

118TH CONGRESS
2D SESSION

H. R. 9769

To ensure the security and integrity of United States critical infrastructure by establishing an interagency task force and requiring a comprehensive report on the targeting of United States critical infrastructure by People’s Republic of China state-sponsored cyber actors, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 24, 2024

Ms. LEE of Florida (for herself, Mr. GREEN of Tennessee, and Mr. MOOLENAAR) introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To ensure the security and integrity of United States critical infrastructure by establishing an interagency task force and requiring a comprehensive report on the targeting of United States critical infrastructure by People’s Republic of China state-sponsored cyber actors, 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 “Strengthening Cyber
5 Resilience Against State-Sponsored Threats Act”.

1 **SEC. 2. INTERAGENCY TASK FORCE AND REPORT ON THE**
2 **TARGETING OF UNITED STATES CRITICAL IN-**
3 **FRASTRUCTURE BY PEOPLE’S REPUBLIC OF**
4 **CHINA STATE-SPONSORED CYBER ACTORS.**

5 (a) INTERAGENCY TASK FORCE.—Not later than 120
6 days after the date of the enactment of this Act, the Sec-
7 retary of Homeland Security, acting through the Director
8 of the Cybersecurity and Infrastructure Security Agency
9 (CISA) of the Department of Homeland Security, in con-
10 sultation with the Attorney General, the Director of the
11 Federal Bureau of Investigation, and the heads of appro-
12 priate Sector Risk Management Agencies as determined
13 by the Director of CISA, shall establish a joint interagency
14 task force (in this section referred to as the “task force”)
15 to facilitate collaboration and coordination among the Sec-
16 tor Risk Management Agencies assigned a Federal role or
17 responsibility in National Security Memorandum–22,
18 issued April 30, 2024 (relating to critical infrastructure
19 security and resilience), or any successor document, to de-
20 tect, analyze, and respond to the cybersecurity threat
21 posed by State-sponsored cyber actors, including Volt Ty-
22 phoon, of the People’s Republic of China by ensuring that
23 such agencies’ actions are aligned and mutually rein-
24 forcing.

25 (b) CHAIRS.—

1 (1) CHAIRPERSON.—The Director of CISA (or
2 the Director of CISA’s designee) shall serve as the
3 chairperson of the task force.

4 (2) VICE CHAIRPERSON.—The Director of the
5 Federal Bureau of Investigation (or such Director’s
6 designee) shall serve as the vice chairperson of the
7 task force.

8 (c) COMPOSITION.—

9 (1) IN GENERAL.—The task force shall consist
10 of appropriate representatives of the departments
11 and agencies specified in subsection (a).

12 (2) QUALIFICATIONS.—To materially assist in
13 the activities of the task force, representatives under
14 paragraph (1) should be subject matter experts who
15 have familiarity and technical expertise regarding cy-
16 bersecurity, digital forensics, or threat intelligence
17 analysis, or in-depth knowledge of the tactics, tech-
18 niques, and procedures (TTPs) commonly used by
19 State-sponsored cyber actors, including Volt Ty-
20 phoon, of the People’s Republic of China.

21 (d) VACANCY.—Any vacancy occurring in the mem-
22 bership of the task force shall be filled in the same manner
23 in which the original appointment was made.

24 (e) ESTABLISHMENT FLEXIBILITY.—To avoid redun-
25 dancy, the task force may coordinate with any preexisting

1 task force, working group, or cross-intelligence effort with-
2 in the Homeland Security Enterprise or the intelligence
3 community that has examined or responded to the cyberse-
4 curity threat posed by State-sponsored cyber actors, in-
5 cluding Volt Typhoon, of the People's Republic of China.

6 (f) TASK FORCE REPORTS; BRIEFING.—

7 (1) INITIAL REPORT.—Not later than 540 days
8 after the establishment of the task force, the task
9 force shall submit to the appropriate congressional
10 committees the first report containing the initial
11 findings, conclusions, and recommendations of the
12 task force.

13 (2) ANNUAL REPORT.—Not later than one year
14 after the date of the submission of the initial report
15 under paragraph (1) and annually thereafter for five
16 years, the task force shall submit to the appropriate
17 congressional committees an annual report con-
18 taining the findings, conclusions, and recommenda-
19 tions of the task force.

20 (3) CONTENTS.—The reports under this sub-
21 section shall include the following:

22 (A) An assessment at the lowest classifica-
23 tion feasible of the sector-specific risks, trends
24 relating to incidents impacting sectors, and tac-
25 tics, techniques, and procedures utilized by or

1 relating to State-sponsored cyber actors, includ-
2 ing Volt Typhoon, of the People's Republic of
3 China.

