ZEROFOX INTELLIGENCE

Flash

Proposed U.S. Legislation to Sanction Threat Actors

F-2025-12-04a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Geopolitics, Threat Actor, Cybersecurity Policy

December 4, 2025

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 12:00 PM (EST) on December 4, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Proposed U.S. Legislation to Sanction Threat Actors

| Key Findings

- On December 2, 2025, U.S. Congressman August Pfluger proposed a bill that would formally designate foreign parties who conduct attacks against U.S. organizations as “critical” cyber threat actors.
- In November 2025, National Cyber Director Sean Cairncross stated the Trump administration was seeking to establish a unique, coordinated cyber strategy.
- In July 2025, President Trump reportedly approved USD 1 billion in funding for an offensive hacking operation run by the Pentagon, likely signalling his administration’s focus on counter-cyber tactics and strategy.
- Given the current emphasis in Washington on taking a proactive approach to combatting cyber threats, it is very likely that the bill will pass—though it may go through minor revisions and amendments in the legislative process.

| Details

On December 2, 2025, U.S. Congressman August Pfluger proposed a bill that would formally designate foreign parties who conduct attacks against U.S. organizations as

"critical" cyber threat actors.[1] The bill would also create the legal framework for financial sanctions against threat actors, making it more difficult for them to benefit financially from their crimes.

- The 2025 Cyber Deterrence and Response Act would define a critical cyber threat actor as those who, "disrupt the availability of computer networks, compromise computers that provide services in critical infrastructure, steal significant personal data or trade secrets, destabilize the financial or energy sectors or undermine the election process."[2]
- Further, the bill requires an evidentiary framework for attribution of cyberattacks against the United States. Currently, the Departments of Homeland Security, Justice, Defense, and State operate on their own definitions and processes of attribution, which likely limits the government's ability to legally counter threat actors.
- According to a statement from Congressman Pfluger's office, the bill authorizes "robust sanctions against designated actors, including asset blocking, financial restrictions, export controls, procurement prohibitions, visa bans and suspension of assistance."[3] These sanctions would almost certainly limit threat actors' ability to conduct post-attack financial activities.

In November 2025, National Cyber Director Sean Cairncross stated the Trump administration was seeking to establish a coordinated cyber strategy "in a way that hasn't happened before."[4]

---

[1] hXXps://cyberscoop[.]com/legislation-would-designate-critical-cyber-threat-actors-direct-sanctions-against-them/

[2] hXXps://cyberscoop[.]com/legislation-would-designate-critical-cyber-threat-actors-direct-sanctions-against-them/

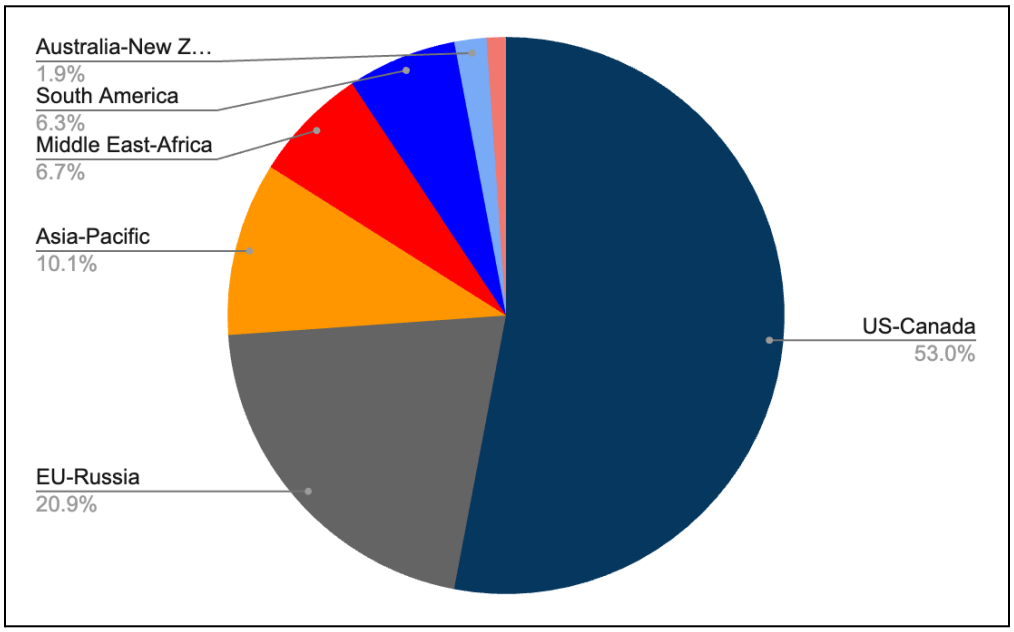
[3] hXXps://pfluger[.]house[.]gov/news/documentsingle.aspx?DocumentID=2687

[4] hXXps://www.cybersecuritydive[.]com/news/trump-administration-national-cyber-strategy-preview-sean-cairncross-aspen/805782/

- Part of that strategy, according to Director Cairncross, would be to impose a cost on countries like Russia and China for their conduct and support of cyberattacks against the United States.

In July 2025, President Trump approved USD 1 billion in funding for a hacking operation run by the Pentagon[5], likely signalling the administration's focus on counter-cyber tactics and strategy.

Bills similar to the Cyber Deterrence and Response Act have been put forward twice before. The most recent, also submitted by Congressman Pfluger in 2022, passed the House of Representatives but failed after not being taken up by the Senate. Given the emphasis on offensive cybersecurity from the current administration, it is likely that the bill will gain traction this time and be passed in some form.



2025 Cyberattacks by Region

Source: ZeroFox Intelligence

ZeroFox has observed that, throughout 2025, the United States has remained the most targeted country in the world for cyberattacks by both politically and financially motivated actors. Congressman Pfluger's submission of the Cyber Deterrence and

[5] hXXps://www.cyberdaily[.]au/government/12380-trump-admin-announces-1b-offensive-hacking-operation-spend

Response Act within a month of National Cyber Director Cairncross stating the Trump administration is seeking to establish a coordinated cyber strategy likely both point to the government prioritizing a unified strategy across federal agencies to combat the threat posed by cyber threat actors to critical U.S. infrastructure.

Given the current emphasis in Washington on taking a proactive approach to combatting cyber threats, it is very likely that the bill will pass, though it may go through minor revisions and amendments in the legislative process. The signals coming from the Trump administration make it almost certain that some form of the provisions in the proposed legislation will be implemented—potentially by executive order if the bill fails.

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%