Congressional Budget Office
Cost Estimate

August 16, 2023

At a Glance

S. 2251, Cybersecurity Act of 2023

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 26, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	0	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	*	*
Spending Subject to Appropriation (Outlays)	0	735	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2034?	< $2.5 billion	Statutory pay-as-you-go procedures apply?	Yes
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	< $5 billion	**Mandate Effects**	
		Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

The bill would

- Update policies, procedures, and programs for information security at federal agencies
- Require all federal agencies to report significant cyber incidents on their networks
- Codify the responsibilities of the federal Chief Information Security Officer
- Direct the Cybersecurity and Infrastructure Security Agency to study cyber threats to rural hospitals

Estimated budgetary effects would mainly stem from

- Reporting and responding to cyber incidents at federal agencies
- Contracting with information security service companies
- Providing cyber incident response training to federal employees
- Hiring information security analysts
- Developing training resources for rural hospital employees

Areas of significant uncertainty include

- Anticipating the adoption schedules of new cybersecurity procedures and programs
- Predicting the staffing and contracting requirements of federal information security offices

Detailed estimate begins on the next page.

See also
CBO's Cost Estimates Explained, *CBO Describes Its Cost-Estimating Process*, *Glossary*

Bill Summary

The Federal Information Security Modernization Act (FISMA) provides a framework to protect government information operations against cybersecurity threats. S. 2251 would update FISMA to require federal agencies to report all cybersecurity incidents and conduct standardized cybersecurity procedures on a regular basis.

S. 2251 also would require the Cybersecurity and Infrastructure Security Agency (CISA) to study cybersecurity threats facing rural hospitals. Under the bill, CISA would provide the Congress with recommendations to improve the recruitment and training of cyber professionals at rural hospitals. The bill also would require CISA to develop and disseminate information on cyber safety measures to employees of rural hospitals.

Estimated Federal Cost

The estimated budgetary effects of S. 2251 are shown in Table 1. The costs of the legislation fall within budget functions 050 (national defense) and 800 (general government).

Table 1.
Estimated Budgetary Effects of S. 2251

	By Fiscal Year, Millions of Dollars						
	2023	2024	2025	2026	2027	2028	2023-2028
Federal Information Security Modernization							
Estimated Authorization	0	75	125	175	225	230	830
Estimated Outlays	0	44	103	153	203	227	730
Rural Hospital Cybersecurity							
Estimated Authorization	0	1	1	1	1	1	5
Estimated Outlays	0	1	1	1	1	1	5
Total Changes							
Estimated Authorization	0	76	126	176	226	231	835
Estimated Outlays	0	45	104	154	204	228	735

In addition to the budgetary effects shown above, CBO estimates that enacting S. 2251 would have insignificant effects on direct spending and the deficit over the 2023-2033 period.

Basis of Estimate

For this estimate, CBO assumes that S. 2251 will be enacted early in fiscal year 2024. Outlays are based on historical spending patterns for existing or similar programs.

Spending Subject to Appropriation

CBO estimates that implementing the bill would cost $735 million over the 2023-2028 period. Such spending would be subject to the availability of appropriated funds.

Federal Information Security Modernization. Most of the provisions of S. 2251 would codify or expand current practices of the federal government. FISMA established regulations and guidelines for ensuring the effectiveness of security controls over information resources that support federal information security operations and assets. Specifically, FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems used or operated by each agency. The Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency develop policies, measures, standards, and guidelines for these purposes. Inspectors general perform independent evaluations of the information security programs and practices of individual agencies. Federal civilian agencies spent more than $10 billion on cybersecurity activities in fiscal year 2022.

CBO expects that implementing S. 2251 would require agencies to perform additional cybersecurity procedures to identify weaknesses in federal networks and report security incidents to CISA. CBO anticipates that agencies would hire additional personnel and contract with third-party entities to implement new data management and reporting requirements under S. 2251. Based on information from OMB and other agencies about the costs to administer similar policies, CBO estimates that the new and expanded activities under the legislation would increase current civilian cybersecurity expenses by 2 percent, or about $225 million annually when fully implemented. CBO expects that it would take about four years to reach that level of effort for the roughly 10,000 federal computer systems currently operating. CBO estimates that implementing those new requirements would increase costs by $44 million in 2024 and $730 million over the 2023-2028 period.

Rural Hospital Cybersecurity. Using information from CISA about studies, information sharing, and training efforts similar to those that the bill would require for rural hospitals, CBO anticipates that the agency would need two full-time employees to prepare the reports and to develop online training resources for rural hospital employees. CBO estimates that staff salaries and technology costs to publish instructional materials would total $5 million over the 2023-2028 period.

Direct Spending

Enacting the bill could affect direct spending by some federal agencies that are allowed to use fees, receipts from the sale of goods, and other collections to cover operating costs. CBO estimates that any net changes in direct spending by those agencies would be negligible because most of them can adjust amounts collected to reflect changes in operating costs.

Uncertainty

Areas of uncertainty in this estimate include predicting the implementation timeline at federal agencies. The budgetary effects of the bill could be significantly higher or lower than

CBO's estimate if the time needed to adopt new cybersecurity procedures and technology differs from CBO's estimate.

The budgetary effects of the bill also would depend on the number of additional employees that would be needed at OMB, CISA, and other federal agencies to satisfy the requirements of the bill. Costs would be moderately larger or smaller than this estimate depending on how the number of software analysts hired differs from CBO's estimate.

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 the bill would increase direct spending by less than $500,000 over the 2023-2033 period.

Increase in Long-Term Net Direct Spending and Deficits:

CBO estimates that enacting S. 2251 would not significantly increase net direct spending in any of the four consecutive 10-year periods beginning in 2034.

CBO estimates that enacting S. 2251 would not significantly increase on-budget deficits in any of the four consecutive 10-year periods beginning in 2034.

Mandates: None.

Previous CBO Estimate

On June 23, 2023, CBO transmitted a cost estimate for S. 1560, the Rural Hospital Cybersecurity Enhancement Act, as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on June 14, 2023. Title II of S. 2251 is similar to S. 1560 and CBO's estimates of their budgetary effects are the same.

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

Christina Hawley Anthony
Deputy Director of Budget Analysis

Estimate Approved By

Phillip L. Swagel
Director, Congressional Budget Office