Calendar No. 59

118TH CONGRESS *1st Session*	SENATE	REPORT 118–20

NATIONAL RISK MANAGEMENT ACT OF 2023

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 824

TO REQUIRE THE SECRETARY OF HOMELAND SECURITY TO ESTABLISH A NATIONAL RISK MANAGEMENT CYCLE, AND FOR OTHER PURPOSES

MAY 9, 2023.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
ALEX PADILLA, California	RICK SCOTT, Florida
JON OSSOFF, Georgia	JOSH HAWLEY, Missouri
RICHARD BLUMENTHAL, Connecticut	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 59

118TH CONGRESS *1st Session* | SENATE | REPORT 118–20

NATIONAL RISK MANAGEMENT ACT OF 2023

MAY 9, 2023.—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. 824]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 824) to require the Secretary of Homeland Security to establish a national risk management cycle, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	2
III. Legislative History	3
IV. Section-by-Section Analysis of the Bill, as Reported	3
V. Evaluation of Regulatory Impact	4
VI. Congressional Budget Office Cost Estimate	5
VI. Changes in Existing Law Made by the Bill, as Reported	5

I. PURPOSE AND SUMMARY

S. 824, the *National Risk Management Act of 2023*, would require the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a recurring national risk management assessment that identifies and compiles cyber and physical risks to our nation's critical infrastructure. It would also require the President to develop a national critical infrastructure resilience strategy to combat these risks. Additionally, the bill would require the Secretary of the De-

partment of Homeland Security (DHS) to conduct an annual congressional briefing on the strategy.[1]

II. Background and Need for the Legislation

For more than two decades, "nation-states and non-state actors have used cyberspace to subvert American power, American security, and the American way of life."[2] Cyber-attacks attributed to China have stolen "hundreds of billions of dollars in intellectual property,"[3] Russian cyber operators have influenced American elections and stolen government data,[4] and cyber criminals have struck state, local, and private entities with debilitating ransomware attacks.[5] As our economy and society become increasingly interconnected and digitized, adversaries will have more opportunities to "destroy private lives, disrupt critical infrastructure, and damage our economic and democratic institutions."[6]

In response to this threat, Congress established the Cyberspace Solarium Commission, which issued a report detailing a layered strategy to protect the United States from cyber adversaries.[7] One keystone recommendation of the Commission's strategy is developing a consistent, ongoing process to create "an accurate picture of 'national risk,'" which would help the United States better understand and mitigate risks to critical sectors.[8]

The National Risk Management Act of 2023 would codify that recommendation by establishing a five-year national risk management cycle to ensure the federal government stays ahead of emerging and evolving threats. The bill first requires CISA to identify and prioritize key risks to critical infrastructure in a report to the President and Congress. This report must be developed in consultation with sector risk management agencies and the National Cyber Director. CISA must also allow critical infrastructure owners and operators to provide information on a voluntary basis to CISA for the development of the report. The bill then requires the President to deliver to Congress a strategy addressing these risks, with recommendations on any necessary Congressional action. This cycle

---

[1] On May 12, 2021, the Committee approved S. 1350, the National Risk Management Act of 2021. That bill is substantially similar to S. 824. Accordingly, this committee report is in many respects similar to the committee report for S. 1350. *See* S. Rept. No. 117–261.

[2] U.S. Cyberspace Solarium Commission, *Report*, at 1 (March 2020) (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf/) (hereinafter "Solarium Report").

[3] *Id.; see also* White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China* (July 19, 2021) (https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/).

[4] *See* Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election* (Nov. 10, 2020) (S. Rept. 116–290); National Cyber Security Centre, Cybersecurity and Infrastructure Agency, Federal Bureau of Investigation, and National Security Agency, *Advisory: Further TTPs Associated with SVR Cyber Actors* (May 7, 2021) (https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf).

