

119<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

**S.** \_\_\_\_\_

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 SENATE OF THE UNITED STATES

---

Mr. SCOTT of Florida introduced the following bill; which was read twice and 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,*

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) DEFINITIONS.—In this section:

6 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
7 TEES.—The term “appropriate congressional com-  
8 mittees” means—

9 (A) the Committee on Homeland Security  
10 and Governmental Affairs, the Committee on  
11 the Judiciary, and the Select Committee on In-  
12 telligence of the Senate; and

13 (B) the Committee on Homeland Security,  
14 the Committee on the Judiciary, and the Per-  
15 manent Select Committee on Intelligence of the  
16 House of Representatives.

17 (2) ASSET.—The term “asset” means a person,  
18 structure, facility, information, material, equipment,  
19 network, or process, whether physical or virtual, that  
20 enables the services, functions, or capabilities of an  
21 organization.

22 (3) CRITICAL INFRASTRUCTURE.—The term  
23 “critical infrastructure” has the meaning given the  
24 term in section 1016(e) of the Critical Infrastruc-  
25 tures Protection Act of 2001 (42 U.S.C. 5195c(e)).

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

5           (5) DIRECTOR.—The term “Director” means  
6           the Director of the Cybersecurity and Infrastructure  
7           Security Agency.

8           (6) HOMELAND SECURITY ENTERPRISE.—The  
9           term “Homeland Security Enterprise” has the  
10          meaning given the term in section 2200 of the  
11          Homeland Security Act of 2002 (6 U.S.C. 650).

12          (7) INCIDENT.—The term “incident” has the  
13          meaning given the term in section 2200 of the  
14          Homeland Security Act of 2002 (6 U.S.C. 650).

15          (8) INFORMATION SHARING.—The term “infor-  
16          mation sharing” means the bidirectional sharing of  
17          timely and relevant information concerning a cyber-  
18          security threat posed by a State-sponsored cyber  
19          actor of the People’s Republic of China to United  
20          States critical infrastructure.

21          (9) INTELLIGENCE COMMUNITY.—The term  
22          “intelligence community” has the meaning given the  
23          term in section 3(4) of the National Security Act of  
24          1947 (50 U.S.C. 3003(4)).

1           (10) LOCALITY.—The term “locality” means  
2 any local government authority or agency or compo-  
3 nent thereof within a State having jurisdiction over  
4 matters at a county, municipal, or other local gov-  
5 ernment level.

6           (11) SECRETARY.—The term “Secretary”  
7 means the Secretary of Homeland Security.

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

15           (13) SECTOR RISK MANAGEMENT AGENCY.—  
16 The term “Sector Risk Management Agency” has  
17 the meaning given the term in section 2200 of the  
18 Homeland Security Act of 2002 (6 U.S.C. 650).

19           (14) STATE.—The term “State” means any  
20 State of the United States, the District of Columbia,  
21 the Commonwealth of Puerto Rico, the Northern  
22 Mariana Islands, the United States Virgin Islands,  
23 Guam, American Samoa, and any other territory or  
24 possession of the United States.

1           (15) SYSTEMS.—The term “systems” means a  
2           combination of personnel, structures, facilities, infor-  
3           mation, materials, equipment, networks, or proc-  
4           esses, whether physical or virtual, integrated or  
5           interconnected for a specific purpose that enables  
6           the services, functions, or capabilities of an organi-  
7           zation.

8           (16) TASK FORCE.—The term “task force”  
9           means the joint interagency task force established  
10          under subsection (b).

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

14          (18) VOLT TYPHOON.—The term “Volt Ty-  
15          phoon” means the People’s Republic of China State-  
16          sponsored cyber actor described in the Cybersecurity  
17          and Infrastructure Security Agency cybersecurity  
18          advisory entitled “PRC State-Sponsored Actors  
19          Compromise and Maintain Persistent Access to U.S.  
20          Critical Infrastructure”, issued on February 07,  
21          2024, or any successor advisory.

