117TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
117–245

DHS ROLES AND RESPONSIBILITIES IN CYBER SPACE ACT

FEBRUARY 11, 2022.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 5658]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 5658) to require the Secretary of Homeland Security to submit a report on the cybersecurity roles and responsibilities of the Federal Government, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "DHS Roles and Responsibilities in Cyber Space Act".

SEC. 2. FINDINGS.

Congress finds the following:

(1) The Department of Homeland Security, through the Cybersecurity and Infrastructure Security Agency, is the lead Federal coordinator for securing critical infrastructure across all 16 sectors, in coordination with designated Sector Risk Management Agencies.

(2) Cyber incidents require technical resources and are only sometimes sector specific.

(3) The Cybersecurity and Infrastructure Security Agency is the central agency that can quickly analyze and coordinate mitigations when a malicious cyber campaign spans multiple sectors.

(4) Section 2209 of the Homeland Security Act of 2002 authorizes the Cybersecurity and Infrastructure Security Agency as the Federal civilian interface for multi-directional and cross-sector sharing of information related to cyber threat indicators with and between the government and the private sector.

(5) Section 2209 of the Homeland Security Act of 2002 authorizes the Cybersecurity and Infrastructure Security Agency to facilitate cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors.

(6) Presidential Policy Directive-41 directs the Department of Homeland Security, via the national cybersecurity and communications integration center, to be the lead Federal agency for asset response during a significant cyber incident.

(7) The functions of the national cybersecurity and communications integration center are carried about by the Cybersecurity and Infrastructure Security Agency's Cybersecurity Division.

(8) Presidential Policy Directive-21 directs the Department of Homeland Security to lead the coordination of critical infrastructure protection among the Sector Risk Management Agencies.

(9) Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 codified the duties of Sector Risk Management Agencies for critical infrastructure sectors, laying out the roles and responsibilities they have in coordinating with the Cybersecurity and Infrastructure Security Agency to secure the nation's critical infrastructure.

(10) Enhancing the security and resilience of our critical infrastructure is a priority for Congress and for the Nation.

(11) The Department of Homeland Security maintains and continues to build partnerships across all infrastructure sectors to enhance control systems cybersecurity.

(12) Section 1731 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 directed the Secretary of Homeland Security to submit a report on the potential for better coordination of Federal cybersecurity efforts at an integrated cybersecurity center within the Cybersecurity and Infrastructure Security Agency.

SEC. 3. REPORT ON CYBERSECURITY ROLES AND RESPONSIBILITIES OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the roles and responsibilities of the Department and its components relating to cyber incident response.

(b) CONTENTS.—The report required under subsection (a) shall include the following:

(1) A review of how the cyber incident response plans under section 2210(c) of the Homeland Security Act of 2002 (6 U.S.C. 660(c)) are utilized in the Federal Government's response to a cyber incident.

(2) An explanation of the roles and responsibilities of the Department of Homeland Security and its components with responsibility for, or in support of, the Federal Government's response to a cyber incident, including primary responsibility for working with impacted private sector entities.

(3) An explanation of which and how authorities of the Department and its components are utilized in the Federal Government's response to a cyber incident.

(4) Recommendations to provide further clarity for roles and responsibilities of the Department and its components relating to cyber incident response.

PURPOSE AND SUMMARY

H.R. 5658, "DHS Roles and Responsibilities in Cyber Space Act," seeks to clarify the roles and responsibilities of officials across the Department of Homeland Security (DHS) related to the Department's cyber incident response mission. Specifically, it directs the Secretary of Homeland Security, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency (CISA), to report to Congress on the roles and responsibilities of the Department and its components relating to cyber incident response. The report must include: (1) a review of how cyber incident response plans developed by CISA are utilized in the Federal Government's response to a cyber incident; (2) an explanation of the roles and responsibilities of DHS and its components in the Federal Government's response to a cyber incident; (3) an explanation of how the Department and its components leverage existing authorities in cyber incident response; and (4) recommendations to clarify roles and responsibilities among DHS components related to the its cybersecurity mission.

