Congressional Budget Office
Cost Estimate

May 22, 2023

At a Glance

H.R. 3286, Securing Open Source Software Act of 2023

As ordered reported by the House Committee on Homeland Security on May 17, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	42	not estimated

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

The bill would

- Require assessments of open-source software used by federal agencies
- Direct the Cybersecurity and Infrastructure Security Agency to hire open-source software analysts
- Require several reports and studies about the effectiveness of open-source software assessments

Estimated budgetary effects would mainly stem from

- Testing information systems for open-source software vulnerabilities
- Assessing federal network security
- Hiring open-source software analysts

Areas of significant uncertainty include

- Anticipating the contract costs of software assessments
- Predicting staffing requirements

Detailed estimate begins on the next page.

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

Bill Summary

H.R. 3286 would authorize the Cybersecurity and Infrastructure Security Agency (CISA) to improve the security of open-source software, or computer code that is publicly available for anyone to use or modify. The bill would require the agency to identify and mitigate vulnerabilities in open-source software used by federal agencies. Under the bill, CISA would conduct annual assessments of the security of commonly used open-source software.

Estimated Federal Cost

The estimated budgetary effects of H.R. 3286 are shown in Table 1. The costs of the legislation fall within budget function 050 (national defense).

Table 1.
Estimated Budgetary Effects of H.R. 3286

	By Fiscal Year, Millions of Dollars						
	2023	2024	2025	2026	2027	2028	2023-2028
Open-Source Software Assessments							
Estimated Authorization	0	0	6	6	6	6	24
Estimated Outlays	0	0	6	6	6	6	24
CISA Open-Source Staff							
Estimated Authorization	0	2	4	4	4	4	18
Estimated Outlays	0	2	4	4	4	4	18
Total Changes							
Estimated Authorization	0	2	10	10	10	10	42
Estimated Outlays	0	2	10	10	10	10	42

Basis of Estimate

For this estimate, CBO assumes that H.R. 3286 will be enacted in 2023 and that CISA would begin to implement most of the bill’s requirements in 2025.

CBO expects that the costs to implement H.R. 3286 would include the salaries and benefits of additional federal staff and procurement of new software. Outlays are based on historical spending patterns for existing or similar programs.

Spending Subject to Appropriation

CBO estimates that implementing the bill would cost $42 million over the 2023-2028 period. Such spending would be subject to the availability of appropriated funds.

Open-Source Software Assessments. CISA currently operates programs to identify and mitigate threats to federal information systems. H.R. 3286 would require CISA to assess open-source software used by the federal government for security vulnerabilities. Under the bill, CISA would review the supply chain histories of open-source applications to identify any potential cybersecurity vulnerabilities in the underlying code. CISA would be required to share its findings so that software users could remediate any weaknesses.

Using information from CISA, CBO expects that the agency would implement this program by procuring new software and tools capable of scanning for vulnerabilities in open-source code used by federal agencies. On the basis of similar acquisition programs, CBO estimates that the cost to acquire and annually update those tools would total $24 million over the 2023-2028 period.

CISA Open-Source Staff. H.R. 3286 would require CISA to publish a framework for the secure adoption and management of open-source software in the information networks and devices of federal, state, and private-sector entities. CISA also would provide information about vulnerabilities in open-source software. CBO anticipates that the framework and vulnerability assessments would be updated annually. CBO expects that CISA would need 20 open-source software analysts beginning in 2024 at an average annual cost of about $175,000 per employee. On that basis and accounting for the effects of anticipated inflation, CBO estimates that salaries and benefits of those employees would total $18 million over the 2023-2028 period.

Uncertainty

Areas of uncertainty in this estimate include predicting the acquisition timeline to support assessments at federal agencies and critical infrastructure operators. CBO anticipates that CISA would be able to procure and deploy the necessary software to assess federal open-source software in the 2023-2028 period. The budgetary effects of the bill could be millions of dollars higher or lower than CBO's estimate if the time needed to deploy these tools differs from CBO's estimate.

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

Pay-As-You-Go Considerations: None.

Increase in Long-Term Net Direct Spending and Deficits: None.

Mandates: None.

Previous CBO Estimate

On April 6, 2023, CBO transmitted a cost estimate for S. 917, the Securing Open Source Software Act of 2023, as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 29, 2023. The estimated cost of S. 917 is higher than the cost of H.R. 3286 because the former bill would authorize a federal pilot program that would not be authorized by the latter.

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

Chad Chirico
Deputy Director of Budget Analysis

Estimate Approved By

Phillip L. Swagel
Director, Congressional Budget Office