

119TH CONGRESS
1ST SESSION

H. R. 5900

To direct the Department of Defense to establish a joint task force to investigate transnational cybercrimes, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 31, 2025

Mr. VINDMAN (for himself and Mr. BAIRD) introduced the following bill; which was referred to the Committee on Foreign Affairs

A BILL

To direct the Department of Defense to establish a joint task force to investigate transnational cybercrimes, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Stopping Cross-border
5 Attacks and Manipulation Act” or the “SCAM Act”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

8 (1) According to estimates from the United
9 States Institute of Peace, China-linked transnational
10 organized crime (TOC) groups operating “fraud

1 farms” in Southeast Asia are stealing nearly
2 \$43,800,000,000 annually through digital scams.

3 (2) These scams increasingly affect Americans,
4 disproportionately targeting populations such as the
5 elderly and socially isolated.

6 (3) According to the Federal Trade Commission
7 (FTC), in 2024 alone—

8 (A) 246,783 scam text messages were re-
9 ported, resulting in \$469,000,000 in losses to
10 Americans;

11 (B) 371,664 scam emails were reported,
12 leading to \$502,000,000 in losses to Americans;
13 and

14 (C) 284,651 scam phone calls were re-
15 ported, causing \$948,000,000 in losses to
16 Americans.

17 (4) Transnational organized crime (TOC)
18 groups maintain documented ties to the Chinese
19 Communist Party (CCP). Chinese officials and
20 state-owned enterprises (SOEs) have provided direct
21 support for the construction and operation of TOC-
22 linked facilities, raising serious concerns about a co-
23 ordinated campaign of foreign interference and sabo-
24 tage.

1 (5) The CCP's involvement in TOC networks
2 presents an urgent national security threat. These
3 networks funnel financial assets and sensitive per-
4 sonal information of U.S. citizens to a hostile for-
5 eign power, undermining both American economic
6 security and individual privacy.

7 (6) These criminal networks have deeply embed-
8 ded themselves into Southeast Asian economies, ex-
9 erting destabilizing influence across the region.

10 (7) Proceeds from these scams are used to fund
11 warlords and fuel ongoing civil conflicts,
12 compounding regional instability.

13 (8) TOC networks have trafficked an estimated
14 300,000 individuals into cyber scam operations
15 across Southeast Asia. Victims, including United
16 States citizens, are forced to work under conditions
17 that the U.S.-China Economic and Security Review
18 Commission compares to modern slavery. The
19 United Nations has warned that human trafficking
20 tied to these scam centers has reached the level of
21 a humanitarian and human rights crisis.

22 (9) The U.S.-China Economic and Security Re-
23 view Commission has acknowledged credible reports
24 linking scam compounds in the Philippines to Chi-
25 nese espionage activity. These facilities are being

1 constructed near air bases strategically important to
2 U.S. operations, including Clark Air Base and Basa
3 Air Base, which is part of the Enhanced Defense
4 Cooperation Agreement. The Philippine intelligence
5 community has provided compelling evidence that
6 these compounds have been used for surveillance and
7 cyber intrusions.

8 (10) The Chinese government has used the
9 presence of Chinese TOC networks in Southeast
10 Asia to pressure regional governments to allow a
11 greater role for Chinese security forces. This effort
12 threatens national sovereignty and regional stability.

13 (11) TOC networks endanger American defense
14 priorities as well as democracy, good governance,
15 and stability around the world by co-opting local
16 elites, undermining law enforcement, weakening
17 state authority, and threatening the United States'
18 strategic interest in building a free and open Indo-
19 Pacific.

20 (12) An effective response by the United States
21 Government will require a coordinated, whole-of-gov-
22 ernment effort that draws on the competencies of
23 Federal agencies in information collection, financial
24 enforcement, diplomatic engagement, defense and in-
25 telligence preparedness, and law enforcement.

1 **SEC. 3. JOINT TASK FORCE TO INVESTIGATE**
2 **TRANSNATIONAL CYBERCRIMES.**

3 (a) ESTABLISHMENT.—

4 (1) IN GENERAL.—The Secretary of Defense,
5 acting through the head of U.S. Cyber Command
6 and in coordination with the heads of other appro-
7 priate agencies, shall establish a joint task force to
8 coordinate efforts to investigate, disrupt, and protect
9 citizens of the United States from transnational
10 cybercrimes and foreign-operated scam networks, in-
11 cluding fraudulent text and direct messaging centers
12 and other digital fraud schemes targeting citizens of
13 the United States.