[5] *See, e.g.*, Senator Gary Peters, *Peters Presses Colonial Pipeline CEO on Recent Hack That Caused Gas Shortages and Price Increases for Millions of Americans* (June 8, 2021) (https://www.hsgac.senate.gov/media/majority-media/peters-presses-colonial-pipeline-ceo-on-recent-hack-that-caused-gas-shortages-and-price-increases-for-millions-of-americans); Senator Gary Peters, *Peters Convenes Second Hearing with Top Federal Cybersecurity Officials to Discuss Recent Breaches and Attacks Against U.S. Systems* (May 11, 2021) (https://www.hsgac.senate.gov/media/majority-media/peters-convenes-second-hearing-with-top-federal-cybersecurity-officials-to-discuss-recent-breaches-and-attacks-against-us-systems).

[6] Solarium Report, *supra* note 2, at 1.

[7] Cyberspace Solarium Commission, Home Page (https://www.solarium.gov/home) (accessed Aug. 12, 2021).

[8] Solarium Report, *supra* note 2, at 55.

would repeat every five years, ensuring the federal government stays on top of constantly evolving cyber risks and threats to national security. The bill also requires the Secretary of Homeland Security to brief Congress annually on any actions taken or resources needed to implement the strategy.

III. Legislative History

Senator Margaret Wood Hassan (D–NH) introduced S. 824, the *National Risk Management Act of 2023*, on March 15, 2023, with original cosponsor Senator Mitt Romney (R–UT). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 824 at a business meeting on March 29, 2023. At the business meeting, Senator Paul offered an amendment to the bill, to strike all language requiring CISA to identify and prioritize key risks to critical infrastructure in a report to the President and Congress, leaving only the requirement for the President to deliver a strategy to Congress to address risks to critical infrastructure. The Paul amendment was not adopted by voice vote with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Paul, Lankford, Romney, Scott, and Hawley present. The bill was ordered reported favorably by roll call vote of 11 yeas to 1 nay, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Lankford, Romney, Scott, and Hawley voting in the affirmative, and Senator Paul voting in the negative. Senators Carper, Johnson, and Marshall voted yea by proxy, for the record only.

Consistent with Committee Rule 3(G), the Committee reports the bill with a technical amendment by mutual agreement of the Chairman and Ranking Member.

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

Section 1. Short title

This section establishes the short title of the bill as the "National Risk Management Act of 2023."

Section 2. National risk management cycle

This section adds a new section, section 2220F, to the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) creating a national risk management cycle to identify and mitigate risks to critical national functions.

Section 2220F, "National Risk Management Cycle" (as added by this Act) includes the following:

Subsection (a) defines "national critical functions" to include any functions of the government or private sector so vital that their disruption, corruption, or dysfunction would have "debilitating" effects on national security, public health and safety, or the economy.

Subsection (b) outlines the national risk management cycle.

Subsection (b)(1) details the risk identification and assessment process. Subsection (b)(1)(A) instructs the Secretary of Homeland Security, through the Director of CISA, to establish a recurring process to identify and assess both physical and cyber risks to critical infrastructure and associated likelihoods, vulnerabilities, and consequences.

Subsection (b)(1)(B) requires the Secretary to establish a process to consult with Sector Risk Management Agencies, critical infrastructure owners and operators, and federal officials including the National Cyber Director.

Subsection (b)(1)(C) requires the Secretary to establish processes that include how to collect information from Sector Risk Management Agencies and how to allow critical infrastructure owners and operators to submit relevant information to the Secretary on a voluntary basis.

Subsection (b)(1)(D) requires the Secretary to publish the procedures of the risk identification and assessment process described in (b)(1)(A) in the Federal Register.

Subsection (b)(1)(E) requires the Secretary to submit a report on the risk identification and assessment process to the President, as well as the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Homeland Security within one year of enactment and every five years thereafter.

Subsection (b)(2) details the requirements for the national critical infrastructure resilience strategy. Subsection (b)(2)(A) requires the President to develop a national strategy addressing the risks identified in subsection (b)(1). This strategy must be delivered to congressional leadership and certain committees every five years.

Subsection (b)(2)(B) specifies that the national critical infrastructure resilience strategy must: prioritize areas of risk to critical infrastructure and functions that impact national security, economic security, or public health and safety; assess the implementation of the previous national strategy; identify current and proposed national-level actions, including resource requirements, and programs to address the risks identified, along with which federal departments are leading those efforts; and request any additional authorities needed to execute the strategy.