22          (b) INTERAGENCY TASK FORCE.—Not later than 120  
23          days after the date of enactment of this Act, the Sec-  
24          retary, acting through the Director, in consultation with  
25          the Attorney General, the Director of the Federal Bureau

1 of Investigation, and the heads of appropriate Sector Risk  
2 Management Agencies as determined by the Director,  
3 shall establish a joint interagency task force to facilitate  
4 collaboration and coordination among the Sector Risk  
5 Management Agencies assigned a Federal role or responsi-  
6 bility in National Security Memorandum–22, issued April  
7 30, 2024 (relating to critical infrastructure security and  
8 resilience), or any successor document, to detect, analyze,  
9 and respond to the cybersecurity threat posed by State-  
10 sponsored cyber actors, including Volt Typhoon, of the  
11 People’s Republic of China by ensuring that the actions  
12 of those agencies are aligned and mutually reinforcing.

13 (c) CHAIRS.—

14 (1) CHAIRPERSON.—The Director, or the des-  
15 ignee of the Director, shall serve as the Chairperson  
16 of the task force.

17 (2) VICE CHAIRPERSON.—The Director of the  
18 Federal Bureau of Investigation, or the designee of  
19 the Director, shall serve as the Vice Chairperson of  
20 the task force.

21 (d) COMPOSITION.—

22 (1) IN GENERAL.—The task force shall consist  
23 of appropriate representatives of the departments  
24 and agencies specified in subsection (b) appointed by

1 the Chairperson in consultation with the Vice Chair-  
2 person.

3 (2) QUALIFICATIONS.—To materially assist in  
4 the activities of the task force, representatives under  
5 paragraph (1) shall be subject matter experts who  
6 have familiarity and technical expertise regarding cy-  
7 bersecurity, digital forensics, or threat intelligence  
8 analysis, or in-depth knowledge of the tactics, tech-  
9 niques, and procedures commonly used by State-  
10 sponsored cyber actors, including Volt Typhoon, of  
11 the People’s Republic of China.

12 (e) VACANCY.—Any vacancy occurring in the mem-  
13 bership of the task force shall be filled in the same manner  
14 in which the original appointment was made.

15 (f) ESTABLISHMENT FLEXIBILITY.—To avoid redun-  
16 dancy, the task force may coordinate with any preexisting  
17 task force, working group, or cross-intelligence effort with-  
18 in the Homeland Security Enterprise or the intelligence  
19 community that has examined or responded to the cyberse-  
20 curity threat posed by State-sponsored cyber actors, in-  
21 cluding Volt Typhoon, of the People’s Republic of China.

22 (g) TASK FORCE REPORTS; BRIEFING.—

23 (1) INITIAL REPORT.—Not later than 540 days  
24 after the establishment of the task force, the task  
25 force shall submit to the appropriate congressional

1 committees the first report containing the initial  
2 findings, conclusions, and recommendations of the  
3 task force.

4 (2) ANNUAL REPORT.—Not later than 1 year  
5 after the date of the submission of the initial report  
6 under paragraph (1), and annually thereafter for 5  
7 years, the task force shall submit to the appropriate  
8 congressional committees an annual report con-  
9 taining the findings, conclusions, and recommenda-  
10 tions of the task force.

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

13 (A) An assessment at the lowest classifica-  
14 tion feasible of the sector-specific risks, trends  
15 relating to incidents impacting sectors, and tac-  
16 tics, techniques, and procedures utilized by or  
17 relating to State-sponsored cyber actors, includ-  
18 ing Volt Typhoon, of the People’s Republic of  
19 China.

20 (B) An assessment of additional resources  
21 and authorities needed by Federal departments  
22 and agencies to better counter the cybersecurity  
23 threat posed by State-sponsored cyber actors,  
24 including Volt Typhoon, of the People’s Repub-  
25 lic of China.

1 (C) A classified assessment of the extent of  
2 potential destruction, compromise, or disruption  
3 to United States critical infrastructure by  
4 State-sponsored cyber actors, including Volt Ty-  
5 phoon, of the People's Republic of China in the  
6 event of a major crisis or future conflict be-  
7 tween the People's Republic of China and the  
8 United States.

