Congressional Budget Office
Cost Estimate

November 30, 2021

At a Glance

S. 2875, Cyber Incident Reporting Act of 2021

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on October 6, 2021

By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	*	*
Revenues	0	*	*
Increase or Decrease (-) in the Deficit	0	*	*
Spending Subject to Appropriation (Outlays)	3	55	not estimated

Statutory pay-as-you-go procedures apply?	Yes	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	Yes, Under Threshold
		Contains private-sector mandate?	Yes, Under Threshold

* = between -$500,000 and $500,000.

The bill would

- Require operators of critical infrastructure to report cyber attacks and ransom payments
- Establish a program office to receive and analyze reports on cyber incidents
- Create a pilot program to warn federal agencies and nonfederal entities that are vulnerable to ransomware
- Impose intergovernmental and private-sector mandates by requiring the owners and operators of critical infrastructure to file reports about cyber incidents and ransom payments and to retain relevant data. The bill also would preempt state, local, and tribal public disclosure laws

Estimated budgetary effects would mainly stem from

- Implementing new cyber incident reporting processes
- Identifying information systems that have security vulnerabilities
- Collecting civil and criminal fines from entities that do not comply with disclosure requirements

Areas of significant uncertainty include

- Predicting the annual number of cyber incidents reported to the federal government
- Anticipating how often the federal government would impose fines and penalties

Detailed estimate begins on the next page.

Bill Summary

S. 2875 would require operators of critical infrastructure (such as utilities providers) to report to the federal government about cyber attacks on their systems and about ransom payments they make to hackers. The bill would establish an office under the Cybersecurity and Infrastructure Security Agency (CISA) to receive and analyze such reports and to inform those operators of the new reporting requirements. The bill also would authorize CISA to fine critical infrastructure operators that fail to report cyber incidents.

S. 2875 also would expand CISA's authority to share information about threats of ransomware attacks with federal agencies and nonfederal entities. Ransomware attacks are attacks on information technology systems to extort a ransom payment from victims. In the rare instances when CISA would not be able to identify the owners of computers or devices that are vulnerable to ransomware threats, the bill would authorize the agency to compel Internet service providers (ISPs) to disclose the identity of owners of such technology.

Estimated Federal Cost

The estimated budgetary effects of S. 2875 are shown in Table 1. The costs of the legislation fall within budget function 050 (national defense).

Table 1.
Estimated Budgetary Effects of S. 2875

	By Fiscal Year, Millions of Dollars					
	2022	2023	2024	2025	2026	2022-2026
Cyber Incident Review Office						
Estimated Authorization	2	6	11	11	12	42
Estimated Outlays	2	6	11	11	12	42
Ransomware Vulnerability Warning Program						
Estimated Authorization	1	2	2	2	2	9
Estimated Outlays	1	2	2	2	2	9
Outreach Campaign						
Estimated Authorization	0	2	2	0	0	4
Estimated Outlays	0	2	2	0	0	4
Total Changes						
Estimated Authorization	3	10	15	13	14	55
Estimated Outlays	3	10	15	13	14	55

In addition to the budgetary effects shown above, CBO estimates that enacting S. 2875 would have insignificant effects on direct spending and revenues and would decrease the deficit by an insignificant amount over the 2022-2031 period.

Basis of Estimate

For this estimate, CBO assumes that S. 2875 will be enacted in early fiscal year 2022 and that regulations for cyber incident reporting would take effect in fiscal year 2023. Outlays are based on historical spending patterns for existing or similar programs.

Under current law, nonfederal entities can voluntarily report cyber incidents to CISA. Using available data from cybersecurity firms, CBO anticipates that CISA would receive several hundred additional reports of cyber incidents per year as a result of the mandatory reporting requirements of the bill. On the basis of information from CISA, CBO expects that the costs to implement the bill would be limited to the salaries and benefits of the new staff necessary to carry out the bill's cyber incident and ransomware reporting requirements. The agency indicates it would not need new information technology systems to do so.

Spending Subject to Appropriation

CBO estimates that implementing the bill would cost $55 million over the 2022-2026 period. Such spending would be subject to the availability of appropriated funds.

