Calendar No. 631

117TH CONGRESS *2d Session*	SENATE	REPORT 117–247

DHS INDUSTRIAL CONTROL SYSTEMS CAPABILITIES ENHANCEMENT ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2439

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO PROVIDE FOR THE RESPONSIBILITY OF THE CYBERSECURIY AND INFRASTRUCTURE SECURITY AGENCY TO MAINTAIN CAPABILITIES TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS, AND FOR OTHER PURPOSES

DECEMBER 13, 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. 631

117TH CONGRESS
2d Session

SENATE

REPORT
117–247

DHS INDUSTRIAL CONTROL SYSTEMS CAPABILITIES ENHANCEMENT ACT OF 2021

DECEMBER 13, 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. 2439]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2439) to amend the Homeland Security Act of 2002 to provide provide for the responsibility of the Cybersecurity and Infrastructure Security Agency to maintain capabilities to identify threats to industrial control systems, and for other purposes, having considered the same, reports favorably thereon with an amendment 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	4
VII. Changes in Existing Law Made by the Bill, as Reported	5

I. PURPOSE AND SUMMARY

S. 2439, the *DHS Industrial Control Systems Capabilities Enhancement Act of 2021*, directs the Department of Homeland Security (DHS)'s Cybersecurity and Infrastructure Security Agency (CISA) to maintain capabilities to identify and address threats and vulnerabilities to industrial control systems (ICS) products and technologies used by critical infrastructure. ICS are the informa-

tional and operational technologies that monitor and control the physical functions of critical infrastructure, such as water and sewer system pumps, power grid controls, and pipeline valves. Malicious cyber actors are increasingly targeting ICS to disrupt the operations of critical infrastructure. This bill will ensure that CISA leads and coordinates Federal efforts to provide assistance to these entities, mitigate threats to ICS, and share pertinent information with various ICS stakeholders.

II. Background and Need for the Legislation

ICS are the informational technologies and operational technologies, commonly referred to as IT and OT, respectively, that monitor and control the functions of critical infrastructure such as water and sewer systems, power grids, and pipelines.[1] IT systems are those systems that manage data and virtual information, while OT systems manage the functioning of physical operations of an enterprise. Successful cyber-attacks on these systems can have consequential physical-world ramifications.[2] In July 2020, CISA found that a cyber-attack on an ICS "could result in significant physical consequences, including loss of life, property damage, and disruption of the essential services and critical functions upon which society relies."[3] The owners and operators of smaller critical infrastructure systems, like municipal water and sewer departments, may not have adequate resources or personnel to actively identify and mitigate cybersecurity threats and vulnerabilities within their ICS.[4] Malicious cyber actors have frequently targeted these systems to disrupt, destroy, or alter the functioning of critical infrastructure operations.[5] For example, malicious cyber actors nearly succeeded in coopting the ICS of a water treatment facility in Oldsmar, Florida to potentially poison the community's water supply.[6]

CISA recognizes this threat and created a multi-year strategy to help critical infrastructure owners and operators secure their ICS components.[7] CISA has also released dozens of advisories, alerts, and reports to provide timely information to critical infrastructure owners and operators about security issues, vulnerabilities, and threats related to their ICS.[8]

S. 2439 requires CISA to maintain their existing capabilities to identify and address threats and vulnerabilities to ICS products and technologies. Additionally, S. 2439 requires CISA to lead, in

---

[1] Congressional Research Service, *Pipeline Cybersecurity: Federal Programs*, at 3 (R46903) (Sept. 9, 2021) (https://crsreports.congress.gov/product/pdf/R/R44939).

[2] *See id.* at 4.

[3] Cybersecurity and Infrastructure Security Agency, *Securing Industrial Control Systems:* A Unified Initiative FY 2019–2023, at 4 (July 2020) (https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf).

[4] *See Congress Steers Clear of Industrial Control Systems Cybersecurity*, CSO Online (Mar. 14, 2019) (https://www.csoonline.com/article/3365239/congress-steers-clear-of-industrial-control-systems-cybersecurity.html) (quoting one cybersecurity expert as saying that "small operators have one security person if they're that lucky" and that these operators lack the bandwidth to address ICS cybersecurity concerns).

[5] *See generally* Joseph Slowik, *Evolution of ICS Attacks and the Prospects for Future Disruptive Events*, (Feb. 25, 2019) (https://www.dragos.com/wp-content/uploads/Evolution-of-ICS Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf).

[6] *See A Hacker Tried to Poison a Florida City's Water Supply, Officials Say*, WIRED (Feb. 8, 2021) (https://www.wired.com/story/oldsmar-florida-water-utility-hack/).

[7] *See generally* Cybersecurity and Infrastructure Security Agency, *supra* note 3 (https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf).

[8] Cybersecurity and Infrastructure Security Agency, *Industrial Control Systems* (https://uscert.cisa.gov/ics) (accessed Oct. 20, 2021).

consultation with Sector Risk Management Agencies (SRMAs), Federal government efforts to identify and mitigate cybersecurity threats to ICS by maintaining current threat hunting and incident response capabilities. The bill also requires CISA to provide cybersecurity technical assistance to industry end-users, product manufacturers, SRMAs, and other ICS stakeholders to identify, evaluate, assess, and mitigate vulnerabilities. The bill requires CISA to provide a semi-annual report to Congress 180 days after the enactment of this legislation to detail its ICS capabilities.[9] Finally, the bill requires the Government Accountability Office (GAO) to detail CISA's implementation of the bill to relevant Congressional committees no later than two years after this legislation's enactment.

