ZEROFOX INTELLIGENCE

Flash

U.S. Private Companies to Conduct Cyberattacks

F-2026-08-20a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Ransomware, Cybercrime

August 20, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on August 20, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | U.S. Private Companies to Conduct Cyberattacks

| Key Findings

- On August 12, 2026, U.S. President Donald Trump signed a National Security Presidential Memorandum (NSPM) directing the National Coordination Center (NCC) to develop a program authorizing vetted U.S. companies to conduct cyber surveillance and disruption operations against foreign Cyber-Enabled Transnational Criminal Organizations (CE-TCOs).
- The NSPM authorizes two activities that 18 U.S.C. § 1030 had previously not allowed for commercial actors: Cyber Surveillance Operations (covering clandestine collection from adversary systems) and Cyber Effects Operations (covering disruption, degradation, or destruction). Operating procedures and participation standards are due by mid-October.
- ZeroFox assesses that criminal groups are likely to develop defensive adaptations in response to adversary capabilities that combine U.S. commercial engineering speed with federal legal cover rather than be deterred by them.
- ZeroFox assesses with moderate confidence that the program will almost certainly proceed. However, it is likely that the October deadline will yield interim rather than complete procedures and that first-cohort vetting will run into 2027,

given that the NSPM did not provide details regarding how the NCC should implement the program.

Overview

On August 12, 2026, President Trump signed an NSPM directing the NCC to develop a program authorizing vetted U.S. companies to conduct cyber surveillance and disruption operations against foreign CE-TCOs.[1] It is the first formal U.S. mechanism placing offensive cyber capabilities into commercial hands under federal directive. ZeroFox assesses this very likely marks a durable change in how ransomware and fraud infrastructure is disrupted, though operational shifts will likely not occur until implementation procedures land in October.

- **Who runs it?** The NCC, hosted within the Homeland Security Task Force. Co-Executive Directors from the Department of Justice (DOJ) and Department of Homeland Security (DHS) must jointly approve every operational package in writing before action.
- **Who acts?** Vetted U.S. firms under contract to DOJ or DHS that post a bond of not less than USD 1 million, forfeitable on noncompliance.
- **Who can be targeted?** Foreign criminal groups only. The memorandum excludes any group that is an institutional part of a foreign government or wholly operated under its direction, placing nation-state actors outside the remit.
- **Hard limits:** Nothing likely to cause loss of life or to rise to use of force under international law. Operations must halt and minimize contact with a U.S. person or a U.S.-based system.
- **Timeline:** Operating procedures and participation standards due on or about October 11, 2026; first program status report due by February 8, 2027.

[1] hXXps://www.whitehouse[.]gov/fact-sheets/2026/08/fact-sheet-president-donald-j-trump-expands-capabilities-to-combat-transnational-cyber-enabled-crime/

Details

The NSPM authorizes two activity types that 18 U.S.C. § 1030 had not previously allowed for commercial actors: Cyber Surveillance Operations (covering clandestine collection from adversary systems) and Cyber Effects Operations (covering disruption, degradation, or destruction). The structure is a chain of contracts. The DOJ and DHS will vet participating companies on technical proficiency, prior operational performance, facility security, and personnel vetting; the companies may then enter downstream agreements with other private entities to receive threat information and with federal, state, local, tribal, and territorial agencies to receive CE-TCO leads. Every proposed operation will then go to the NCC for written approval; all contractual relationships must be disclosed, and participation is reviewed annually. Notably, rather than amend the Computer Fraud and Abuse Act, the NSPM leans on an interpretive reading of 18 U.S.C. § 1030(f) extended to cover private delegates, which no federal appellate court has tested to date.

Effect on Criminal Landscape

Once the NCC program goes into effect, criminal groups would likely face U.S. adversaries that combine commercial engineering speed with federal legal cover. However, ZeroFox assesses cyber threat actors are likely to develop defensive adaptations to these new adversaries' operations rather than being deterred by them. The clearest loophole is the halt-and-minimize rule. Because an operation must stop the moment it touches a U.S.-based system, criminals who hide inside hacked American infrastructure (such as hospital networks, small business servers, and cloud tenancies) will very likely put themselves effectively out of reach. Sophisticated groups will likely adapt to and exploit this loophole deliberately within two to three quarters of the NCC's operating procedures becoming public. Further, accelerated threat actor migration toward bulletproof hosting in non-cooperative jurisdictions, onion-only leak sites, and shorter infrastructure lifecycles is likely.

Ransomware-as-as-serice (RaaS) groups will likely tighten affiliate vetting and retreat from public forums, making human-source collection harder and more expensive. That is expected to be the biggest "cost" of the NCC program to defenders: the ecosystem will almost certainly become harder to see before it becomes smaller. Named U.S. participating companies and their staff will also likely become threat actor targets, and

some financially motivated groups will likely seek or fabricate closer nation-state actor associations to place themselves outside the CE-TCO definition.

Outlook and Assessment

ZeroFox assesses with moderate confidence that the NCC program will almost certainly proceed. However, it is likely that the October deadline will yield interim rather than complete procedures and that first-cohort vetting will run into 2027, given that the NSPM did not provide the NCC with implementation details. Initial entrants are likely to be U.S. firms with existing federal clearances and offensive cyber threat-hunting pedigrees rather than large brand-sensitive vendors. There is a roughly even chance a misattribution or collateral-impact incident becomes public within 18 months of the first approved operations, which would likely expose NCC program participants and result in a legal challenge regarding the extension of 18 U.S.C. § 1030(f) to covering private delegates.

For ransomware specifically, ZeroFox assesses the program is unlikely to reduce top-tier extortion revenue measurably within 12 months; state-directed actors are outside the scope of its operations, and its immediate effect on criminal behavior is likely operational security improvement rather than attrition. Defenders should expect degraded visibility before any disruption dividend.

Signs the NCC Program Has Likely Launched

- Publication of NCC operating procedures and minimum participation standards on or around October 11, 2026, and whether the government solicits industry comment first.
- Procurement signals such as DOJ or DHS solicitations, sole source justifications, or broad agency announcements or awards referencing the program, CE-TCO operations, or the NCC.
- Disclosure or leak of participating company identities, including self-disclosure in vendor marketing or investor communications.
- First observable Cyber Effects Operation comprising infrastructure seizure, panel defacement, or data destruction on criminal assets, with no corresponding indictment, seizure banner, or international takedown announcement.

- Criminal ecosystem chatter referencing U.S. "privateers" or named vendors, and any affiliate rules newly prohibiting U.S.-hosted infrastructure.
- Deliberate co-location of criminal infrastructure inside U.S.-located or U.S.-person-controlled systems, indicating actors are exploiting the halt-and-minimize provisions.
- Targeting of security vendor personnel, including credential stuffing attacks against vendor identity providers, impersonation domains, and executive doxxing or physical security incidents involving named staff.
- Congressional activity, such as oversight hearings, authorization or restriction bills, appropriations riders, and the outcome of Cybersecurity Information Sharing Act reauthorization.
- Reciprocal announcements from allied or adversary governments licensing private offensive cyber actors.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%