119TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
119–230

STRENGTHENING CYBER RESILIENCE AGAINST STATE-SPONSORED THREATS ACT

AUGUST 15, 2025.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GARBARINO, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 2659]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 2659) 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, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

H.R. 2659, the "Strengthening Cyber Resilience Against State-Sponsored Threats Act," directs the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), in consultation with the Attorney General, the Director of the Federal Bureau of Investigation (FBI), and the heads of appropriate Sector Risk Management Agencies (SRMAs), to establish an interagency task force to facilitate coordination to respond to the cybersecurity threat posed by state-sponsored cyber actors of the People's Republic of China (PRC). Additionally, over a six-year period, the task force will be required to submit an annual report to the appropriate congressional committees on the targeting of United States critical infrastructure by PRC state-sponsored cyber actors.

BACKGROUND AND NEED FOR LEGISLATION

In recent years, the PRC has significantly escalated its malicious cyber operations targeting the United States. Whether it is compromising power grids or water systems, infiltrating telecommunications infrastructure, or probing vulnerabilities in financial networks, the PRC's state-sponsored cyber operations continue to pose a direct threat to U.S. national security.[1] The PRC's state-sponsored cyber actors, including Volt Typhoon and Salt Typhoon, have not only refined their techniques but have also broadened their objectives, encompassing intelligence gathering, economic espionage, and the capability to conduct damaging cyberattacks in times of geopolitical tension.[2]

Despite widespread recognition of the threat posed by PRC state-sponsored cyber actors, the U.S. government's response has been fragmented and ultimately insufficient. Federal agencies such as the Department of Homeland Security (DHS), CISA, and the FBI have all made efforts to detect and mitigate the impacts of these cyber operations, but they continue to operate in silos. These agencies have often lacked the resources and coordination necessary to fully understand the scope of the threat, share intelligence in real-time, and deploy effective countermeasures. The disjointed nature of these efforts has enabled PRC-sponsored cyber actors to go undetected for extended periods or, when detected, has exploited bureaucratic inefficiencies to evade meaningful consequences.

For instance, the PRC state-sponsored cyber actor known as Volt Typhoon has specialized in stealthy, long-term espionage operations that target key critical infrastructure sectors such as energy, telecommunications, transportation, and water systems. Volt Typhoon uses "living off the land" techniques, which has enabled the threat actor to go undetected within U.S. critical infrastructure systems for multiple years.[3] Additionally, Volt Typhoon has pre-positioned itself to move laterally—and easily—between information

---

[1] Max Colchester and Daniel Michaels, "*Scale of Chinese Spying Overwhelms Western Governments*," WSJ, (Oct. 14, 2024), https://www.wsj.com/politics/national-security/scale-of-chinese-spying-overwhelms-western-governments-6ae644d2?mod=china_more_article_pos1.

[2] Christopher Wray, Director, Federal Bureau of Investigation. *The CCP Cyber Threat to the American Homeland and National Security*. Testimony before the House Select Committee on China, (Jan. 24, 2024).

[3] CISA. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Cybersecurity Advisory (Feb. 07, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

technology (IT) and operational technology (OT) networks to cause disruption in the event of a conflict with the United States.[4]

Volt Typhoon's success to date is due in part to the vast and interconnected nature of U.S. networks, and vulnerabilities inherent in often outdated infrastructure. Today, most U.S. critical infrastructure is owned or operated by the private sector, meaning strong public-private partnerships are imperative for ensuring its resiliency.[5] This creates challenges for coordinating an effective U.S. government response. Given the number of government stakeholders that are involved—including CISA, the FBI, the intelligence community, and SRMAs—the U.S. government must streamline its own information sharing to work effectively with private sector owners and operators.

Whether dealing with Volt Typhoon or other PRC state-sponsored cyber actors, the U.S. response has been largely reactive, which is insufficient for confronting persistent and well-resourced PRC state-sponsored cyber operations. Given the magnitude of the PRC cyber threat, there is an urgent need for legislation that establishes an interagency task force dedicated solely to addressing the activities of PRC state-sponsored cyber actors. Such a task force would provide the structure and authority necessary to coordinate a comprehensive U.S. response. By bringing together representatives from CISA, the FBI, and other relevant entities, the task force would ensure that intelligence is shared effectively, vulnerabilities are identified and mitigated, and proactive strategies are developed to protect U.S. interests.

To ensure accountability and transparency, the task force would be required to submit an annual, comprehensive report to the appropriate congressional committees. This report will provide detailed information on the targeting of U.S. critical infrastructure by PRC cyber actors, including data on the number of incidents, the sectors affected, and the nature of the attacks. Additionally, the report will outline the steps taken by the task force to mitigate these threats, as well as any challenges or obstacles encountered. By mandating this annual report, Congress will ensure that the task force remains focused on its mission, while also providing lawmakers with the information necessary to adapt and refine U.S. cybersecurity policy in response to the evolving threat landscape.

The annual report would also serve as a critical tool for enhancing public awareness of the threat posed by PRC cyber actors. While much of the task force's work would remain classified, the report will include unclassified sections that inform the American public and private sector stakeholders about the risks to U.S. critical infrastructure and the steps taken to address them. This would promote greater collaboration between the government and the private sector.