9 (D) A classified assessment of the ability  
10 of the United States to counter the cybersecu-  
11 rity threat posed by State-sponsored cyber ac-  
12 tors, including Volt Typhoon, of the People's  
13 Republic of China in the event of a major crisis  
14 or future conflict between the People's Republic  
15 of China and the United States, including with  
16 respect to different cybersecurity measures and  
17 recommendations that could mitigate such a  
18 threat.

19 (E) A classified assessment of the ability  
20 of State-sponsored cyber actors, including Volt  
21 Typhoon, of the People's Republic of China to  
22 disrupt operations of the United States Armed  
23 Forces by hindering mobility across critical in-  
24 frastructure such as rail, aviation, and ports,  
25 including how such disruption would impair the

1 ability of the United States Armed Forces to  
2 deploy and maneuver forces effectively.

3 (F) A classified assessment of the eco-  
4 nomic and social ramifications of a disruption  
5 to 1 or multiple United States critical infra-  
6 structure sectors by State-sponsored cyber ac-  
7 tors, including Volt Typhoon, of the People's  
8 Republic of China in the event of a major crisis  
9 or future conflict between the People's Republic  
10 of China and the United States.

11 (G) Such recommendations as the task  
12 force may have for the Homeland Security En-  
13 terprise, the intelligence community, or critical  
14 infrastructure owners and operators to improve  
15 the detection and mitigation of the cybersecu-  
16 rity threat posed by State-sponsored cyber ac-  
17 tors, including Volt Typhoon, of the People's  
18 Republic of China.

19 (H) A one-time plan for an awareness  
20 campaign to familiarize critical infrastructure  
21 owners and operators with security resources  
22 and support offered by Federal departments  
23 and agencies to mitigate the cybersecurity  
24 threat posed by State-sponsored cyber actors,

1 including Volt Typhoon, of the People's Repub-  
2 lic of China.

3 (4) BRIEFING.—Not later than 30 days after  
4 the date of the submission of each report under this  
5 subsection, the task force shall provide to the appro-  
6 priate congressional committees a classified briefing  
7 on the findings, conclusions, and recommendations  
8 of the task force.

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

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

17 (h) ACCESS TO INFORMATION.—

18 (1) IN GENERAL.—The Secretary, the Director,  
19 the Attorney General, the Director of the Federal  
20 Bureau of Investigation, and the heads of appro-  
21 priate Sector Risk Management Agencies, as deter-  
22 mined by the Director, shall provide to the task  
23 force such information, documents, analysis, assess-  
24 ments, findings, evaluations, inspections, audits, or  
25 reviews relating to efforts to counter the cybersecu-

1 rity threat posed by State-sponsored cyber actors,  
2 including Volt Typhoon, of the People's Republic of  
3 China as the task force considers necessary to carry  
4 out this section.

5 (2) RECEIPT, HANDLING, STORAGE, AND DIS-  
6 SEMINATION.—Information, documents, analysis, as-  
7 sessments, findings, evaluations, inspections, audits,  
8 and reviews described in this subsection shall be re-  
9 ceived, handled, stored, and disseminated only by  
10 members of the task force consistent with all appli-  
11 cable statutes, regulations, and Executive orders.

12 (3) SECURITY CLEARANCES FOR TASK FORCE  
13 MEMBERS.—No member of the task force may be  
14 provided with access to classified information under  
15 this section without the appropriate security clear-  
16 ances.

17 (i) TERMINATION.—The task force, and all the au-  
18 thorities of this section, shall terminate on the date that  
19 is 60 days after the final briefing required under sub-  
20 section (g)(4).

21 (j) EXEMPTION FROM FACA.—Chapter 10 of title  
22 5, United States Code, shall not apply to the task force.

23 (k) EXEMPTION FROM PAPERWORK REDUCTION  
24 ACT.—Chapter 35 of title 44, United States Code (com-

- 1 monly known as the “Paperwork Reduction Act”), shall
- 2 not apply to the task force.