an incident, at the point where it is most expensive to learn about [10]. The $1 million bond requirement in the memo can be read as a partial substitute for insurance from the government's perspective, giving DOJ and DHS a pool of forfeitable capital tied to "non-compliance" — a term the memo does not define, leaving its scope to the operating procedures due within 60 days [1][6].

A third, less-discussed exposure category falls on companies that never sign up for the program at all. Wiley's review notes that cloud providers, network operators, and other infrastructure owners whose systems happen to host or transit CE-TCO activity may find government-supervised operations touching their environment without their direct consent, and that "protections under this program are essential" for these third parties precisely because the memo, as written, does not clearly extend any to them [6]. Deconfliction failures are a live concern here: Gary Corn, a former U.S. Cyber Command

official, has warned that coordinating private-sector operations with classified government activity will be "exponentially more challenging" than coordinating among cleared government operators alone, raising the odds that an approved private operation collides with an unrelated government or allied action on the same infrastructure [5]. Columbia University's Erica Lonergan has raised parallel concerns about vetting rigor, goal-setting, and the risk that loosely scoped targeting could edge into operations against nation-state-affiliated actors rather than the criminal groups the memo is nominally aimed at [5]. Former DHS official Paul Rosenzweig was blunter still, calling the approach "a bad idea" and arguing there are "much better ways to revive what it seems to me is an essentially governmental function" than deputizing private companies to perform it [5].

Recommendations

Immediate Actions

Enterprises that are considering participation, and those that are not but could be affected as third parties, should have general counsel review the NSPM's public text now, rather than waiting for the DOJ/DHS operating procedures due by roughly October 11, 2026, so that internal risk committees are not evaluating an unfamiliar legal framework under time pressure once the program opens for applications [1][6]. Risk and legal teams should specifically ask their cyber liability and technology E&O carriers, in writing, whether existing policies would respond to a claim arising from government-directed offensive cyber activity, since the honest answer at most carriers today is likely to be "unclear," and getting that in writing now creates a paper trail useful for coverage negotiation later [6][10]. Companies that operate cloud, hosting, or network infrastructure that criminal groups are known or suspected to use should also confirm, through counsel, what recourse they would have if a government-supervised operation touches their environment without prior notice, given that the memo does not currently spell out third-party protections [6].

Short-Term Mitigations

Organizations evaluating formal participation should treat the contractual negotiation with DOJ and DHS as the primary — and possibly only — opportunity to secure indemnification, litigation support, and clearly allocated liability for operations that exceed approved parameters, since the memo's text leaves all of this to be resolved contract-by-contract rather than by statute [3][6]. Given that written approval from two Program Executive Directors is required before any operation and that "non-compliance" triggering bond forfeiture is currently undefined, participating firms should push for the operating procedures to specify objective compliance criteria rather than accepting open-ended discretionary

language, and should build internal documentation practices now that can demonstrate adherence to whatever approval workflow the government ultimately publishes [1][6]. Firms should also assume that deconfliction gaps are a realistic operational risk rather than a remote one, given informed former-official commentary to that effect, and should build technical safeguards — geofencing, target-scope validation, and hard stops tied to the approved operation's written parameters — that reduce the odds of an unintended collision with unrelated government or third-party activity on the same infrastructure [5].

Strategic Considerations

Security and risk leaders should recognize that this program, however it ultimately performs, is a leading indicator of a broader policy direction: shifting some portion of offensive cyber response capacity from purely governmental hands toward vetted private actors operating under contract. Enterprises with mature threat-intelligence and incident-response capabilities may eventually see this program as a revenue or capability-building opportunity, but should weigh that opportunity against the CFAA, foreign-law, insurance, and reputational exposure documented above, and should not assume that early participation carries a first-mover advantage that outweighs those risks before the operating procedures are public. Boards and audit committees at any company weighing participation should treat this as a material strategic decision warranting the same governance rigor applied to other high-risk business lines, including explicit sign-off on the company's risk tolerance for operating in a legal space that, by outside legal analysts' own description, remains genuinely untested in court [4][6].

CSA Resource Alignment

The clearest connection to CSA's existing research base is on the insurance and risk-transfer side. CSA's AI Breach Velocity and the 2026 Cyber Insurance Reckoning documents how the cyber insurance market has moved from ambiguous "silent" coverage toward express inclusion or exclusion of emerging exposures, and its recommendation that enterprises proactively map their coverage against novel risk categories before a claim arises applies directly to the government-directed-offensive-operations gap identified in this note; companies evaluating participation in the NCC program should treat that policy-review exercise as a prerequisite, not a formality [10].

CSA's Trump's AI Cybersecurity Order: Voluntary Review, Enterprise Implications analyzed a separate June 2026 executive action that also created a voluntary federal program built on incomplete public detail, with substantive requirements deferred to a forthcoming rulemaking process. Its core

methodological lesson — that enterprises should track a phased, time-bound federal framework through named milestones rather than react only once final procedures are published — applies equally to the 60-day operating-procedures deadline this NSPM establishes.

CSA's Best Practices for Cyber Incident Exchange provides relevant guidance on structuring information-sharing and coordination relationships between private organizations and government or industry partners, which is directly applicable to the deconfliction and mandatory-reporting obligations this program imposes on participating companies.

Where these artifacts do not reach a specific control area, the AI Controls Matrix (AICM v1.1) offers the underlying governance baseline enterprises can use to structure the internal decision, particularly its domains covering legal and compliance risk, third-party and supply chain risk, and incident response, each of which maps to the participation-decision, contractual, and deconfliction risks this note identifies [11].

References

[1] CyberScoop. "Trump turns to private sector in offensive hacking operations memo." CyberScoop, August 2026.

[2] CNN. "'Cyber privateers': Trump issues order allowing US companies to hack overseas groups under certain conditions." CNN, August 13, 2026.

[3] Federal News Network. "Trump's move to 'unleash' private sector hackers raises novel oversight, liability questions." Federal News Network, August 2026.

[4] Lawfare. "Cybersecurity & Tech: Trump Admin Cyber Strategy Centers Private Sector in Offensive Cyber Operations." Lawfare, 2026.

[5] CyberSecurity Dive. "US government will let private companies hack criminal gangs." CyberSecurity Dive, August 13, 2026.

[6] Wiley Rein LLP. "Navigating the New Presidential Memorandum on Transnational Cyber-Enabled Crime." Wiley, August 2026.

[7] Decrypt. "White House Lets Private Firms Hack Cybercriminals—At Their Own Legal Risk." Decrypt, August 2026.

[8] NPR. "Trump administration wants to allow companies to hack foreign cybercriminals." NPR, August 15, 2026.

[9] Mayer Brown. "Presidential Memorandum Authorizes Vetted Private Companies to Conduct Offensive Cyber Operations Against Foreign Criminal Organizations." Mayer Brown, August 2026.

[10] Cloud Security Alliance. "AI Breach Velocity and the 2026 Cyber Insurance Reckoning." Cloud Security Alliance, June 21, 2026.

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

[12] Washington Post. "Trump signs memo authorizing private sector to launch cyberattacks." Washington Post, August 14, 2026.