Calendar No. 680

117TH CONGRESS *2d Session*	SENATE	REPORT 117–281

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING ACT

REPORT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

TO ACCOMPANY

H.R. 7777

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO AUTHORIZE THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO ESTABLISH AN INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING INITIATIVE, AND FOR OTHER PURPOSES

DECEMBER 19, 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. 680

117TH CONGRESS 2d Session | SENATE | REPORT 117–281

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING ACT

DECEMBER 19, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

REPORT

[To accompany H.R. 7777]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (H.R. 7777) to amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency to establish an industrial control systems cybersecurity training initiative, and for other purposes, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

Industrial Control Systems are information systems used to control, generally, physical industrial processes and often consist of combinations of components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective, such as manufacturing, product handling, or transportation.[1] H.R. 7777, the *Industrial Control Systems Cybersecurity Training Act*, recognizes the unique challenges in securing industrial control systems (ICS) and requires specialized training to implement such security.[2] The bill would establish an ICS Training Initiative (Initiative) at the Cybersecurity and Infrastructure Security Agency (CISA), and authorizes CISA to provide training and courses on ICS cybersecurity to public and private sector organizations. The bill requires CISA to publish an annual report on the Initiative, including future plans of the Initiative and recommendations for additional actions to strengthen ICS cybersecurity resources.

II. Background and Need for the Legislation

ICS cybersecurity is different from traditional information technology (IT) cybersecurity, in part due to the "unique performance, reliability, and safety requirements" of ICS systems.[3] Many of these differences stem from the fact that ICS systems have a direct effect on the physical world as they execute industrial processes, meaning cybersecurity risks can lead to significant physical world consequences, including on the health and safety of human lives, serious damage to the environment, and negative impacts to the nation's economy.[4]

The risks to ICS are not hypothetical. In recent years, there have been numerous threats and attacks to ICS systems, many of which are part of the country's critical infrastructure for providing lifeline services. A recent report found 93% of ICS organizations experienced an intrusion in 2022; 78% of those organizations experienced three or more intrusions.[5] In January of 2021, a hacker was able to gain access to a water treatment plant that served large parts of the San Francisco Bay area and was in a position to augment the chemical levels used in treating wastewater.[6] Similarly, in February of 2021, a hacker utilized the same exploit against an Oldsmar, Florida drinking water treatment facility.[7] In this incident, the attacker gained access to the ICS that controlled the sodium hydroxide levels in the water and raised them to poisonous levels before being manually overridden, avoiding anyone from being harmed.[8] The 2021 Colonial Pipeline cyber attack targeted

[1] National Institute of Standards and Technology, Glossary: industrial control system (ICS) (https://csrc.nist.gov/glossary/term/industrial_control_system) (accessed Dec. 12, 2022).

[2] The terms operational technology (OT) and ICS are often used interchangeably by the private sector entities who develop operate such technology, as well as cybersecurity companies that work to protect such technology. Some organizations use OT as an umbrella term with ICS as the predominant technology within OT. For purposes of this report, the term ICS will be used throughout for consistency, even though some citations refer to OT rather than ICS.

[3] National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security* (SP-800-82 Rev.3 (Draft)) (Apr. 26, 2022).

[4] National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security* (SP-800-82 Rev.3 (Draft)) (Apr. 26, 2022).

[5] Fortinet, *2022 State of Operational Technology and Cybersecurity Report* (2022) (https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf).

[6] *50,000 security disasters waiting to happen: The problem of America's water supplies,* NBC News (Jun. 17, 2021) (https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206).

[7] *50,000 security disasters waiting to happen: The problem of America's water supplies,* NBC News (Jun. 17, 2021) (https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206); *FBI Called In After Hacker Tries To Poison Tampa-Area City's Water With Lye,* NPR (Feb. 9, 2021) (https://www.npr.org/2021/02/09/965791252/fbi-called-in-after-hacker-tries-to-poison-tampa-area-citys-water-with-lye).

[8] *50,000 security disasters waiting to happen: The problem of America's water supplies,* NBC News (Jun. 17, 2021) (https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206); *FBI Called In After Hacker Tries To Poison*

the company's IT systems and the resulting multi-day shutdown of the company's pipeline and ICS technology lead to a destabilization of fuel supply across the East coast.[9] These attacks foreshadow the scale and severity that more aggressive attacks on ICS systems can yield.

Studies have shown there are hundreds of thousands of cybersecurity job openings in the United States.[10] The consequences of the is workforce shortage impact all sections, but are particularly severe for the ICS community.[11] ICS systems have unique performance and reliability requirements, thus the cybersecurity requirements are often unfamiliar or seen as unconventional to typical IT cybersecurity personnel.[12] While traditional cybersecurity education programs cover most aspects of IT cybersecurity, there are six industrial cybersecurity education domains where there is little educational focus: industrial operations, instrumentation and control, equipment, communications, safety, and regulation.[13] [14]

H.R. 7777 would help address this education gap by providing specific ICS training. H.R. 7777 would authorize CISA to provide no-cost virtual and in-person trainings and courses to help the cyber workforce develop skills that are more focused on ICS cybersecurity and the specific threats to ICS. The bill would also give Congress an annual report on the program which will highlight program progression, expansion opportunities, and the participation of women and underserved communities.

