

.....
(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. _____

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

Ms. LEE of Florida introduced the following bill; which was referred to the Committee on _____

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Strengthening Cyber
3 Resilience Against State-Sponsored Threats Act”.

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

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

1 such agencies' actions are aligned and mutually rein-
2 forcing.

3 (b) CHAIRS.—

4 (1) CHAIRPERSON.—The Director of CISA (or
5 the Director of CISA's designee) shall serve as the
6 chairperson of the task force.

7 (2) VICE CHAIRPERSON.—The Director of the
8 Federal Bureau of Investigation (or such Director's
9 designee) shall serve as the vice chairperson of the
10 task force.

11 (c) COMPOSITION.—

12 (1) IN GENERAL.—The task force shall consist
13 of appropriate representatives of the departments
14 and agencies specified in subsection (a).

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

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

4 (e) ESTABLISHMENT FLEXIBILITY.—To avoid redun-
5 dancy, the task force may coordinate with any preexisting
6 task force, working group, or cross-intelligence effort with-
7 in the Homeland Security Enterprise or the intelligence
8 community that has examined or responded to the cyberse-
9 curity threat posed by state-sponsored cyber actors, in-
10 cluding Volt Typhoon, of the People’s Republic of China.

11 (f) TASK FORCE REPORTS; BRIEFING.—

12 (1) INITIAL REPORT.—Not later than 540 days
13 after the establishment of the task force, the task
14 force shall submit to the appropriate congressional
15 committees the first report containing the initial
16 findings, conclusions, and recommendations of the
17 task force.

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

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

3 (A) An assessment at the lowest classifica-
4 tion feasible of the sector-specific risks, trends
5 relating to incidents impacting sectors, and tac-
6 tics, techniques, and procedures utilized by or
7 relating to state-sponsored cyber actors, includ-
8 ing Volt Typhoon, of the People’s Republic of
9 China.

10 (B) An assessment of additional resources
11 and authorities needed by Federal departments
12 and agencies to better counter the cybersecurity
13 threat posed by state-sponsored cyber actors,
14 including Volt Typhoon, of the People’s Repub-
15 lic of China .

16 (C) A classified assessment of the extent of
17 potential destruction, compromise, or disruption
18 to United States critical infrastructure by state-
19 sponsored cyber actors, including Volt Typhoon,
20 of the People’s Republic of China in the event
21 of a major crisis or future conflict between the
22 People’s Republic of China and the United
23 States.

24 (D) A classified assessment of the ability
25 of the United States to counter the cybersecu-

1 rity threat posed by state-sponsored cyber ac-
2 tors, including Volt Typhoon, of the People's
3 Republic of China in the event of a major crisis
4 or future conflict between the People's Republic
5 of China and the United States, including with
6 respect to different cybersecurity measures and
7 recommendations that could mitigate such a
8 threat.

9 (E) A classified assessment of the ability
10 of state-sponsored cyber actors, including Volt
11 Typhoon, of the People's Republic of China to
12 disrupt operations of the United States Armed
13 Forces by hindering mobility across critical in-
14 frastructure such as rail, aviation, and ports,
15 including how such would impair the ability of
16 the United States Armed Forces to deploy and
17 maneuver forces effectively.

18 (F) A classified assessment of the eco-
19 nomic and social ramifications of a disruption
20 to one or multiple United States critical infra-
21 structure sectors by state-sponsored cyber ac-
22 tors, including Volt Typhoon, of the People's
23 Republic of China in the event of a major crisis
24 or future conflict between the People's Republic
25 of China and the United States.

1 (G) Such recommendations as the task
2 force may have for the Homeland Security En-
3 terprise, the intelligence community, or critical
4 infrastructure owners and operators to improve
5 the detection and mitigation of the cybersecu-
6 rity threat posed by state-sponsored cyber ac-
7 tors, including Volt Typhoon, of the People's
8 Republic of China.