BACKGROUND AND NEED FOR LEGISLATION

The volume of cyber attacks impacting our Nation's critical infrastructure in 2021 highlighted the lack of clarity among the roles and responsibilities among the Federal Government pertaining to cyber incident response. Pursuant to longstanding doctrine, including Presidential Policy Directive–21, DHS, through CISA, is the lead Federal coordinator for securing critical infrastructure across all 16 sectors, in coordination with designated Sector Risk Management Agencies. As cybersecurity incidents have grown in frequency and sophistication, the Federal Government and the private sector have demanded more of CISA's technical, analytic, and operational capabilities during incident response. DHS's cross-sector coordination responsibilities related to cyber incident response have become increasingly important particularly because cyber incidents are rarely sector specific.

Presidential Policy Directive–41 directs DHS, through the National Cybersecurity and Communications Integration Center, to be the lead Federal agency for asset response during a significant cyber incident. CISA is the central agency charged with quickly analyzing and coordinating mitigation when a malicious cyber campaign spans multiple sectors. Section 2209 of the Homeland Security Act of 2002 authorizes the agency as the Federal civilian interface for multi-directional and cross-sector sharing of information related to cyber threat indicators with, and between, the government and the private sector. It also directs CISA to facilitate cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors.

Although CISA plays a prominent role in executing DHS's cybersecurity responsibilities, other DHS components also bring to bear important capabilities. For example, the Transportation Security

Administration and the United States Coast Guard carry out DHS responsibilities as the co-Sector Risk Management Agency for the transportation sector. Notably, those responsibilities include partnering with sector stakeholders on incident preventions, mitigation, response, and recovery activities.

The United States Secret Service (USSS) is charged with investigating complex cyber crimes. To carry out its mission, USSS houses Cyber Fraud Task Forces (CFTFs), which are partnerships between the Secret Service, other law enforcement agencies, prosecutors, private industry, and academia, leveraged to enhance cyber investigative efforts. USSS also maintains a Global Investigative Operations Center, which supports strategic domestic and international investigations with potential impact on the integrity of the financial infrastructure and works with CFTFs to combat translational criminal organizations.

Similarly, the Homeland Security Investigations (HSI) Cyber Crimes Center within Immigrations and Customs Enforcement brings together highly technical assets dedicated to conducting trans-border criminal investigations of cyber-related crimes within the HSI portfolio of customs and immigration authorities.

Other activities related to DHS's cybersecurity preparedness and response missions are carried out, or supported by, other components of the Department, including the Office of Strategy, Policy, and Plans, the Science and Technology Directorate, and the Office of Intelligence and Analysis. A DHS strategy that articulates the roles and responsibilities for each component will ensure the efficient, strategic allocation of resources for the Department's cybersecurity missions.

HEARINGS

For the purposes of clause 3(c)(6) of rule XIII of the Rules of the House of Representatives, the following hearings were used to develop H.R. 5658:

- On June 15, 2021, the Subcommittees on Cybersecurity, Infrastructure Protection, and Innovation and Transportation and Maritime Security held a joint hearing entitled "Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack." Ms. Sonya Proctor, Assistant Administrator for Surface Operations, Transportation Security Administration, Department of Homeland Security; and Mr. Eric Goldstein, Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security testified.
- On October 26, 2021, the Subcommittees on Cybersecurity, Infrastructure Protection, and Innovation and Transportation and Maritime Security held a joint hearing titled, "Transportation Cybersecurity: Protecting Planes, Trains, and Pipelines from Cyber Threats." Ms. Suzanne Spaulding, Senior Adviser, Center for Strategic and International Studies (formerly Under Secretary, National Protection and Programs Directorate); Ms. Patty Cogswell, Strategic Advisor, Guidehouse (formerly Deputy Administrator, Transportation Security Administration); Mr. Jeffrey Troy, President & Chief Executive Officer, Aviation Information Sharing and Analysis Center (formerly Deputy Assistant Director, Cyber Division, Federal Bu-

reau of Investigation); and Mr. Scott Dickerson, Executive Director, Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) testified.