III. Legislative History

Representative Swalwell (D–CA–15) introduced H.R. 7777, the *Industrial Control Systems Cybersecurity Training Act*, on May 16, 2022. The bill was referred to the House Committee on Homeland Security. On May 19, 2022, the bill was marked up by the House Committee on Homeland Security favorably by voice vote. On June 21, 2022, the House of Representatives passed the bill under a suspension of the rules by a vote of 368 to 47. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

Tampa-Area City's Water With Lye, NPR (Feb. 9, 2021) (https://www.npr.org/2021/02/09/965791252/fbi-called-in-after-hacker-tries-to-poison-tampa-area-citys-water-with-lye).

[9] *'Juglar' of the U.S. fuel pipeline system shuts down after cyberattack,* Politico, (May 8, 2021) (https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984).

[10] While the number of openings vary, as does the methods of measuring the number of openings, the range is most often stated to be between 400,000 and 700,000 cybersecurity openings in the United States. (ISC)^2's annual Cybersecurity Workforce Study for 2022 found about 400,000 cybersecurity job openings in the United States in, while Cyber Seek found about 465,000 openings and the Biden administration has said that the number has grown to more than 700,000. *See* U.S. has almost 500,000 job openings in cybersecurity, CBS News (May 21, 2021) (https://www.cbsnews.com/news/cybersecurity-job-openings-united-states/), *Biden administration pushes to close the growing cybersecurity workforce gap,* CNN (Jul. 19, 2021) (https://www.cnn.com/2022/07/19/tech/biden-cyber-workforce-gap/index.html), and (ISC)^2, *2022 Cybersecurity Workforce Study* (2022) (https://www.isc2.org/Research/Workforce-Study).

[11] Fortinet, *2022 State of Operational Technology and Cybersecurity Report* (2022) (https://www.fortinet.com/com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf)

[12] National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security* (SP-800-82 Rev.3 (Draft)) (Apr. 26, 2022).

[13] *Building an Industrial Cybersecurity Workforce: A Manager's Guide*, Idaho State University and Idaho National Laboratory, (accessed December 7, 2022), available at https://inl.gov/wp-content/uploads/2021/02/ICS_Workforce-ManagersGuide2021.pdf.

[14] *Building an Industrial Cybersecurity Workforce: A Manager's Guide,* Idaho State University and Idaho National Laboratory, (accessed December 7, 2022), available at https://inl.gov/wp-content/uploads/2021/02/ICS_Workforce-ManagersGuide2021.pdf.

The Committee considered H.R. 7777 at a business meeting on September 28, 2022. During the business meeting, Senator Portman (R–OH) offered a modified substitute amendment that made several technical amendments and added a provision requiring CISA to consult with commercial training providers and academia to minimize the potential for duplication of other training opportunities. The Portman substitute amendment, as modified, was adopted by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Paul, Lankford, Romney, Scott, and Hawley present for the vote. The Committee ordered the bill, as amended, to be favorably reported by voice vote *en bloc*. Senators present for the vote were: Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Paul, Lankford, Romney, Scott, and Hawley.

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

Section 1. Short title

This section states that the Act may be cited as the "Industrial Control Systems Cybersecurity Training Act".

Sec. 2. Establishment of the Industrial Control Systems Training Initiative

Subsection (a) amends the Homeland Security Act of 2002 to add a new section, 2220E, which authorizes CISA to establish the Industrial Control Systems Cybersecurity Training Initiative.

Sec. 2220E subsection (a) establishes that the Initiative in order to develop and strengthen the skills of the cybersecurity workforce related to securing ICS.

Sec. 2220E subsection (b) requires CISA to include virtual and in-person trainings and courses provided at no cost to participants. Trainings and courses will be accessible to different skill levels, cover cyber defense strategies for ICS, and make appropriate considerations for the availability of trainings and courses in different regions of the United States. This section further directs CISA to engage in collaboration with the Department of Energy's National Laboratories, consultation with Sector Risk Management Agencies, and, as appropriate, consultation with private sector entities.

Sec. 2220E subsection (c) directs CISA to provide an annual report to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Government Affairs with a description of Initiative courses, outreach efforts, the number and demographics of participants, and the participation of workers from each critical infrastructure sector, along with plans for expanding access to ICS cybersecurity training and recommendations on how to improve the state of ICS cybersecurity education and training.

Subsection (b) has a clerical amendment to update the table of contents of the Homeland Security Act of 2002.

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.

VI. Congressional Budget Office Cost Estimate

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 17, 2022.