9 (H) A one-time plan for an awareness
10 campaign to familiarize critical infrastructure
11 owners and operators with security resources
12 and support offered by Federal departments
13 and agencies to mitigate the cybersecurity
14 threat posed by state-sponsored cyber actors,
15 including Volt Typhoon, of the People's Repub-
16 lic of China.

17 (4) BRIEFING.—Not later than 30 days after
18 the date of the submission of each report under this
19 subsection, the task force shall provide to the appro-
20 priate congressional committees a classified briefing
21 on the findings, conclusions, and recommendations
22 of the task force.

23 (5) FORM.—Each report under this subsection
24 shall be submitted in classified form, consistent with

1 the protection of intelligence sources and methods,
2 but may include an unclassified executive summary.

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

7 (g) ACCESS TO INFORMATION.—

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

21 (2) RECEIPT, HANDLING, STORAGE, AND DIS-
22 SEMINATION.—Information, documents, analysis, as-
23 sessments, findings, evaluations, inspections, audits,
24 and reviews described in this subsection shall be re-
25 ceived, handled, stored, and disseminated only by

1 members of the task force consistent with all appli-
2 cable statutes, regulations, and executive orders.

3 (3) SECURITY CLEARANCES FOR TASK FORCE
4 MEMBERS.—No member of the task force may be
5 provided with access to classified information under
6 this section without the appropriate security clear-
7 ances.

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

12 (i) EXEMPTION FROM FACA.—Chapter 10 of title
13 5, United States Code (commonly referred to as the “Fed-
14 eral Advisory Committee Act”), shall not apply to the task
15 force.

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

20 (k) DEFINITIONS.—In this section:

21 (1) APPROPRIATE CONGRESSIONAL COMMIT-
22 TEES.—The term “appropriate congressional com-
23 mittees” means—

24 (A) the Committee on Homeland Security,
25 the Committee on Judiciary, and the Select

1 Committee on Intelligence of the House of Rep-
2 resentatives; and

3 (B) the Committee on Homeland Security
4 and Governmental Affairs, the Committee on
5 Judiciary, and the Select Committee on Intel-
6 ligence of the Senate.

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

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

16 (4) CYBERSECURITY THREAT.—The term “cy-
17 bersecurity threat” has the meaning given such term
18 in section 2200 of the Homeland Security Act of
19 2002 (6 U.S.C. 650).

20 (5) HOMELAND SECURITY ENTERPRISE.—The
21 term “Homeland Security Enterprise” has the
22 meaning given such term in section 2200 of the
23 Homeland Security Act of 2002 (6 U.S.C. 650).

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

4 (7) INFORMATION SHARING.—The term “infor-
5 mation sharing” means the bidirectional sharing of
6 timely and relevant information concerning a cyber-
7 security threat posed by a state-sponsored cyber
8 actor of the People’s Republic of China to United
9 States critical infrastructure.

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

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

19 (10) SECTOR.—The term “sector” means a col-
20 lection of assets, systems, networks, entities, or or-
21 ganizations that provide or enable a common func-
22 tion for national security (including national defense
23 and continuity of Government), national economic
24 security, national public health or safety, or any
25 combination thereof.

1 (11) SECTOR RISK MANAGEMENT AGENCY.—

2 The term “Sector Risk Management Agency” has
3 the meaning given such term in section 2200 of the
4 Homeland Security Act of 2002 (6 U.S.C. 650).

5 (12) STATE.—The term “State” means any
6 State of the United States, the District of Columbia,
7 the Commonwealth of Puerto Rico, the Northern
8 Mariana Islands, the United States Virgin Islands,
9 Guam, American Samoa, and any other territory or
10 possession of the United States.

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

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

20 (15) VOLT TYPHOON.—The term “Volt Ty-
21 phoon” means the People’s Republic of China state-
22 sponsored cyber actor described in the Cybersecurity
23 and Infrastructure Security Agency cybersecurity
24 advisory entitled “PRC State-Sponsored Actors
25 Compromise and Maintain Persistent Access to U.S.

1 Critical Infrastructure”, issued on February 07,
2 2024, or any successor advisory.