119TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
119–376

PIPELINE SECURITY ACT

NOVEMBER 12, 2025.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GARBARINO, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 5062]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 5062) to amend the Implementing Recommendations of the 9/11 Commission Act of 2007 to codify the Transportation Security Administration's responsibility relating to securing pipeline transportation and pipeline facilities against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of pipelines, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

H.R. 5062, the "Pipeline Security Act," amends the Implementing Recommendations of the 9/11 Commission Act of 2007 to codify the Transportation Security Administration's (TSA) responsibility for securing pipeline transportation and pipeline facilities against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize their physical and cyber integrity. The legislation formally establishes TSA's lead role, in consultation with the Cybersecurity and Infrastructure Security Agency (CISA), in ensuring the security of the Nation's pipelines against a wide range of physical and cyber threats.

Specifically, H.R. 5062 directs the TSA Administrator to develop and maintain guidelines, directives, and regulations related to pipeline security, conduct assessments and inspections of pipeline security practices, engage stakeholders through industry outreach, and report regularly to Congress on the agency's progress. The legislation also mandates that TSA develop a personnel strategy to ensure sufficient cybersecurity expertise and resources to carry out its pipeline security mission, and requires the Government Accountability Office (GAO) to review TSA's implementation of the Act within two years of enactment.

BACKGROUND AND NEED FOR LEGISLATION

Pipelines are among the most critical assets within the nation's transportation infrastructure, transporting billions of barrels of liquid fuels and trillions of cubic feet of natural gas annually. Disruptions to pipeline operations can have far-reaching effects on energy supply, economic stability, and national security.

Since its establishment in 2001, TSA has served as the lead federal agency responsible for the security of the nation's pipeline systems. While the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) oversees the safety of pipeline operations, TSA is charged with ensuring their security, including from acts of terrorism and evolving cybersecurity threats. These responsibilities derive from TSA's statutory mission to exercise "security responsibilities over other [non-aviation] modes of transportation that are exercised by the Department of Transportation" (49 U.S.C. 114(d)) but are not more explicitly outlined in statute, leaving questions about TSA's long-term authority, resourcing, and accountability for pipeline security.

The Committee recognizes that the threat environment for U.S. critical infrastructure is evolving rapidly, with cyber actors, including those linked to the People's Republic of China, Russia, and Iran, targeting the transportation sector to compromise operational technology (OT) systems, disrupt service, and erode public confidence. TSA's ability to address these threats requires statutory clarity, consistent oversight, and strengthened coordination with CISA, which leads the federal government's broader cybersecurity efforts.

H.R. 5062 responds directly to these challenges by explicitly codifying TSA's security responsibilities, enhancing interagency collaboration, and requiring strategic planning to expand TSA's cybersecurity expertise. The legislation ensures that TSA's pipeline security mission is aligned with national cyber defense priorities while pro-

viding Congress with the tools to evaluate its effectiveness through biennial reporting and GAO review.

HEARINGS

The Committee has not held a hearing that guided the development of this legislation in the 119th Congress.

COMMITTEE CONSIDERATION

The Committee met on September 3, 2025, a quorum being present, to consider H.R. 5062 and ordered the measure to be favorably reported to the House by a recorded vote of 22 yeas to 0 nays.

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.

The vote was as follows:

COMMITTEE ON HOMELAND SECURITY 119TH CONGRESS		
Date: September 3, 2025 **Roll Call Vote No. 56**		
Ordering H.R. 5062 to be favorably reported to the House		
Yeas		**Nays**
X	Mr. McCaul, Texas	
X	Mr. Guest, Mississippi	
X	Mr. Gimenez, Florida	
	Mr. Pfluger, Texas	
	Ms. Greene, Georgia	
X	Mr. Gonzales, Texas	
X	Mr. Luttrell, Texas	
	Mr. Strong, Alabama	
X	Mr. Brecheen, Oklahoma	
X	Mr. Crane, Arizona	
X	Mr. Ogles, Tennessee	
X	Mrs. Biggs, South Carolina	
X	Mr. Evans, Colorado	
X	Mr. Mackenzie, Pennsylvania	
	Mr. Knott, North Carolina	
X	*Mr. Thompson, Mississippi, Ranking Member*	
	Mr. Swalwell, California	
	Mr. Correa, California	
X	*Mr. Thanedar, Michigan*	
X	*Mr. Magaziner, Rhode Island*	
X	*Mr. Goldman, New York*	
X	*Mrs. Ramirez, Illinois*	
X	*Mr. Kennedy, New York*	
X	*Mrs. McIver, New Jersey*	
X	*Ms. Johnson, Texas*	
X	*Mr. Hernández, Puerto Rico*	
	Ms. Pou, New Jersey	
X	*Mr. Carter, Louisiana*	
	Mr. Green, Texas	
X	Mr. Garbarino, New York, Chairman	
22	**TOTAL**	0

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.

H.R. 5062, Pipeline Security Act
As ordered reported by the House Committee on Homeland Security on September 3, 2025

By Fiscal Year, Millions of Dollars	2026	2026-2030	2026-2035
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	1	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2036?	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 2036?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	Yes, Cannot Determine Costs

* = between zero and $500,000.

