II

Calendar No. 680

117TH CONGRESS
2D SESSION

H. R. 7777

[Report No. 117–281]

IN THE SENATE OF THE UNITED STATES

JUNE 22, 2022

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 19, 2022

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

AN ACT

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

~~SECTION 1. SHORT TITLE.~~

~~This Act may be cited as the "Industrial Control Systems Cybersecurity Training Act".~~

~~SEC. 2. ESTABLISHMENT OF THE INDUSTRIAL CONTROL SYSTEMS TRAINING INITIATIVE.~~

~~(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following new section:~~

~~"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) 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; 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.”.~~

~~(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2220C the following new item:~~

~~“Sec. 2220D. Industrial Control Systems Cybersecurity Training Initiative.”.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the “Industrial Control Systems Cybersecurity Training Act”.

SEC. 2. ESTABLISHMENT OF THE INDUSTRIAL CONTROL SYSTEMS TRAINING INITIATIVE.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following new section:

“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 cybersecu-

rity 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.".

(b) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by moving the item relating to section 2220D to appear after the item relating to section 2220C; and

(2) by inserting after the item relating to section 2220D the following:

"Sec. 2220E. Industrial Control Systems Cybersecurity Training Initiative.".

Calendar No. 680

117TH CONGRESS
2D SESSION

H. R. 7777

[Report No. 117–281]

AN ACT

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

Reported with an amendment