Subsection (b)(2)(C) requires the strategy to be unclassified, but allows for a classified annex.

Subsection (b)(3) requires the Secretary of Homeland Security, in coordination with Sector Risk Management Agencies, to brief the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Homeland Security on the activities taken in response to the strategy and the funding that the Secretary has determined would be necessary to execute the strategy.

Subsection (b) of the underlying bill contains a conforming amendment adding the new section of the Homeland Security Act of 2002 to the table of contents.

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

S. 824, National Risk Management Act of 2023

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 29, 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)	*	*	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	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 824 would establish an administrative process for the Cybersecurity and Infrastructure Security Agency (CISA) to study cyber and physical threats to critical infrastructure (such as power generation and water treatment facilities). The bill also would require CISA to periodically report to the Congress on proposals to mitigate such security risks.

CISA currently assesses security threats to critical infrastructure and shares risk mitigation strategies with nonfederal entities; thus, the bill would codify those responsibilities and would not impose new operating requirements on the agency. Using information about similar reporting requirements, CBO estimates that implementing S. 824 would cost less than $500,000 over the 2023–2028 period; such spending would be subject to the availability of appropriated funds.

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

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

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.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Sec. 2220F. National risk management cycle.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2220F. NATIONAL RISK MANAGEMENT CYCLE.

(a) NATIONAL CRITICAL FUNCTIONS DEFINED.—In this section, the term "national critical functions" means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

(b) NATIONAL RISK MANAGEMENT CYCLE.—

(1) RISK IDENTIFICATION AND ASSESSMENT.—

(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a recurring process by which to identify and assess risks to critical infrastructure, considering both cyber and physical threats and the associated likelihoods, vulnerabilities, and consequences.

(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult—

(i) Sector Risk Management Agencies;

(ii) critical infrastructure owners and operators;

(iii) the Assistant to the President for National Security Affairs;

(iv) the Assistant to the President for Homeland Security; and

(v) the National Cyber Director.

(C) PROCESS ELEMENTS.—The process established under subparagraph (A) shall include elements to—

(i) collect relevant information, collected pursuant to section 2218, from Sector Risk Management Agencies relating to the threats, vulnerabilities, and consequences related to the particular sectors of those Sector Risk Management Agencies;

(ii) allow critical infrastructure owners and operators to submit relevant information to the Secretary for consideration; and

(iii) outline how the Secretary will solicit input from other Federal departments and agencies.

(D) PUBLICATION.—Not later than 180 days after the date of enactment of this section, the Secretary shall publish in the Federal Register procedures for the process established

under subparagraph (A), subject to any redactions the Secretary determines are necessary to protect classified or other sensitive information.

(E) REPORT.—The Secretary shall submit to the President, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the risks identified by the process established under subparagraph (A)—

(i) not later than 1 year after the date of enactment of this section; and

(ii) not later than 1 year after the date on which the Secretary submits a periodic evaluation described in section 9002(b)(2) of title XC of division H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a(b)(2)).

(2) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers each report required under paragraph (1), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

(B) ELEMENTS.—Each strategy delivered under subparagraph (A) shall—

(i) prioritize areas of risk to critical infrastructure that would compromise or disrupt national critical functions impacting national security, economic security, or public health and safety;

(ii) assess the implementation of the previous national critical infrastructure resilience strategy, as applicable;

(iii) identify and outline current and proposed national-level actions, programs, and efforts, including resource requirements, to be taken to address the risks identified;

(iv) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each; and

(v) request any additional authorities necessary to successfully execute the strategy.

(C) FORM.—Each strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers the first strategy required under paragraph (2)(A), and each year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the Committee on Homeland Security and Gov-

ernmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on—

(A) the national risk management cycle activities undertaken pursuant to the strategy delivered under paragraph (2)(A); and

(B) the amounts and timeline for funding that the Secretary has determined would be necessary to address risks and successfully execute the full range of activities proposed by the strategy delivered under paragraph (2)(A).

* * * * * * *

○