- On November 3, 2021, the Committee on Homeland Security held a hearing entitled, "Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow." The Honorable Chris Inglis, National Cyber Director, Executive Office of the President; and The Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency testified.
- On November 17, 2021, the Subcommittees on Intelligence and Counterterrorism and Cybersecurity, Infrastructure Protection, and Innovation held a joint hearing entitled "A Whole-of-Government Approach to Combatting Ransomware: Examining DHS's Role." The Honorable Rob Silvers, Under Secretary, Office of Strategy, Policy, and Plans, DHS, Mr. Brandon Wales, Executive Director, Cybersecurity and Infrastructure Security Agency (CISA), DHS, and Mr. Jeremy Sheridan, Assistant Director of Investigations, U.S. Secret Service (USSS), DHS testified.

COMMITTEE CONSIDERATION

The Committee met on October 26, 2021, a quorum being present, to consider H.R. 5658 and ordered the measure to be favorably reported to the House, as amended, by voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 5658.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures contained in the cost estimate prepared by the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, November 22, 2021.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5658, the DHS Roles and Responsibilities in Cyber Space 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.

H.R. 5658, DHS Roles and Responsibilities in Cyber Space Act
As ordered reported by the House Committee on Homeland Security on October 26, 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)	*	*	not estimated

		Mandate Effects	
Statutory pay-as-you-go procedures apply?	No		
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

* = between zero and $500,000

H.R. 5658 would require the Department of Homeland Security (DHS) to report to the Congress on the effectiveness of the department's responses to cybersecurity incidents. Under the bill, DHS also would provide the Congress with recommendations to further clarify cybersecurity responsibilities across the department's component agencies.

Based on the costs of similar studies, CBO estimates that preparing and delivering the required report would cost less than $500,000 over the 2022–2026 period. Such spending would be subject to the availability of appropriations.

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

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 5658 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 5658 is to clarify the roles and responsibilities of components within the Department of Homeland Security related to the Department's cybersecurity mission.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that H.R. 5658 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section states that the Act may be cited as the "DHS Roles and Responsibilities in Cyber Space Act".

Sec. 2. Findings.

This section makes the following findings related to the cybersecurity roles and responsibilities within the Department of Homeland Security:

1. The Department of Homeland Security, through the Cybersecurity and Infrastructure Security Agency, is the lead Federal coordinator for securing critical infrastructure across all 16 sectors, in coordination with designated Sector Risk Management Agencies.
2. Cyber incidents require technical resources and are very rarely sector specific.
3. The Cybersecurity and Infrastructure Security Agency is the central agency that can quickly analyze and coordinate mitigations when a malicious cyber campaign spans multiple sectors.
4. Section 2209 of the Homeland Security Act of 2002 authorizes the Cybersecurity and Infrastructure Security Agency as the Federal civilian interface for multi-directional and cross-sector sharing of information related to cyber threat indicators with and between the government and the private sector.

5. Section 2209 of the Homeland Security Act of 2002 authorizes the Cybersecurity and Infrastructure Security Agency to facilitate cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors.

6. Presidential Policy Directive–41 directs the Department of Homeland Security, via the national cybersecurity and communications integration center, to be the lead Federal agency for asset response during a significant cyber incident.

7. The functions of the national cybersecurity and communications integration center are carried about by the Cybersecurity and Infrastructure Security Agency's Cybersecurity Division.

8. Presidential Policy Directive–21 directs the Department of Homeland Security to lead the coordination of critical infrastructure protection among the Sector Risk Management Agencies.

9. Enhancing the security and resilience of our critical infrastructure is a priority for Congress and for the Nation.

10. The Department of Homeland Security maintains and continues to build partnerships across all infrastructure sectors to enhance control systems cybersecurity.

Sec. 3. Report on Cybersecurity Roles and Responsibilities of the Department of Homeland Security.

This section requires the Secretary of Homeland Security, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, to submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate within 1 year of enactment a report on the roles and responsibilities of the Department and its components relating to cyber incident response.

The report must contain:

1. A review of how the cyber incident response plans under section 2210(c) of the Homeland Security Act of 2002 (6 U.S.C. 660(c)) are utilized in the Federal Government's response to a cyber incident;

2. An explanation of the roles and responsibilities of the Department of Homeland Security and its components with responsibility for, or in support of, the Federal Government's response to a cyber incident, including primary responsibility for working with impacted private sector entities;

3. An explanation of which and how authorities of the Department and its components are utilized in the Federal Government's response to a cyber incident; and

4. Recommendations to provide further clarity for roles and responsibilities of the Department and its components relating to cyber incident response.

○