4 (B) An assessment of additional resources
5 and authorities needed by Federal departments
6 and agencies to better counter the cybersecurity
7 threat posed by State-sponsored cyber actors,
8 including Volt Typhoon, of the People's Repub-
9 lic of China.

10 (C) A classified assessment of the extent of
11 potential destruction, compromise, or disruption
12 to United States critical infrastructure by
13 State-sponsored cyber actors, including Volt Ty-
14 phoon, of the People's Republic of China in the
15 event of a major crisis or future conflict be-
16 tween the People's Republic of China and the
17 United States.

18 (D) A classified assessment of the ability
19 of the United States to counter the cybersecu-
20 rity threat posed by State-sponsored cyber ac-
21 tors, including Volt Typhoon, of the People's
22 Republic of China in the event of a major crisis
23 or future conflict between the People's Republic
24 of China and the United States, including with
25 respect to different cybersecurity measures and

1 recommendations that could mitigate such a
2 threat.

3 (E) A classified assessment of the ability
4 of State-sponsored cyber actors, including Volt
5 Typhoon, of the People's Republic of China to
6 disrupt operations of the United States Armed
7 Forces by hindering mobility across critical in-
8 frastructure such as rail, aviation, and ports,
9 including how such would impair the ability of
10 the United States Armed Forces to deploy and
11 maneuver forces effectively.

12 (F) A classified assessment of the eco-
13 nomic and social ramifications of a disruption
14 to one or multiple United States critical infra-
15 structure sectors by State-sponsored cyber ac-
16 tors, including Volt Typhoon, of the People's
17 Republic of China in the event of a major crisis
18 or future conflict between the People's Republic
19 of China and the United States.

20 (G) Such recommendations as the task
21 force may have for the Homeland Security En-
22 terprise, the intelligence community, or critical
23 infrastructure owners and operators to improve
24 the detection and mitigation of the cybersecu-
25 rity threat posed by State-sponsored cyber ac-

1 tors, including Volt Typhoon, of the People's
2 Republic of China.

3 (H) A one-time plan for an awareness
4 campaign to familiarize critical infrastructure
5 owners and operators with security resources
6 and support offered by Federal departments
7 and agencies to mitigate the cybersecurity
8 threat posed by State-sponsored cyber actors,
9 including Volt Typhoon, of the People's Repub-
10 lic of China.

11 (4) BRIEFING.—Not later than 30 days after
12 the date of the submission of each report under this
13 subsection, the task force shall provide to the appro-
14 priate congressional committees a classified briefing
15 on the findings, conclusions, and recommendations
16 of the task force.

17 (5) FORM.—Each report under this subsection
18 shall be submitted in classified form, consistent with
19 the protection of intelligence sources and methods,
20 but may include an unclassified executive summary.

21 (6) PUBLICATION.—The unclassified executive
22 summary of each report required under this sub-
23 section shall be published on a publicly accessible
24 website of the Department of Homeland Security.

25 (g) ACCESS TO INFORMATION.—

1 (1) IN GENERAL.—The Secretary of Homeland
2 Security, the Director of CISA, the Attorney Gen-
3 eral, the Director of the Federal Bureau of Inves-
4 tigation, and the heads of appropriate Sector Risk
5 Management Agencies, as determined by the Direc-
6 tor of CISA, shall provide to the task force such in-
7 formation, documents, analysis, assessments, find-
8 ings, evaluations, inspections, audits, or reviews re-
9 lating to efforts to counter the cybersecurity threat
10 posed by State-sponsored cyber actors, including
11 Volt Typhoon, of the People’s Republic of China as
12 the task force considers necessary to carry out this
13 section.

14 (2) RECEIPT, HANDLING, STORAGE, AND DIS-
15 SEMINATION.—Information, documents, analysis, as-
16 sessments, findings, evaluations, inspections, audits,
17 and reviews described in this subsection shall be re-
18 ceived, handled, stored, and disseminated only by
19 members of the task force consistent with all appli-
20 cable statutes, regulations, and executive orders.

21 (3) SECURITY CLEARANCES FOR TASK FORCE
22 MEMBERS.—No member of the task force may be
23 provided with access to classified information under
24 this section without the appropriate security clear-
25 ances.