HEARINGS

The Committee held the following hearing in the 119th Congress that informed H.R. 2659:

---

[4] *Id.*

[5] Tina Won Sherman, Director, Homeland Security and Justice. *Critical Infrastructure Protection: DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure*. Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, Committee on Homeland Security, House of Representatives, (Apr. 06, 2022).

On January 22, 2025, the Committee on Homeland Security held a hearing entitled, "Unconstrained Actors: Assessing Global Cyber Threats to the Homeland." Members heard testimony from the following witnesses: Mr. Adam Meyers, Senior Vice President of Counter Adversary Operations, CrowdStrike; Rear Admiral Mark Montgomery, USN, (ret.), Senior Director of the Center on Cyber and Technology Innovation, Foundation for Defense of Democracies; Mr. Brandon Wales, Vice President of Cybersecurity Strategy, SentinelOne; and Ms. Kemba Walden, President, Paladin Global Institute, who testified as a private citizen.

COMMITTEE CONSIDERATION

The Committee met on Wednesday, April 9, 2025, a quorum being present, to consider H.R. 2659 and ordered the measure to be favorably reported to the House.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 2659.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures contained in the cost estimate prepared by the Director of the Congressional Budget Office.

H.R. 2659, Strengthening Cyber Resilience Against State-Sponsored Threats Act

As ordered reported by the House Committee on Homeland Security on April 9, 2025

By Fiscal Year, Millions of Dollars	2025	2025-2030	2025-2035
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	5	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2036?	No	Statutory pay-as-you-go procedures apply?	No
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2036?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

H.R. 2659 would establish an interagency task force to detect, analyze, and respond to cybersecurity threats from state-sponsored actors. Under the bill, the task force would publish a list of federal resources available to help safeguard information technology systems at critical infrastructure facilities. The bill also would require the task force to report annually to the Congress on its findings and actions.

The task force would consist of representatives from federal agencies, including the Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation. Using information about the cost of similar efforts, CBO estimates that implementing H.R. 2659 would cost $5 million over the 2025–2030 period for staff salaries, travel, and other administrative expenses to operate the task force; satisfying the reporting requirements would cost less than $500,000. Such spending would be subject to the availability of appropriated funds.

The costs of the legislation, detailed in Table 1, fall within budget function 050 (national defense).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 2659

	By fiscal year, millions of dollars—						
	2025	2026	2027	2028	2029	2030	2025–2030
Estimated Authorization	*	1	1	1	1	1	5
Estimated Outlays	*	1	1	1	1	1	5

* = between zero and $500,000.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Christina Hawley Anthony, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act of 1995.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 2659 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 2659 is 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.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO THE LEGISLATIVE BRANCH

The Committee finds that H.R. 2659 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section states that the Act may be cited as the "Strengthening Cyber Resilience Against State-Sponsored Threats Act."

Section 2. Interagency task force and report on the targeting of United States Critical Infrastructure by People's Republic of China State-Sponsored Cyber Actors

This section directs the Secretary of Homeland Security, acting through the Director of CISA, in consultation with the Attorney General, the Director of the FBI, and the heads of appropriate SRMAs, to establish an interagency task force to facilitate collaboration and coordination among the SRMA's 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 (PRC).

Furthermore, this section designates the Director of CISA as the chair of the task force and the FBI Director as the vice-chair. The task force will be composed of representatives from relevant federal departments and agencies. Representatives must possess subject matter expertise in areas such as cybersecurity, digital forensics, threat intelligence analysis, and the tactics, techniques, and procedures (TTPs) commonly used by PRC state-sponsored actors like Volt Typhoon and Salt Typhoon.

To prevent redundancy, this section provides flexibility for the task force to coordinate with existing groups or efforts that have already examined or responded to similar cybersecurity threats. This ensures that resources are efficiently allocated, and that duplication of efforts is minimized.

Under this section, the task force is also required to report its findings to Congress. The initial report must be submitted within 540 days of the task force's establishment, with annual reports to follow for the next five years. These reports will assess sector-specific risks, identify trends in cyber incidents, and provide insights into the TTPs used by state-sponsored actors. The reports will also address the potential impact on U.S. critical infrastructure and provide recommendations for improving defenses against these threats. Some portions of the reports, especially those related to sensitive intelligence, will be classified. However, each report will include an unclassified executive summary that will be publicly available on the Department of Homeland Security's website.

In addition to regular reports, the task force is required to deliver classified briefings to Congress within 30 days of each report submission. These briefings will allow for deeper discussion on the task force's findings and recommendations.

This section clarifies that the task force will exist only as long as necessary to fulfill its purpose. It will terminate 60 days after delivering its final classified briefing to Congress. This ensures that the task force remains focused and does not become a permanent entity. Importantly, the task force is exempt from the Federal Advisory Committee Act (FACA) and the Paperwork Reduction Act, allowing it to operate with greater flexibility and without procedural delays.

Finally, this section provides clear definitions of key terms, such as "critical infrastructure," and "cybersecurity threat," among others. These definitions are intended to align with existing legal frameworks and provide clarity for how the task force should operate.

○