Calendar No. 674

117TH CONGRESS *2d Session*	SENATE	REPORT 117–275

CISA CYBER EXERCISE ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2993

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO ESTABLISH IN THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY THE NATIONAL CYBER EXERCISE PROGRAM, AND FOR OTHER PURPOSES

DECEMBER 19, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 674

117TH CONGRESS, *2d Session* | SENATE | REPORT 117–275

CISA CYBER EXERCISE ACT

DECEMBER 19, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2993]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2993) to amend the Homeland Security Act of 2002 to establish in the Cybersecurity and Infrastructure Security Agency the National Cyber Exercise Program, and for other purposes, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) currently engages in cyber resiliency exercises to effectively "provide stakeholders with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures."[1] CISA also developed and maintains the National Cyber Incident Response Plan (NCIRP), which defines the

[1] Cybersecurity and Infrastructure Security Agency, *Critical Infrastructure Exercises*, (accessed Dec. 7, 2022) (https://www.cisa.gov/critical-infrastructure-exercises).

roles and responsibilities for Federal agencies when responding to cyber incidents. S. 2993, *CISA Cyber Exercise Act*, would codify CISA's existing exercise work by requiring the establishment of a National Cyber Exercise Program that would also be required to evaluate the NCIRP. The program would also develop model exercises that public and private sector stakeholders can utilize to evaluate their cyber readiness.

II. Background and Need for the Legislation

Cyber attacks continue to increase in both frequency and consequence. Recent unprecedented cyberattacks targeting critical infrastructure have exposed significant vulnerabilities in the United States' networks, such as the Colonial Pipeline Company attack in May 2021 which caused a multi-day outage of the largest pipeline system for refined oil products in the U.S.[2] In the first half of 2021, there was a 125% increase in cyber attacks worldwide, with the United States accounting for 36% of those attacks.[3]

One of the most effective ways to enhance the security and resilience of critical infrastructure, and to ensure system defenders are able to effectively mitigate and respond to cyber attacks, is to conduct regular cyber exercises that test and evaluate critical infrastructure readiness.[4] CISA regularly conducts cybersecurity exercises with both government and private sector organizations to "enhance security and resilience of critical infrastructure."[5] These exercises are designed to "identify best practices, lessons learned, and areas for improvement in [cyber response] plans and procedures."[6] For example, CISA's Cyber Storm biennial exercises bring together the public and private sectors to "simulate discovery of and response to a significant cyber incident impacting the Nation's critical infrastructure."[7] These exercises help to assess and strengthen the nation's cyber preparedness and improve cyber incident response.[8]

In addition to its cyber exercise program, CISA, at the direction of Presidential Policy Directive–41, developed the NCIRP.[9] This plan "articulate[s] the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure."[10] The NCIRP is not a tactical plan for cyber incident response, rather, it is a framework for understanding how the government will provide resources to support operations. The NCIRP addresses an important role that the private sector, state and local governments, and multiple federal agencies play in re-

---

[2] Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity, New York Times (May 14, 2021, updated Jun. 8, 2021) (https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html).

[3] Accenture, *Triple digit increase in cyberattacks: What next?*, Accenture Cybersecurity Blog (Blog) (August 4, 2021) (https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks).

[4] Cybersecurity and Infrastructure Security Agency, Critical Infrastructure Exercises (https://www.cisa.gov/critical-infrastructure-exercises) (accessed Dec. 8, 2022).

[5] Cybersecurity and Infrastructure Security Agency, Cybersecurity Training and Exercises (https://www.cisa.gov/cybersecurity-training-exercises) (accessed Dec. 8, 2022).

[6] *Id.*

[7] Cybersecurity and Infrastructure Security Agency, Cyber Storm: Securing Cyber Space (https://www.cisa.gov/cyber-storm-securing-cyber-space) (accessed Dec. 8, 2022).

[8] *Id.*

[9] White House, *United States Cyber Incident Coordination* (PPD–41) (Jul. 26, 2016).