1 (h) TERMINATION.—The task force, and all the au-
2 thorities of this section, shall terminate on the date that
3 is 60 days after the final briefing required under sub-
4 section (h)(4).

5 (i) EXEMPTION FROM FACCA.—Chapter 10 of title
6 5, United States Code (commonly referred to as the “Fed-
7 eral Advisory Committee Act”), shall not apply to the task
8 force.

9 (j) EXEMPTION FROM PAPERWORK REDUCTION
10 ACT.—Chapter 35 of title 44, United States Code (com-
11 monly known as the “Paperwork Reduction Act”), shall
12 not apply to the task force.

13 (k) DEFINITIONS.—In this section:

14 (1) APPROPRIATE CONGRESSIONAL COMMIT-
15 TEES.—The term “appropriate congressional com-
16 mittees” means—

17 (A) the Committee on Homeland Security,
18 the Committee on Judiciary, and the Select
19 Committee on Intelligence of the House of Rep-
20 resentatives; and

21 (B) the Committee on Homeland Security
22 and Governmental Affairs, the Committee on
23 Judiciary, and the Select Committee on Intel-
24 ligence of the Senate.

1 (2) ASSETS.—The term “assets” means a per-
2 son, structure, facility, information, material, equip-
3 ment, network, or process, whether physical or vir-
4 tual, that enables an organization’s services, func-
5 tions, or capabilities.

6 (3) CRITICAL INFRASTRUCTURE.—The term
7 “critical infrastructure” has the meaning given such
8 term in section 1016(e) of Public Law 107–56 (42
9 U.S.C. 5195c(e)).

10 (4) CYBERSECURITY THREAT.—The term “cy-
11 bersecurity threat” has the meaning given such term
12 in section 2200 of the Homeland Security Act of
13 2002 (6 U.S.C. 650).

14 (5) HOMELAND SECURITY ENTERPRISE.—The
15 term “Homeland Security Enterprise” has the
16 meaning given such term in section 2200 of the
17 Homeland Security Act of 2002 (6 U.S.C. 650).

18 (6) INCIDENT.—The term “incident” has the
19 meaning given such term in section 2200 of the
20 Homeland Security Act of 2002 (6 U.S.C. 650).

21 (7) INFORMATION SHARING.—The term “infor-
22 mation sharing” means the bidirectional sharing of
23 timely and relevant information concerning a cyber-
24 security threat posed by a State-sponsored cyber

1 actor of the People’s Republic of China to United
2 States critical infrastructure.

3 (8) INTELLIGENCE COMMUNITY.—The term
4 “intelligence community” has the meaning given
5 such term in section 3(4) of the National Security
6 Act of 1947 (50 U.S.C. 3003(4)).

7 (9) LOCALITY.—The term “locality” means any
8 local government authority or agency or component
9 thereof within a State having jurisdiction over mat-
10 ters at a county, municipal, or other local govern-
11 ment level.

12 (10) SECTOR.—The term “sector” means a col-
13 lection of assets, systems, networks, entities, or or-
14 ganizations that provide or enable a common func-
15 tion for national security (including national defense
16 and continuity of Government), national economic
17 security, national public health or safety, or any
18 combination thereof.

19 (11) SECTOR RISK MANAGEMENT AGENCY.—
20 The term “Sector Risk Management Agency” has
21 the meaning given such term in section 2200 of the
22 Homeland Security Act of 2002 (6 U.S.C. 650).

23 (12) STATE.—The term “State” means any
24 State of the United States, the District of Columbia,
25 the Commonwealth of Puerto Rico, the Northern

1 Mariana Islands, the United States Virgin Islands,
2 Guam, American Samoa, and any other territory or
3 possession of the United States.

4 (13) SYSTEMS.—The term “systems” means a
5 combination of personnel, structures, facilities, infor-
6 mation, materials, equipment, networks, or proc-
7 esses, whether physical or virtual, integrated or
8 interconnected for a specific purpose that enables an
9 organization’s services, functions, or capabilities.

10 (14) UNITED STATES.—The term “United
11 States”, when used in a geographic sense, means
12 any State of the United States.

13 (15) VOLT TYPHOON.—The term “Volt Ty-
14 phoon” means the People’s Republic of China State-
15 sponsored cyber actor described in the Cybersecurity
16 and Infrastructure Security Agency cybersecurity
17 advisory entitled “PRC State-Sponsored Actors
18 Compromise and Maintain Persistent Access to U.S.
19 Critical Infrastructure”, issued on February 07,
20 2024, or any successor advisory.

○