Hon. GARY C. PETERS,
Chairman, Committee on Homeland Security, and Governmental Affairs, U.S. Senate, Washington, DC.

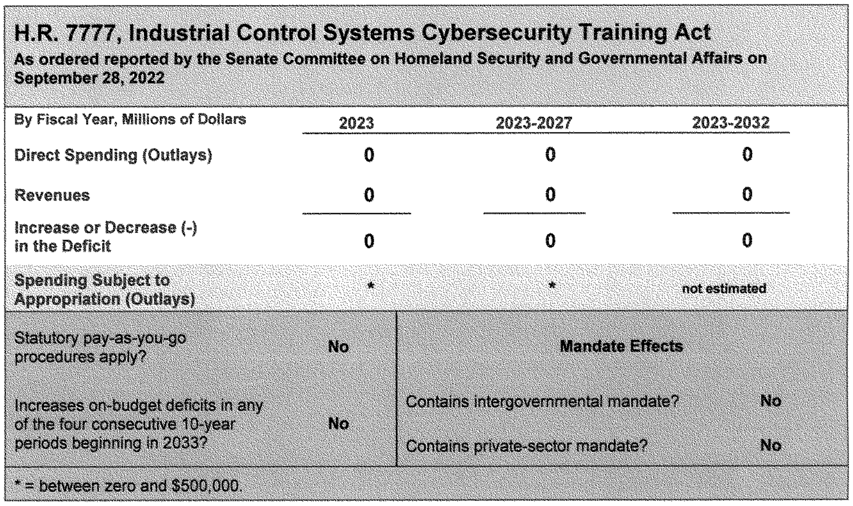
DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 7777, the Industrial Control Systems Cybersecurity Training Act.

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. 7777, Industrial Control Systems Cybersecurity Training Act

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on September 28, 2022

By Fiscal Year, Millions of Dollars	2023	2023-2027	2023-2032
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

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
		Contains intergovernmental mandate?	No
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2033?	No	Contains private-sector mandate?	No

* = between zero and $500,000.

H.R. 7777 would require the Cybersecurity and Infrastructure Security Agency (CISA) to offer voluntary cybersecurity training to critical infrastructure operators. Under the bill, CISA would teach attendees to identify and mitigate threats to information systems that are used in the automated control of critical infrastructure processes (such as power generation and water treatment). In addition, the bill would require CISA to report to the Congress on the effectiveness of its efforts.

CISA already provides cybersecurity training courses for critical infrastructure operators; thus, the bill would codify those responsibilities and would not impose any new operating requirements on the agency. CBO estimates that implementing H.R. 7777 would cost less than $500,000 over the 2023–2027 period to prepare and deliver the required reports; such spending would be subject to the availability of appropriated funds.

On June 9, 2022, CBO transmitted a cost estimate for H.R. 7777, the Industrial Control Systems Cybersecurity Training Act, as ordered reported by the House Committee on Homeland Security on

May 19, 2022. The two bills are similar, and CBO's estimates of their costs are the same.

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

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.

(a) * * *

(b) Table of Contents.—The table of contents for this Act is as follows:

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2220E. INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING INITIATIVE

(a) Establishment.—

(1) In general.—The Industrial Control Systems Cybersecurity Training Initiative (in this section referred to as the 'Initiative') is established within the Agency.

(2) Purpose.—The purpose of the Initiative is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

(b) Requirements.—In carrying out the Initiative, the Director shall—

(1) ensure the Initiative includes—

(A) virtual and in-person trainings and courses provided at no cost to participants;

(B) trainings and courses available at different skill levels, including introductory level courses;

(C) trainings and courses that cover cyber defense strategies for industrial control systems, including an understanding of the unique cyber threats facing industrial control systems and the mitigation of security vulnerabilities in industrial control systems technology; and

(D) appropriate consideration regarding the availability of trainings and courses in different regions of the United States;

(2) engage in—

(A) collaboration with the Department of Energy national laboratories in accordance with section 309;

(B) consultation with Sector Risk Management Agencies; and

(C) as appropriate, consultation with private sector entities with relevant expertise, such as vendors of industrial control systems technologies; and

(3) consult, to the maximum extent practicable, with commercial training providers and academia to minimize the potential for duplication of other training opportunities.

(c) REPORTS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, and annually thereafter, the Director 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 Initiative.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

(A) A description of the courses provided under the Initiative.

(B) A description of outreach efforts to raise awareness of the availability of such courses.

(C) The number of participants in each course.

(D) Voluntarily provided information on the demographics of participants in such courses, including by gender, race, and place of residence.

(E) Information on the participation in such courses of workers from each critical infrastructure sector.

(F) Plans for expanding access to industrial control systems education and training, including expanding access to women and underrepresented populations, and expanding access to different regions of the United States.

(G) Recommendations on how to strengthen the state of industrial control systems cybersecurity education and training.

○