ZEROFOX INTELLIGENCE

Flash

U.S. Directive to Withdraw from Global Cybersecurity Organizations

F-2026-01-16a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Geopolitics, Cybersecurity Policy

January 16, 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 (EST) on January 16, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | U.S. Directive to Withdraw from Global Cybersecurity Organizations

| Key Findings

- On January 7, 2026, U.S. President Donald Trump signed a Presidential Memorandum directing the withdrawal of the United States from 66 international organizations, including several global cybersecurity entities.
- This memorandum aligns with the Trump administration's broader and ongoing review of U.S. participation in all international intergovernmental organizations, conventions, and treaties.
- There is a roughly even chance that reduced U.S. participation in international cybersecurity and digital policy efforts will affect information-sharing, coordination on standards, and the alignment of U.S. law and policy with evolving multinational cybersecurity frameworks.

Details

On January 7, 2026, President Trump signed a Presidential Memorandum directing the withdrawal of the United States from 66 international organizations, including several global cybersecurity efforts.[1] These cybersecurity entities are an integral part of international collaboration frameworks on policy alignment and capacity development for the digital landscape. The United States will reportedly withdraw from the following cybersecurity and digital policy international bodies:[2]

- Global Forum on Cyber Expertise (GFCE), which supports issues with critical infrastructure protection, cybercrime, cyber skills and policy, and emerging technology;
- European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), which supports its members—including countries of the North Atlantic Treaty Organization (NATO)—against cyber threats; and
- Freedom Online Coalition (FOC), which works towards advancing internet freedom and protecting human rights online.

A fact sheet issued by the White House about the withdrawal states that the 66 organizations—which also include entities focused on climate change, democracy promotion, and gender equality—"operate contrary to U.S. national interests, security, economic prosperity, or sovereignty."[3] However, cybersecurity experts have reportedly expressed concerns regarding the cyber-related withdrawals, especially in light of the increasing volume and severity of cyber threats.[4]

The signing of this Presidential Memorandum aligns with the Trump administration's broader and ongoing review of U.S. participation in all international intergovernmental organizations, conventions, and treaties stemming from an executive order issued on

[1] hXXps://www.whitehouse[.]gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-withdraws-the-united-states-from-international-organizations-that-are-contrary-to-the-interests-of-the-united-states/
[2] hXXps://cyberscoop[.]com/trump-pulls-us-out-of-international-cyber-orgs/
[3] hXXps://www.whitehouse[.]gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-withdraws-the-united-states-from-international-organizations-that-are-contrary-to-the-interests-of-the-united-states/
[4] hXXps://cyberscoop[.]com/trump-pulls-us-out-of-international-cyber-orgs/

February 4, 2025.[5] Additional similar withdrawals are likely within the year, as the administration continues its reviews.

The Trump administration has demonstrated a mistrust of the utility and efficacy of multilateral organizations, especially those considered unaligned with the administration's "America First" agenda and other political ideologies. However, despite the directive to withdraw from the international organizations listed above, the U.S. government has taken other efforts to demonstrate its commitment to cybersecurity, as exemplified by proposed December 2025 legislation to pursue specific threat actors.[6] This likely signals the Trump administration is interested in operating individually rather than as part of multinational collectives.

The United Kingdom has taken a similar interest in focusing its internal political efforts towards individual implementation of cybersecurity law—likely in response to the series of prominent European-based retail cyberattacks in the first half of 2025.[7] According to media reports on January 11, 2026, the United Kingdom is investing GBP 210 million (approximately USD 281 million) to establish a new Government Cyber Unit to centralize risk management and coordinate cyber incident responses.[8]

While the U.S. withdrawal from international cybersecurity and digital policy bodies does not, in itself, indicate a lack of engagement with cybersecurity issues, it likely signals potential disruptions to multinational collaboration mechanisms. There is a roughly even chance that reduced participation in these coordinated efforts will affect information-sharing, coordination on standards, and the alignment of U.S. law and policy with evolving multinational cybersecurity frameworks.

---

[5] hXXps://www.whitehouse[.]gov/presidential-actions/2026/01/withdrawing-the-united-states-from-international-organizations-conventions-and-treaties-that-are-contrary-to-the-interests-of-the-united-states/

[6] https://www.zerofox.com/intelligence/flash-report-proposed-u-s-legislation-to-sanction-threat-actors/

[7] https://www.zerofox.com/intelligence/flash-report-series-of-uk-cyberattacks-inspires-new-cybersecurity-law/

[8] hXXps://unn[.]ua/en/news/uk-establishes-government-cyber-unit-to-protect-against-large-scale-cyberattacks-szr

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%