117TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
117–377

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING ACT

JUNE 17, 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. 7777]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom 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 without amendment and recommends that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

H.R. 7777, the "Industrial Control Systems Cybersecurity Training Act," authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to establish the Industrial Control Systems Cybersecurity Initiative (the "Initiative") to strengthen the skills of the cybersecurity workforce related to securing industrial control systems. Through the Initiative, CISA provides no-cost virtual and in-person courses and trainings on cybersecurity for industrial control systems (ICS). In carrying out the Initiative, the bill directs CISA to engage in collaboration with the Department of Energy's National Laboratories and consultation with Sector Risk Management Agencies and, as appropriate, the private sector. Additionally, the bill directs CISA to provide an annual report on the Initiative, along with any plans and recommendations for expanding and strengthening industrial control systems cybersecurity education and training.

BACKGROUND AND NEED FOR LEGISLATION

Ensuring that the Nation's workforce has expertise across a broad range of cybersecurity disciplines is essential to strengthening the Nation's cyber defenses. Despite many efforts to address the shortage of trained cybersecurity professionals in the United States, there remain ongoing challenges. According to CyberSeek, a tool funded by the National Institute for Standards and Technology (NIST), there were 597,767 cybersecurity job openings between October 2020 and September 2021, and across the United States there are only enough cybersecurity workers to fill 68 percent of the employer demand.[1]

While cybersecurity education is often focused on information technology (IT), there are unique skills required to secure ICS as it relies on both IT and operational technology (OT) that, if exploited, could result in material harm, including loss of life, and significant economic damage. In contrast to IT cybersecurity, which prioritizes ensuring confidentiality, integrity, and availability of data, ICS cybersecurity prioritizes safety, reliability, and functionality of systems.[2] Because those working in ICS cybersecurity must understand how technology impacts industrial operations, there are additional types of training required. According to a group of industrial cybersecurity experts convened by Idaho National Laboratory and Idaho State University, there are six industrial cybersecurity knowledge domains that are not included in traditional cybersecurity education: industrial operations, instrumentation and control, equipment, communications, safety, and regulation.[3] Expanded Federal support for ICS cybersecurity training would ensure more workers have the necessary, specialized skills to protect ICS.

Recent events have highlighted the threats to ICS and the potential impact any successful attack could have. In February 2021, a cyber attack on a water treatment facility in Oldsmar, Florida, un-

---

[1] "Cybersecurity Supply/Demand Heat Map," CyberSeek, (accessed May 27, 2022), available at https://www.cyberseek.org/heatmap.html.

[2] *Building an Industrial Cybersecurity Workforce: A Manager's Guide*, Idaho State University and Idaho National Laboratory, (accessed May 31, 2022), available at https://inl.gov/wp-content/uploads/2021/02/ICS_Workforce-ManagersGuide2021.pdf.

[3] *Id.,* at p. 5.

successfully attempted to increase the level of sodium hydroxide in the city's water supply by a factor of more than 100.[4] Then, in May 2021, due to a ransomware attack on their business networks, Colonial Pipeline shut down its operational technology as a precautionary measure, resulting in significant disruption to gasoline supplies across the East Coast.[5] In April 2022, multiple Federal agencies released a Joint Cybersecurity Advisory which warned that an advanced persistent threat actor had developed malware designed to target certain ICS.[6] Because of the complexity of defending ICS, mitigating the risk posed by this malware will take time. As the threats posed to ICS only increase, additional workers will specialized skills to defend these vital systems will be needed.

To address these challenges, H.R. 7777 codifies CISA's ICS cybersecurity training program, under which CISA provides no-cost virtual and in-person trainings and courses to help workers across critical infrastructure develop the skills necessary to better defend ICS from cyber threats. H.R. 7777 also includes important oversight mechanisms by requiring an annual report to Congress on the program, along with plans and recommendations for expanding access to ICS cybersecurity training and increasing participation by women and underrepresented communities, better ensuring that the Nation's full talent pool is utilized in this important mission. These reports will also provide Congress with critical insights to develop future legislative actions that may be necessary to support the ongoing effort to strengthen the ICS cybersecurity workforce.

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. 7777:

- On July 29, 2021, the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled "The Cyber Talent Pipeline: Educating a Workforce to Match Today's Threats." The Subcommittee received testimony from Mr. Kevin Nolten, Director of Academic Outreach at CYBER.ORG; Dr. Tony Coulson, Executive Director of the Cybersecurity Center and Lead at the National Centers of Academic Excellence in Cybersecurity Community, California State University, San Bernardino; Mr. Ralph Ley, Department Manager of National and Homeland Security Workforce Development and Training at the Idaho National Laboratory; and Mr. Max Stier, President and CEO, Partnership for Public Service.

---

[4] Jack Evans, "Someone tried to poison Oldsmar's water supply during hack, sheriff says," *Tampa Bay Times,* (Feb. 9, 2021), available at https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/.

[5] Aaron Gregg, Sean Sullivan, and Stephanie Hunt, "As Colonial Pipeline recovers from cyberattack, leaders point to a 'wake-up call' for U.S. energy infrastructure," *Washington Post*, (May 13, 2021), available at https://www.washingtonpost.com/business/2021/05/13/colonial-pipeline-ransomware-gas-shortages/.

[6] Department of Energy, Cybersecurity and Infrastructure Agency, National Security Agency, and Federal Bureau of Investigation, *Joint Cybersecurity Advisory: APT Cyber Tools Targeting ICS/SCADA Devices* (April 13, 2022).

COMMITTEE CONSIDERATION

The Committee met on May 19, 2022, a quorum being present, to consider H.R. 7777 and ordered the measure to be favorably reported to the House, without amendment, 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. 7777.

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, June 9, 2022.

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. 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 House Committee on Homeland Security on May 19, 2022

By Fiscal Year, Millions of Dollars	2022	2022-2027	2022-2032
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	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2033?	No	Contains intergovernmental mandate?	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 2022–2027 period to prepare and deliver the required reports; such spending would be subject to the availability of appropriated funds.

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. 7777 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. 7777 is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

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. 7777 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 "Industrial Control Systems Cybersecurity Training Act".

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

This section authorizes the CISA to establish the Industrial Control Systems Cybersecurity Training Initiative in order to develop and strengthen the skills of the cybersecurity workforce related to securing ICS. This section establishes that the Initiative shall 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.

This section further 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.

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):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(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. 2220D. 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) training 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; and

(2) engage in—

(A) collaboration with the National Laboratories of the Department of Energy 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.

(c) REPORTS.—

(1) IN GENERAL.—Not later than one year after the date of the 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 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) Information on the number and demographics of participants in such courses, including by gender, race, and place of residence.

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

(E) 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.

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

* * * * * * *

○