Executive Order 14390—Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens

March 6, 2026

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose and Policy. Cybercrime, fraud, and predatory schemes are draining American families of their life savings, stealing the benefits of years of work, and destroying the lives of our youth. These activities—which include deploying ransomware and malware, phishing, financial fraud, "sextortion" and other extortion schemes, impersonation, and more—are often coordinated campaigns carried out by Transnational Criminal Organizations (TCOs) aimed at the most vulnerable among us. In many cases, foreign regimes provide willing or tacit state support to cybercrime and predatory schemes, creating a shadow economy fueled by stolen identities, coercion, forced labor, and human trafficking.

It is the policy of the United States to protect Americans from, and harden our financial and digital systems against, these threats. The United States shall counter attacks on Americans with a commensurate response that includes law enforcement, diplomacy, and potential offensive actions. It is further the policy of the United States to provide support to victims of these crimes, expand public alerts, and prioritize protection for those most at risk to end the exploitation and victimization of Americans.

Sec. 2. Combating Scam Centers and Cybercrime. (a) The Secretary of State, the Secretary of the Treasury, the Secretary of War, the Attorney General, and the Secretary of Homeland Security, in consultation with the Office of the National Cyber Director, and in coordination with the Assistant to the President and Homeland Security Advisor (APHSA), shall:

> (i) within 60 days of the date of this order, review the relevant operational, technical, diplomatic, and regulatory frameworks in place to determine how each can be improved to best combat TCOs engaged in cyber-enabled crime and similar predatory schemes against Americans; and
>
> (ii) within 120 days of the date of this order, using the results of the review directed in subsection (a)(i) of this section, submit to the President, through the APHSA, an action plan that identifies the TCOs responsible for scam centers and cybercrime and proposes solutions to prevent, disrupt, investigate, and dismantle these TCOs. This action plan shall provide for the creation of an operational cell within the National Coordination Center (NCC) established pursuant to section 6(d) of Executive Order 14159 of January 20, 2025 (Protecting the American People Against Invasion), which will be responsible for coordinating Federal efforts to detect, disrupt, dismantle, and deter—including by involving the private sector as appropriate—cyber-enabled criminal activity conducted by foreign TCOs and associated networks that target United States persons, businesses, critical infrastructure, or public services.

(b) The action plan shall describe how, consistent with applicable law, the Attorney General and the Secretary of Homeland Security, supported by the Secretary of War, shall use relevant technical capabilities, threat intelligence, and operational insights from commercial cybersecurity firms and other non-Federal entities, as appropriate, to enhance attribution, tracking, and disruption of malicious cyber actors and enabling infrastructure engaged in cybercrime, fraud, and predatory schemes.

(c) The action plan and NCC operational cell shall include mechanisms to improve information sharing, operational coordination, and rapid response across the Federal Government, and shall align with existing law enforcement frameworks and efforts to counter cyber-enabled threats emanating from foreign jurisdictions.

(d) The Attorney General shall continue to prioritize prosecutions of defendants engaged in cyber-enabled fraud, including scam centers and sextortion schemes, and, consistent with the principles of Federal prosecution, shall pursue the most serious, provable offenses encompassed by such fraudulent schemes.

(e) To the maximum extent permitted by law, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall partner with the NCC to provide training, technical assistance, and resilience building to support State, local, Tribal, and territorial (SLTT) partners, including to expand defensive capacity, share threat intelligence, and harden SLTT partners' critical infrastructure systems against cybercrime exploitation by TCOs.

Sec. 3. Victim Restoration Program. Within 90 days of the date of this order, the Attorney General shall submit a recommendation to the President, through the APHSA, regarding the establishment of a Victims Restoration Program designed to provide, to the greatest extent authorized by law and in consideration of the Department of Justice's goal of serving all victims of crime, restoration or remission to victims of cyber-enabled fraud schemes from funds clawed back, forfeited, or seized from the TCOs that perpetrate such schemes.

Sec. 4. International Engagement. The Secretary of State, in coordination with the NCC, shall engage with foreign governments to demand enforcement actions against TCOs operating within their borders and greater cooperation with United States law enforcement. The Secretary of State shall take all necessary and appropriate steps to ensure that nations that tolerate such predatory activity shall face consequences consistent with United States law and policy, such as the limitation of foreign assistance, the application of targeted sanctions, visa restrictions, trade penalties, and, where appropriate, the immediate expulsion from the United States of foreign officials and diplomats complicit in these schemes. The Secretary of State shall also coordinate these actions with allies and partners to enhance the consequences of actions taken against nations that tolerate predatory activity.

Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise effect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(d) The costs for publication of this order shall be borne by the Department of Homeland Security.

DONALD J. TRUMP

The White House,

March 6, 2026.

[Filed with the Office of the Federal Register, 11:15 a.m., March 10, 2026]

NOTE: This Executive order was published in the *Federal Register* on March 11.

Categories: Executive Orders : Cybercrime, fraud, and predatory schemes against U.S. citizens, efforts to combat.

Subjects: Attorney General; Cybersecurity, strengthening efforts; Fraud enforcement, strengthening efforts; Secretary of Homeland Security; Secretary of State; Secretary of the Treasury; Secretary of War; Transnational criminal organizations.

DCPD Number: DCPD202600154.