

HR 2659

Strengthening Cyber Resilience Against State-Sponsored Threats Act

Congress: 119 (2025–2027, Current)

Chamber: House

Policy Area: Science, Technology, Communications

Introduced: Apr 7, 2025

Current Status: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governm

Latest Action: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Nov 18, 2025)

Official Text: <https://www.congress.gov/bill/119th-congress/house-bill/2659>

Sponsor

Name: Rep. Ogles, Andrew [R-TN-5]

Party: Republican • **State:** TN • **Chamber:** House

Cosponsors (4 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Garbarino, Andrew R. [R-NY-2]	R · NY		Apr 7, 2025
Rep. Green, Mark E. [R-TN-7]	R · TN		Apr 7, 2025
Rep. Lee, Laurel M. [R-FL-15]	R · FL		Apr 7, 2025
Rep. Moolenaar, John R. [R-MI-2]	R · MI		Apr 7, 2025

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Nov 18, 2025
Homeland Security Committee	House	Referred to	Apr 7, 2025

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

Bill	Relationship	Last Action
119 S 4565	Related bill	May 19, 2026: Read twice and referred to the Committee on Homeland Security and Governmental Affairs.

Strengthening Cyber Resilience Against State-Sponsored Threats Act

The bill creates a joint interagency task force to facilitate agency collaboration on efforts to respond to Chinese state-sponsored cyber actors, including Volt Typhoon.

The task force must be established and led by the Cybersecurity and Infrastructure Security Agency (CISA), an agency within the Department of Homeland Security (DHS). The task force must facilitate collaboration and coordination among the Sector Risk Management Agencies (SRMAs) specified in the President's National Security Memorandum- 22 (e.g., the Department of Defense, the Department of Energy, and the Department of Agriculture) to detect, analyze, and respond to Chinese state-sponsored cyber actors by ensuring that such agencies' actions are aligned and mutually reinforcing.

The bill directs DHS, CISA, the Department of Justice, the Federal Bureau of Investigation, and specified SRMAs to provide the task force with analysis, inspections, audits, and other relevant information necessary for the task force to carry out its responsibilities. The production and use of information must comply with all applicable statutes, regulations, and executive orders, and task force members must have appropriate security clearances to access classified information.

The task force must provide annual reports and briefings to Congress detailing its assessment of cyber threats and recommendations to improve the detection and mitigation of the cybersecurity threat posed by Chinese state-sponsored cyber actors.

The first report must be provided no later than 540 days after the establishment of the task force, and additional reports must be provided annually thereafter for six years.

Actions Timeline

- **Nov 18, 2025:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
- **Nov 17, 2025:** Mr. Garbarino moved to suspend the rules and pass the bill.
- **Nov 17, 2025:** Considered under suspension of the rules. (consideration: CR H4682-4685)
- **Nov 17, 2025:** DEBATE - The House proceeded with forty minutes of debate on H.R. 2659.
- **Nov 17, 2025:** At the conclusion of debate, the Yeas and Nays were demanded and ordered. Pursuant to the provisions of clause 8, rule XX, the Chair announced that further proceedings on the motion would be postponed.
- **Nov 17, 2025:** Considered as unfinished business. (consideration: CR H4692)
- **Nov 17, 2025:** Passed/agreed to in House: On motion to suspend the rules and pass the bill Agreed to by the Yeas and Nays: (2/3 required): 402 - 8 (Roll no. 287). (text: CR H4682-4684)
- **Nov 17, 2025:** On motion to suspend the rules and pass the bill Agreed to by the Yeas and Nays: (2/3 required): 402 - 8 (Roll no. 287). (text: CR H4682-4684)
- **Nov 17, 2025:** Motion to reconsider laid on the table Agreed to without objection.
- **Nov 17, 2025:** Considered under suspension of the rules.
- **Nov 17, 2025:** Considered as unfinished business.
- **Nov 17, 2025:** Passed/agreed to in House: On motion to suspend the rules and pass the bill Agreed to by the Yeas and Nays: (2/3 required): 402 - 8 (Roll no. 287).
- **Nov 17, 2025:** On motion to suspend the rules and pass the bill Agreed to by the Yeas and Nays: (2/3 required): 402 - 8 (Roll no. 287).
- **Aug 15, 2025:** Reported by the Committee on Homeland Security. H. Rept. 119-230.
- **Aug 15, 2025:** Placed on the Union Calendar, Calendar No. 188.
- **Apr 9, 2025:** Subcommittee on Cybersecurity and Infrastructure Protection Discharged
- **Apr 9, 2025:** Committee Consideration and Mark-up Session Held
- **Apr 9, 2025:** Ordered to be Reported by Voice Vote.
- **Apr 7, 2025:** Introduced in House
- **Apr 7, 2025:** Referred to the House Committee on Homeland Security.
- **Apr 7, 2025:** Referred to the Subcommittee on Cybersecurity and Infrastructure Protection.

LegiList

CONGRESS, MADE CLEAR.

Search Every Federal Bill, Law, and Vote

LegiList is the fastest way to research Congress. Track any bill from introduction to enactment, see how every legislator voted, follow committee activity, and read the full text of every bill — all in one place, always up to date.

legilist.com

Free Course: Learn How Congress Actually Works

LegiList Learn is a free, self-paced course that walks through the entire legislative process — from drafting a bill to a presidential signature. Seven modules, plain language, no politics. Earn a certificate when you finish.

legilist.com/learn

Developer API: Build Apps on Legislative Data

The LegiList API gives developers direct access to bills, votes, legislators, committees, and more. Start free with 1,000 requests per day — no credit card required. Upgrade to Pro when you need to scale.

legilist.com/api

Public data belongs to the public. — legilist.com