[10] *National Cyber Incident Response Plan*, Department of Homeland Security, (December 2016).

sponding to incidents and how the actions of all fit together to create an integrated response.[11]

To strengthen CISA's ability to evaluate the national cyber incident response system, the *CISA Cyber Exercise Act* would codify CISA's existing exercise work (including Cyber Storm) by creating the National Cyber Exercise Program. This new program would continue performing CISA's existing exercise work, while also being required to regularly exercise and evaluate the NCIRP. The bill also directs CISA to develop model exercises, which could be readily used by Federal, State, local, Tribal, and territorial government organizations, and private sector entities to test their own cybersecurity posture. S. 2993 would also require CISA to assist those government and private entities with the design, implementation, and evaluation of cyber exercises.

III. Legislative History

Senator Rosen (D–NV) introduced S. 2993, the *CISA Cyber Exercise Act,* on October 19, 2021, with Senators Sasse (R–NE) and King (I–ME). The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 2993 at a business meeting on November 3, 2021. During the meeting, a substitute amendment, as modified, was offered by Senator Rosen, which made technical edits to the legislation and clarified that the bill would not affect the authorities of the Administrator of Federal Emergency Management Agency. The Committee adopted the Rosen substitute amendment, as modified, by voice vote *en bloc*. Senators present for the vote were: Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley. The committee then reported the bill favorably by voice vote *en bloc*, as amended. Senators present for the vote were: Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section designates the short title of the bill as the "CISA Cyber Exercise Act."

Section 2. National Cyber Exercise Program

Subsection (a) amends the Homeland Security Act of 2002 to create a new section, 2220A, which would establish the National Cyber Exercise Program.

Sec. 2220A, subsection (a) requires the program to evaluate the National Cyber Incident Response Plan, and other related plans and strategies. As part of the National Cyber Exercise Program, CISA shall include a set of model exercises, which could be readily adapted by governments and private entities to test the safety and security of their own critical infrastructure. In carrying out the National Cyber Exercise Program, the Director of CISA may consult with appropriate representatives from Sector Risk Management

[11] *Id.*

Agencies, the Office of the National Cyber Director, cybersecurity research stakeholders, and Sector Coordinating Councils.

Sec. 2220A, subsection (b) defines "state" and "private entity."

Sec. 2220A, subsection (c) provides a rule of construction to clarify that the bill does not affect the Federal Emergency Management Agency's existing authority or responsibilities to conduct cyber exercises.

Subsection (b) is a clerical amendment updating the table of contents of the Homeland Security Act of 2002 with the new section, 2220A.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, November 23, 2021.

Hon. Gary C. Peters,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2993, the CISA Cyber Exercise Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

Phillip L. Swagel,
Director.

Enclosure.

S. 2993, CISA Cyber Exercise Act

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on November 3, 2021

By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
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	0	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 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

S. 2993 would establish a cybersecurity exercise program to evaluate strategies and plans for responding to cyber incidents. The Cybersecurity and Infrastructure Security Agency currently operates the Cyber Exercise Program, which meets the requirements of the bill. Because S. 2993 would codify the agency's current practices, implementing the bill would not affect the federal budget.

On May 27, 2021, CBO transmitted a cost estimate for H.R. 3223, the CISA Cyber Exercise Act, as ordered reported by the House Committee on Oversight and Reform on May 18, 2021. The two bills are similar, and CBO's estimates of their costs are the same.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. * * *

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Sec. 2220A. National cyber exercise program.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2220A. NATIONAL CYBER EXERCISE PROGRAM.

(a) ESTABLISHMENT OF PROGRAM.—

(1) IN GENERAL.—There is established in the Agency the National Cyber Exercise Program (referred to in this section as the 'Exercise Program') to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(2) REQUIREMENTS.—

(A) IN GENERAL.—The Exercise Program shall be—

(i) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(ii) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident;

(iii) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

(iv) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

(B) MODEL EXERCISE SELECTION.—The Exercise Program shall—

(i) include a selection of model exercises that government and private entities can readily adapt for use; and

(ii) aid such governments and private entities with the design, implementation, and evaluation of exercises that—

(I) conform to the requirements described in subparagraph (A);

(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

(III) provide for systematic evaluation of readiness.

(3) CONSULTATION.—In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, the Office of the National Cyber Director, cybersecurity research stakeholders, and Sector Coordinating Councils.

(b) DEFINITIONS.—In this section:

(1) STATE.—The term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin

Islands, Guam, American Samoa, and any other territory or possession of the United States.

(2) PRIVATE ENTITY.—The term 'private entity' has the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

* * * * * * *

○