S 2875

Cyber Incident Reporting Act of 2021

Congress: 117 (2021–2023, Ended)
Chamber: Senate
Policy Area: Science, Technology, Communications
Introduced: Sep 28, 2021
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 633.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 633. (Dec 13, 2022)
Official Text: https://www.congress.gov/bill/117th-congress/senate-bill/2875

Sponsor

Name: Sen. Peters, Gary C. [D-MI]
Party: Democratic • **State:** MI • **Chamber:** Senate

Cosponsors (3 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Portman, Rob [R-OH]	R · OH		Sep 28, 2021
Sen. Sinema, Kyrsten [D-AZ]	D · AZ		Oct 20, 2021
Sen. Tillis, Thomas [R-NC]	R · NC		Oct 20, 2021

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Reported By	Dec 13, 2022

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of Dec 13, 2022)

Cyber Incident Reporting Act of 2021

This bill requires reporting and other actions to address cybersecurity incidents, including ransomware attacks.

Entities that own or operate critical infrastructure must report cyber incidents and ransom payments within specified time frames while other entities may voluntarily report incidents. The Cybersecurity and Infrastructure Security Agency (CISA) must establish an office to receive and analyze such reports.

The bill limits the use and disclosure of reported information. The information may be shared (subject to protections) with federal agencies or to address cybersecurity threats. However, shared information may not be used as a basis for certain regulatory enforcement. Additionally, an entity may not be liable for submitting required reports. Further, reports do not constitute waivers of applicable protections against disclosure (e.g., attorney-client privilege) and are not subject to laws governing release of federal records.

The bill authorizes CISA to take specified action (e.g., issuing subpoenas) if an entity fails to submit a required report. CISA may share subpoenaed information with a regulator or the Department of Justice for regulatory enforcement or criminal prosecution.

A federal agency must share any information it receives about cyber attacks with CISA.

The bill also establishes (1) an interagency council to standardize federal reporting of cybersecurity threats, (2) a task force on ransomware attacks, and (3) a pilot program to identify information systems vulnerable to ransomware attacks.

Actions Timeline

- **Dec 13, 2022:** Committee on Homeland Security and Governmental Affairs. Reported by Senator Peters with an amendment in the nature of a substitute. With written report No. 117-249.
- **Dec 13, 2022:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 633.
- **Oct 6, 2021:** Committee on Homeland Security and Governmental Affairs. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Sep 28, 2021:** Introduced in Senate
- **Sep 28, 2021:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.