Calendar No. 652

117TH CONGRESS *2d Session*	SENATE	REPORT 117–261

NATIONAL RISK MANAGEMENT ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1350

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

DECEMBER 15, 2022.—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
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. 652

117TH CONGRESS
2d Session

SENATE

REPORT
117–261

NATIONAL RISK MANAGEMENT ACT OF 2021

DECEMBER 15, 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. 1350]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1350), to require the Secretary of Homeland Security to establish a national risk management cycle, and for other purposes, having considered the same, reports favorably with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 1350, the National Risk Management Act of 2021, requires 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 also requires the President to develop a national critical infrastructure resilience strategy to combat these risks. Additionally, the bill requires the Secretary of the Department of Homeland Security (DHS) to conduct an annual congressional briefing on the strategy.

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."[1] Cyber attacks attributed to China have stolen "hundreds of billions of dollars in intellectual property,"[2] Russian cyber operators have influenced American elections and stolen government data,[3] and cyber criminals have struck state, local, and private entities with debilitating ransomware attacks.[4] 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."[5]

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.[6] 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.[7]

The National Risk Management Act of 2021 codifies that recommendation by establishing a five-year national risk management cycle to ensure that 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, critical infrastructure owners and operators, and the National Cyber Director. It then requires the President to deliver to Congress a strategy addressing these risks, with recommendations on any necessary Congressional action. This cycle repeats every five years, ensuring that 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.

---

[1] Cyberspace Solarium Commission, *Report*, at 1 (March, 2020) [hereinafter Solarium Report].

[2] *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/).

[3] *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).

[4] *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).

[5] Solarium Report, *supra* note 1, at 1.

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

[7] Solarium Report, *supra* note 1, at 55.

III. LEGISLATIVE HISTORY

Senators Margaret Hassan (D–NH) and Ben Sasse (R–NE) introduced S. 1350, the National Risk Management Act of 2021, on April 22, 2021. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 1350 at a business meeting on May 12, 2021. During the business meeting, a substitute amendment was offered by Senator Hassan. The Hassan Substitute Amendment made minor edits to the bill, including clarifying that the Secretary of Homeland Security must consult with and collect information from Sector Risk Management Agencies and private sector entities, ensure publication of the process appropriately redacts national security information, and provide a budget plan as part of the strategy. The Hassan Substitute Amendment was adopted *en bloc* by voice vote, with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Paul, Lankford, Romney, Scott, and Hawley present. The Committee ordered the bill to be reported favorably, as amended, *en bloc* by voice vote with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Paul, Lankford, Romney, Scott, and Hawley present.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section designates the name of the bill as the "National Risk Management Act of 2021."

Section 2. National Risk Management Cycle

This section adds a new section 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.

Subsection (a) defines "national critical functions'" to include any functions of the American 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, assess, and prioritize both physical and cyber risks to critical infrastructure, and the resources necessary to address those risks.

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

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

Subsection (b)(1)(D) requires the Secretary of Homeland Security to submit a report on the risks identified and assessed by the 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: identify, assess, and 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 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 certain congressional committees on the activities taken in response to the strategy and the funding that the Secretary has determined would be necessary to execute the strategy.

The bill also 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. 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. 2218. National risk management cycle.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2218. 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, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, the associated likelihoods, vulnerabilities, and consequences, and the resources necessary to address them.

(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with, and request and collect information to support analysis from, Sector Risk Management Agencies, critical infrastructure owners and operators, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the National Cyber Director.

(C) 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.

(D) 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 (Public Law 116–283).

(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) identify, assess, and 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 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;

(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 every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate congressional committees on—

(A) the national risk management cycle activities undertaken pursuant to the strategy; 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.

* * * * * * *

○