.....

(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 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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Strengthening Cyber Resilience Against State-Sponsored Threats Act''.

SEC. 2. INTERAGENCY TASK FORCE AND REPORT ON THE TARGETING OF UNITED STATES CRITICAL INFRASTRUCTURE BY PEOPLE'S REPUBLIC OF CHINA STATE-SPONSORED CYBER ACTORS.

(a) INTERAGENCY TASK FORCE.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, in consultation with the Attorney General, the Director of the Federal Bureau of Investigation, and the heads of appropriate Sector Risk Management Agencies as determined by the Director of CISA, shall establish a joint interagency task force (in this section referred to as the ''task force'') to facilitate collaboration and coordination among the Sector Risk Management Agencies assigned a Federal role or responsibility in National Security Memorandum–22, issued April 30, 2024 (relating to critical infrastructure security and resilience), or any successor document, to detect, analyze, and respond to the cybersecurity threat posed by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China by ensuring that

such agencies' actions are aligned and mutually reinforcing.

(b) CHAIRS.—

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

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

(c) COMPOSITION.—

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

(2) QUALIFICATIONS.—To materially assist in the activities of the task force, representatives under paragraph (1) should be subject matter experts who have familiarity and technical expertise regarding cybersecurity, digital forensics, or threat intelligence analysis, or in-depth knowledge of the tactics, techniques, and procedures (TTPs) commonly used by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(d) VACANCY.—Any vacancy occurring in the membership of the task force shall be filled in the same manner in which the original appointment was made.

(e) ESTABLISHMENT FLEXIBILITY.—To avoid redundancy, the task force may coordinate with any preexisting task force, working group, or cross-intelligence effort within the Homeland Security Enterprise or the intelligence community that has examined or responded to the cybersecurity threat posed by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(f) TASK FORCE REPORTS; BRIEFING.—

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

(2) ANNUAL REPORT.—Not later than one year after the date of the submission of the initial report under paragraph (1) and annually thereafter for five years, the task force shall submit to the appropriate congressional committees an annual report containing the findings, conclusions, and recommendations of the task force.

(3) CONTENTS.—The reports under this subsection shall include the following:

(A) An assessment at the lowest classification feasible of the sector-specific risks, trends relating to incidents impacting sectors, and tactics, techniques, and procedures utilized by or relating to state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(B) An assessment of additional resources and authorities needed by Federal departments and agencies to better counter the cybersecurity threat posed by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China .

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

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

rity threat posed by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China in the event of a major crisis or future conflict between the People's Republic of China and the United States, including with respect to different cybersecurity measures and recommendations that could mitigate such a threat.

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

(F) A classified assessment of the economic and social ramifications of a disruption to one or multiple United States critical infrastructure sectors by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China in the event of a major crisis or future conflict between the People's Republic of China and the United States.

(G) Such recommendations as the task force may have for the Homeland Security Enterprise, the intelligence community, or critical infrastructure owners and operators to improve the detection and mitigation of the cybersecurity threat posed by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

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

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

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

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

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

(g) ACCESS TO INFORMATION.—

(1) IN GENERAL.—The Secretary of Homeland Security, the Director of CISA, the Attorney General, the Director of the Federal Bureau of Investigation, and the heads of appropriate Sector Risk Management Agencies, as determined by the Director of CISA, shall provide to the task force such information, documents, analysis, assessments, findings, evaluations, inspections, audits, or reviews relating to efforts to counter the cybersecurity threat posed by state-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China as the task force considers necessary to carry out this section.

(2) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information, documents, analysis, assessments, findings, evaluations, inspections, audits, and reviews described in this subsection shall be received, handled, stored, and disseminated only by

members of the task force consistent with all applicable statutes, regulations, and executive orders.

(3) SECURITY CLEARANCES FOR TASK FORCE MEMBERS.—No member of the task force may be provided with access to classified information under this section without the appropriate security clearances.

(h) TERMINATION.—The task force, and all the authorities of this section, shall terminate on the date that is 60 days after the final briefing required under subsection (h)(4).

(i) EXEMPTION FROM FACA.—Chapter 10 of title 5, United States Code (commonly referred to as the ''Federal Advisory Committee Act''), shall not apply to the task force.

(j) EXEMPTION FROM PAPERWORK REDUCTION ACT.—Chapter 35 of title 44, United States Code (commonly known as the ''Paperwork Reduction Act''), shall not apply to the task force.

(k) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

Committee on Intelligence of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Judiciary, and the Select Committee on Intelligence of the Senate.

(2) ASSETS.—The term ''assets'' means a person, structure, facility, information, material, equipment, network, or process, whether physical or virtual, that enables an organization's services, functions, or capabilities.

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

(4) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

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

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

(7) INFORMATION SHARING.—The term ''information sharing'' means the bidirectional sharing of timely and relevant information concerning a cybersecurity threat posed by a state-sponsored cyber actor of the People's Republic of China to United States critical infrastructure.

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

(9) LOCALITY.—The term ''locality'' means any local government authority or agency or component thereof within a State having jurisdiction over matters at a county, municipal, or other local government level.

(10) SECTOR.—The term ''sector'' means a collection of assets, systems, networks, entities, or organizations that provide or enable a common function for national security (including national defense and continuity of Government), national economic security, national public health or safety, or any combination thereof.

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

(12) STATE.—The term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(13) SYSTEMS.—The term ''systems'' means a combination of personnel, structures, facilities, information, materials, equipment, networks, or processes, whether physical or virtual, integrated or interconnected for a specific purpose that enables an organization's services, functions, or capabilities.

(14) UNITED STATES.—The term ''United States'', when used in a geographic sense, means any State of the United States.

(15) VOLT TYPHOON.—The term ''Volt Typhoon'' means the People's Republic of China state-sponsored cyber actor described in the Cybersecurity and Infrastructure Security Agency cybersecurity advisory entitled ''PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S.

Critical Infrastructure'', issued on February 07, 2024, or any successor advisory.