14 (2) MEMBERSHIP.—The task force shall, at a
15 minimum, be composed of—

16 (A) an official of the Department of State,
17 including—

18 (i) the Assistant Secretary for Emerg-
19 ing Threats;

20 (ii) the Assistant Secretary for Inter-
21 national Narcotics and Law Enforcement;
22 and

23 (iii) the Assistant Secretary for De-
24 mocracy, Human Rights, and Labor;

1 (B) officials of the Department of Defense,
2 including U.S. Cyber Command and the Na-
3 tional Mission Force;

4 (C) an official of the Office of the Director
5 of National Intelligence;

6 (D) an official of the Federal Trade Com-
7 mission;

8 (E) an official of the Federal Communica-
9 tions Commission;

10 (F) officials of the Office of Foreign Assets
11 Control and the Financial Crimes Enforcement
12 Network of the Department of the Treasury;

13 (G) officials of the Department of Justice,
14 including officials from—

15 (i) the Criminal Division, including
16 the International Unit of the Money Laun-
17 dering and Asset Recovery Section;

18 (ii) the Office of International Affairs;

19 (iii) the National Security Division;

20 and

21 (iv) the Office of the Cyber Amba-
22 sador;

23 (H) an official of the Federal Bureau of
24 Investigation's Internet Crime Complaint Cen-
25 ter;

1 (I) representatives of State and local gov-
2 ernments that—

3 (i) are leading efforts to counter
4 cybercrimes; or

5 (ii) are disproportionately affected by
6 cybercrimes; and

7 (J) representatives of relevant expert non-
8 profit organizations.

9 (3) LEADERSHIP.—The members of the task
10 force, in consultation with the leadership of the De-
11 partment of Defense, may assign responsibility to an
12 appropriate office within the Department of Defense
13 to serve as the lead for the task force to coordinate
14 the preparation and submission of the report re-
15 quired by subsection (c) and hold offices and agen-
16 cies responsible for implementation.

17 (b) PRIORITY.—In carrying out its duties under sub-
18 section (a) and in preparing the report under subsection
19 (c), the task force shall prioritize work related to scam
20 operations with ties to the Chinese Communist Party in
21 the Indo-Pacific region.

22 (c) REPORT.—Not later than one year after the date
23 of enactment of this Act, the task force established under
24 subsection (a) shall submit to the Committees on Armed

1 Services of the House of Representatives and of the Sen-
2 ate a report—

3 (1) identifying emerging trends related to the
4 scam operations described in subsection (a) that are
5 tied to international criminal organizations, includ-
6 ing efforts to—

7 (A) scam and steal data from United
8 States persons;

9 (B) cultivate relationships with adversarial
10 governments and foreign intelligence services;

11 (C) acquire land in proximity to United
12 States military installations and United States
13 treaty allies' and partners' military installa-
14 tions;

15 (D) leverage, collaborate with, or place for-
16 eign nationals of concern in sensitive positions
17 within Indo-Pacific regional governments;

18 (E) undermine United States diplomatic
19 engagement, peacekeeping operations, and secu-
20 rity cooperation efforts throughout the world,
21 with a priority on the Indo-Pacific region;

22 (F) acquire territory or influence around
23 critical waterways; and

24 (G) construct militarily-capable infrastruc-
25 ture such as airports;

(2) recommending policy options for the Federal Government, Congress, and nongovernmental industry leaders to prevent and penalize the scam operations described in subsection (a) that are tied to international criminal organizations, which may include the use of sanctions, civil asset forfeiture, and action in cyberspace in defense of the United States, its persons, assets, and interests against the scam networks described in subsection (a), including—

(A) protecting Americans’ personal data and financial assets;

(B) safeguarding the sovereignty of United States allies and partners; and

(C) securing United States military installations and United States treaty allies’ and partners’ military installations located near known or suspected scam compounds;

(3) proposing a framework for a whole-of-society approach to support disproportionately affected demographic groups, communications platforms, States, and localities impacted by the scam networks described in subsection (a), including methods for timely dissemination of scam-related information and protective guidance through publicly accessible

1 Federal facilities (including United States Postal
2 Service locations, Social Security Administration
3 field offices, military installations, and Department
4 of Veterans Affairs facilities) and comparable State
5 and local venues;

6 (4) including an assessment and updates of the
7 overall scale of scam centers in Southeast Asia and
8 recent trendlines;

9 (5) information about how the Chinese Govern-
10 ment is exploiting the problem of scam centers to ex-
11 pand its security presence and influence in the re-
12 gion; and

13 (6) information about government bodies, indi-
14 vidual government officials, militias, and corpora-
15 tions in Southeast Asia that have ties to
16 transnational criminal organizations or profit from
17 scam centers.

18 (d) IMPLEMENTATION.—The task force shall assist in
19 the implementation of any recommendations or proposals
20 contained in the report submitted under subsection (c).

21 (e) SUNSET.—The authority under this section shall
22 sunset on the date that is 5 years after the date on which
23 the task force submits the report under subsection (c).

○