Cyber Incident Review Office. S. 2875 would create a new office to receive and respond to the reports of cyber incidents. Using information about the current number of cyber incidents expected to occur in the United States each year, CBO anticipates that the new office would manage approximately 500 reports annually. On the basis of information from CISA about the workload requirements of similar expansions of the agency's responsibilities, CBO expects that each analyst in the Cyber Incident Review Office would manage about 10 incident reports per year. CBO estimates that enforcing the notification requirement and managing the reported information would require 50 full-time equivalent employees, at an average annual rate of about $187,000 per employee for compensation and benefits. CBO expects that CISA would begin hiring those employees in 2022 and that all personnel would be hired by 2024. On that basis and accounting for the effects of anticipated inflation, CBO estimates that salaries and benefits expenses of those employees would total $42 million over the 2022-2026 period.

Ransomware Vulnerability Warning Program. S. 2875 would establish a new program to identify information technology systems that are vulnerable to ransomware attacks and inform the owners of those systems about those vulnerabilities. Using information about similar efforts, CBO expects that implementing the program would require 10 full-time equivalent employees beginning in 2022, at an average annual rate of about $187,000 per employee. The salaries and benefits expenses of those employees would total $9 million over the 2022-2026 period, CBO estimates.

Outreach Campaign. S. 2875 would require CISA to inform affected entities of new regulations for cyber incident reporting that are required under the bill. Based on the costs of

similar public outreach campaigns at CISA, CBO estimates that advertising contracts and publication materials would cost about $2 million annually in the first two years after enactment and $4 million over the 2023-2024 period.

Direct Spending
S. 2875 would authorize CISA to issue administrative subpoenas to critical infrastructure operators that do not provide cyber incident reports in a timely manner. The bill also would authorize CISA to issue administrative subpoenas to compel ISPs to disclose the identity of owners of critical infrastructure that are vulnerable to ransomware threats.

Entities that do not comply with subpoenas could be subject to civil and criminal penalties; therefore, the government might collect additional fines under the legislation. Civil fines are recorded in the budget as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent without further appropriation. CBO expects that few critical infrastructure operators would be fined for defying subpoenas. Thus, both revenues and direct spending would increase by insignificant amounts over the 2022-2031 period. On net, enacting the bill would reduce the deficit by an insignificant amount, CBO estimates.

Uncertainty
Areas of uncertainty in this estimate include accurately predicting CISA's additional workload. Nonfederal entities are not currently required to report cyber incidents, and the bill would provide CISA with broad rulemaking authority to define reportable incidents. The budgetary effects of the bill would be moderately larger or smaller than this estimate depending on how the actual number of incidents reported to CISA differs from CBO's estimate of 500 annual reports.

The budgetary effects of the bill also would depend on the number and amounts of fines imposed under the bill's provisions. If more fines were collected than CBO expects, both direct spending and revenues would be higher than estimated.

Pay-As-You-Go Considerations:

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting S. 2875 would have insignificant effects on direct spending and revenues and would, on net, reduce the deficit by insignificant amounts.

Increase in Long-Term Deficits: None.

Mandates:

S. 2875 would impose intergovernmental and private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA). CBO estimates that the aggregate cost of those mandates would not exceed the thresholds established in UMRA for intergovernmental and private-sector mandates ($85 million and $170 million in 2021, respectively, adjusted annually for inflation).

The bill would impose a mandate on owners and operators of critical infrastructure by requiring those entities to file reports with CISA about cyber incidents and ransom payments. The bill also would require entities filing reports to retain all information related to a reported incident or payment. Because public and private entities own critical infrastructure like utilities and public safety networks, the bill would impose an intergovernmental and private-sector mandate. Several hundred entities would be required to file reports under the bill, but the information for those reports would be readily available and would not be expensive to provide. Consequently, CBO estimates the cost to comply with the mandate would be small and well below the thresholds established in UMRA.

The bill would preempt state, local, and tribal laws by exempting information contained in the reports of cyber incidents and ransom payments from any public disclosure laws. It also would prohibit non-federal regulators from using information obtained solely through those reports to regulate the lawful activities of reporting entities. CBO estimates these provisions would not result in additional spending or a loss of revenue.

Estimate Prepared By

Federal Costs: Aldo Prosperi

Mandates: Brandon Lever

Estimate Reviewed By

David Newman
Chief, Defense, International Affairs, and Veterans' Affairs Cost Estimates Unit

Kathleen FitzGerald
Chief, Public and Private Mandates Unit

Leo Lex
Deputy Director of Budget Analysis

Theresa Gullo
Director of Budget Analysis