H.R. 5062 would codify the role of the Transportation Security Administration (TSA) as the lead agency responsible for protecting pipelines from terrorists and cybersecurity threats. The bill would require TSA to develop a personnel strategy to carry out the pipeline security program and report to the Congress biennially on its efforts. Finally, the bill would require the Government Accountability Office (GAO) to review the bill's implementation within two years of enactment.

Many of the bill's requirements are consistent with activities being conducted under current law and would not significantly affect TSA's costs. Based on the cost of similar activities, CBO estimates that implementing other provisions of the bill would cost $1 million over the 2026–2030 period. That amount would cover the additional reporting requirements and the cost of GAO's review. Any related spending would be subject to the availability of appropriated funds.

If TSA issues new regulations on pipeline transportation and pipeline facilities as a result of the legislation, H.R. 5062 would im-

pose a private-sector mandate as defined in the Unfunded Mandates Reform Act (UMRA). Because the cost of the mandate would depend on the regulations yet to be published, CBO cannot determine whether the cost would exceed annual threshold established in UMRA for private-sector mandates ($206 million in 2025, adjusted annually for inflation).

H.R. 5062 would not impose intergovernmental mandates as defined in UMRA.

The CBO staff contacts for this estimate are Aaron Krupkin (for federal costs) and Brandon Lever (for mandates). The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

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 of 1995.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 5062 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. 5062 is to codify the TSA's statutory responsibility for securing pipeline transportation and pipeline facilities against acts of terrorism, cybersecurity threats, and other security risks.

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 THE LEGISLATIVE BRANCH

The Committee finds that H.R. 5062 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 the Act may be cited as the "Pipeline Security Act."

Section 2. Pipeline Transportation and Pipeline Facilities Security responsibilities

This section amends subtitle D of title XV of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (6 U.S.C. 1201 et seq.) by adding a new section, section 1559, entitled "Pipeline Security."

The new section codifies the TSA's responsibility, in consultation with CISA, for the security of pipeline transportation and pipeline facilities against cybersecurity threats, acts of terrorism, and other security risks. It requires TSA to carry out a range of activities related to pipeline security, including developing and maintaining security guidelines, conducting risk assessments and inspections, sharing threat information with owners and operators, and coordinating with relevant federal, state, and industry stakeholders.

The provision further directs TSA to report to the Committee on Homeland Security of the House of Representatives and the Committees on Commerce, Science, and Transportation and on Homeland Security and Governmental Affairs of the Senate on its activities to secure pipeline transportation and pipeline facilities.

Additionally, TSA, in consultation with CISA, must develop a personnel strategy to assess and strengthen the cybersecurity expertise and resources necessary to carry out its pipeline security mission. Finally, the Comptroller General of the United States is required to review the implementation of the Act within two years of enactment.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics and existing law in which no change is proposed is shown in roman):

IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007

* * * * * * *

Sec.

* * * * * * *

1559. Pipeline security.

* * * * * * *

SEC. 1559. PIPELINE SECURITY.

(a) IN GENERAL.—The Administrator of the Transportation Security Administration shall maintain responsibility, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, as appropriate, for securing pipeline transportation and pipeline facilities (as such terms are defined in section 60101 of title 49, United States Code) against cybersecurity

threats (as such term is defined in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650)), acts of terrorism (as such term is defined in section 3077 of title 18, United States Code), and other security threats.

(b) GUIDELINES, DIRECTIVES, AND REGULATIONS.—In carrying out subsection (a), the Administrator of the Transportation Security Administration shall carry out the following:

(1) Ensure the development and updating, in consultation with relevant Federal, State, local, Tribal, and territorial entities and public and private sector stakeholders, as applicable, of guidelines, consistent with the National Institute of Standards and Technology Framework for Improvement of Critical Infrastructure Cybersecurity (and any update to such Framework) pursuant to section 2(c)(15) of the National Institute for Standards and Technology Act (15 U.S.C. 272(c)(15)), to improve the security of pipeline transportation and pipeline facilities against cybersecurity threats, acts of terrorism, and other security threats.

(2) Promulgate any additional security directives or regulations as the Administrator determines necessary to secure pipeline transportation or pipeline facilities.

(3) Share, as appropriate, with relevant Federal, State, local, Tribal, and territorial entities and public and private sector stakeholders, as applicable, the guidelines described in paragraph (1), security directives, and regulations and, as appropriate, intelligence and information, regarding cybersecurity threats, acts of terrorism, and other security threats to pipeline transportation and pipeline facilities.

(4) Assess and inspect, as appropriate, the implementation of such guidelines, security directives, and regulations, including the security policies, plans, practices, and training programs maintained by owners and operators of pipeline transportation and pipeline facilities, to provide recommendations or requirements for the improvement of the security of pipeline transportation and pipeline facilities against cybersecurity threats, acts of terrorism, and other security threats.

(5) Identify and rank the relative security risks to pipeline transportation and pipeline facilities.

(6) Inspect pipeline transportation and pipeline facilities, including such transportation or facilities, as the case may be, designated as critical by owners and operators of such transportation or facilities based on such guidelines, security directives, or regulations.

(c) STAKEHOLDER ENGAGEMENT.—Not later than one year after the date of the enactment of this subsection, the Administrator of the Transportation Security Administration shall convene at least one industry day to engage with relevant pipeline transportation and pipeline facilities stakeholders on matters related to the security of pipeline transportation and pipeline facilities.

* * * * * * *

○