III. Legislative History

Senators Gary Peters (D–MI), Rob Portman (R–OH), Marco Rubio (R–FL), and Mark Warner (D–VA) introduced S. 2439 on July 22, 2021. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 2439 at a business meeting on August 4, 2021. During the business meeting, the Committee ordered the bill favorably reported *en bloc* by voice vote. Senators present for the vote on the bill were: Peters, Carper, 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 "DHS Industrial Control Systems Capabilities Enhancement Act of 2021."

Section 2. Capabilities of the Cybersecurity and Infrastructure Security Agency to identify threats to industrial control systems

Subsection (a)(1) adds a new "principle" to guide the functions of the National Cybersecurity and Communications Integration Center in 6 USC § 659(e), directing that the Center will address the security of information and operational technology, including ICS.

Subsection (a)(2) adds a new subsection, 6 USC § 659(p), instructing the Director of CISA to maintain capabilities to identify and address threats and vulnerabilities to ICS products and technology. To carry out this function, the subsection instructs the Director to: (1) identify and mitigate cybersecurity threats to industrial control systems, in consultation SMRAs; (2) maintain threat hunting and incident response capabilities; (3) provide cybersecurity technical assistance to industry users, manufacturers, SMRAs, other Federal agencies, and other ICS stakeholder to help identify, evaluate, assess, and mitigate vulnerabilities; (4) collect, coordinate, and provide vulnerability information to the ICS community by working with various stakeholders; and (5) conduct other efforts at the discretion of the Secretary of Homeland Security.

Subsection (b) requires the Director of CISA to provide regular briefings on the progress in developing these ICS capabilities to the

[9] Cybersecurity and Infrastructure Security Agency, *CISA Industrial Control Systems Security Offerings* (https://www.cisa.gov/sites/default/files/publications/ics_security_offerings_fact_sheet_S508C.pdf) (accessed Dec. 17, 2021).

House Committee on Homeland Security (CHS) and the Senate Homeland Security and Governmental Affairs Committee (HSGAC). These briefings must occur within 180 days after enactment, and must be provided every six months thereafter during the subsequent four year period.

Subsection (c) requires GAO, within two years after enactment, to review implementation of the new ICS provisions in subsection (a) and submit a report to CHS and HSGAC outlining the findings of that review and recommendations relating to implementation. That report should include information on: (1) any interagency coordination challenges; (2) the capacity, expertise, and resources that CISA has to conduct threat hunting and incident response to ICS cybersecurity threats, and any additional resources needed to close any operational gaps in those capabilities; (3) the extent to which ICS stakeholders sought cybersecurity technical assistance under the provisions of subsection (a), and the utility and effectiveness of that assistance; (4) and the degree to which CISA works with security researchers and other ICS stakeholders to provide vulnerability information to the ICS community.

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, August 24, 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. 2439, the DHS Industrial Control Systems Capabilities Enhancement Act of 2021.

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. 2439, DHS Industrial Control Systems Capabilities Enhancement Act of 2021

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on August 4, 2021

By Fiscal Year, Millions of Dollars	2021	2021-2026	2021-2031
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	*	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

* = between zero and $500,000.

S. 2439 would require the Cybersecurity and Infrastructure Security Agency (CISA) to identify and mitigate threats to systems that are used in the automated control of critical infrastructure processes (such as power generation and water treatment). The bill also would require CISA to brief the Congress on its capability to do so not later than six months after the bill's enactment and every six months thereafter over the four-year period following enactment of the bill. In addition, the bill would require the Government Accountability Office to review and report on CISA's practices for managing cybersecurity risks to industrial control systems.

CISA already assists the owners and operators of critical infrastructure with addressing security vulnerabilities in their industrial control systems. The bill would codify those responsibilities but would not impose any new operating requirements on the agency. CBO estimates that implementing S. 2439 would cost less than $500,000 over the 2021–2026 period to prepare and deliver the required briefings; such spending would be subject to the availability of appropriations.

For this estimate, CBO assumes that the bill will be enacted in fiscal year 2022.

On March 29, 2021, CBO transmitted a cost estimate for H.R. 1833, the DHS Industrial Control Systems Capabilities Enhancement Act of 2021, as ordered reported by the House Committee on Homeland Security on March 18, 2021. The two bills are similar, and CBO's estimates of their costs are similar. Differences in CBO's estimates of the cost of implementing the bills reflect the assumption that S. 2439 will be enacted in 2022.

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

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2209. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

* * * * * * *

(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) * * *

* * * * * * *

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents; [and;]

(H) the Center designates an agency contact for non-Federal entities; *and*

(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;

* * * * * * *

(p) INDUSTRIAL CONTROL SYSTEMS.—The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system

stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;

(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and

(5) conduct such other efforts and assistance as the Secretary determines appropriate.

* * * * * * *

○