Congressional Budget Office
Cost Estimate

November 9, 2022

At a Glance

S. 4913, Securing Open Source Software Act of 2022

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on September 28, 2022

By Fiscal Year, Millions of Dollars	2023	2023-2027	2023-2032
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	2	275	not estimated

Statutory pay-as-you-go procedures apply?	No	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2033?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

The bill would

- Require assessments of open-source software used by federal agencies and critical infrastructure operators
- Establish program offices to manage secure open-source software at federal agencies
- Require 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 deployment schedules of hardware and software solutions
- Predicting the staffing requirements of federal open-source program offices

Detailed estimate begins on the next page.

See also *CBO's Cost Estimates Explained*, www.cbo.gov/publication/54437;
How CBO Prepares Cost Estimates, www.cbo.gov/publication/53519; and *Glossary*, www.cbo.gov/publication/42904.

Bill Summary

S. 4913 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 and critical infrastructure operators. CISA also would conduct annual assessments of the security of commonly used open-source software.

S. 4913 also would require federal agencies to establish open-source software program offices under their chief information security officers. The bill would direct agencies to develop policies for the safe deployment and management of open-source software on their information networks.

Estimated Federal Cost

The estimated budgetary effects of S. 4913 are shown in Table 1.

Table 1.
Estimated Budgetary Effects of S. 4913

	By Fiscal Year, Millions of Dollars					
	2023	2024	2025	2026	2027	2023-2027
Open-Source Software Assessments						
Estimated Authorization	*	90	50	50	30	220
Estimated Outlays	*	25	46	59	45	175
Open-Source Program Offices						
Estimated Authorization	0	12	18	26	26	82
Estimated Outlays	0	12	18	26	26	82
CISA Open-Source Staff						
Estimated Authorization	2	4	4	4	4	18
Estimated Outlays	2	4	4	4	4	18
Total Changes						
Estimated Authorization	2	106	72	80	60	320
Estimated Outlays	2	41	68	89	75	275

* = between zero and $500,000.

Basis of Estimate

For this estimate, CBO assumes that S. 4913 will be enacted by the end of 2022 and that CISA would begin to implement most of the bill’s requirements in 2024. On the basis of information from CISA, CBO expects that the agency would not offer cybersecurity assessments to critical infrastructure operators until after 2027.

CBO expects that the costs to implement S. 4913 would include the salaries and benefits of additional federal staff, procurement of new hardware systems, and service contracts with cybersecurity analytics firms. Outlays are based on historical spending patterns for existing or similar programs.

Spending Subject to Appropriation

CBO estimates that implementing the bill would cost $275 million over the 2023-2027 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. S. 4913 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 then publish 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 a new information technology system with the capability to scan federal networks for weaknesses in the components of open-source software. On the basis of similar acquisition programs, CBO estimates that acquiring that system would require appropriations of $190 million over the 2024-2026 period. CBO expects that beginning in 2027, CISA would subsequently contract with cybersecurity advisory companies to monitor data feeds, analyze results for potential weaknesses, provide vulnerability scans and remote penetration testing, and maintain the system, which would require annual appropriations of $30 million. Accounting for the time needed to complete deployment of the new system, CBO estimates that implementing those requirements would cost $175 million over the 2023-2027 period.

Open-Source Program Offices. S. 4913 would require the 24 federal agencies covered under the Chief Financial Officers Act to establish new offices to manage the use of secure open-source software. CBO expects the agencies covered under this bill would each require on average five analysts to develop policies, share best practices, and monitor open-source applications used by their agencies. CBO estimates that each analyst would earn an average annual rate of about $175,000 and that agencies would begin hiring those employees in 2024. On that basis and accounting for the effects of anticipated inflation, CBO estimates that salaries and benefits of those employees would total $82 million over the 2023-2027 period.

CISA Open-Source Staff. S. 4913 would require CISA to hire additional analysts with expertise in the development of secure open-source software. Within one year of enactment, CISA would be required to publish guidance for federal, state, and private-sector entities to securely adopt and manage open-source software in their information networks and devices. CISA also would identify and publish vulnerabilities in open-source software. CBO expects that CISA would hire 20 new open-source software analysts beginning in 2023 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 2023-2027 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 hardware and software to assess federal open-source software in the 2024-2026 period and that CISA would not likely be able to deploy a solution for critical infrastructure until after 2027. The budgetary effects of the bill could be tens of millions of dollars higher or lower than CBO's estimate if the time needed to deploy the system 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 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 hired open-source software analysts differs from CBO's estimate.

Pay-As-You-Go Considerations: None.

Increase in Long-Term Deficits: None.

Mandates: None.

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-Sector Mandates Unit

Leo Lex
Deputy Director of Budget Analysis

Theresa Gullo
Director of Budget Analysis