Calendar No. 547

118TH CONGRESS *2d Session*	SENATE	REPORT 118–234

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY COMPETITION ACT OF 2024

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3635

TO IMPROVE THE PRESIDENT'S CUP CYBERSECURITY COMPETITIONS

NOVEMBER 12, 2024.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
59–010 WASHINGTON : 2024

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
LAPHONZA R. BUTLER, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ALAN S. KAHN, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
EMILY A. FERGUSON, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
ANDREW J. HOPKINS, *Minority Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 547

118TH CONGRESS *2d Session* | SENATE | REPORT 118–234

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY COMPETITION ACT OF 2024

NOVEMBER 12, 2024.—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. 3635]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3635) to improve the President's Cup Cybersecurity Competitions, having considered the same, reports favorably with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 3635, the *Industrial Control Systems Cybersecurity Competition Act*, enables the Cybersecurity and Infrastructure Security Agency (CISA) to include additional competition parameters in the annual President's Cup Cybersecurity Competition. The bill authorizes the Department of Homeland Security (DHS) to include operational technology (OT) and industrial control systems (ICS) as part of the competition. Currently, the competition is not required to specifically include categories for OT and ICS.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Cyber threats to the United States are constantly evolving and cyber threat actors are developing new tools and employing new strategies to impact our national security by hacking into important systems and networks.[1] Both state-sponsored and cybercriminal actors have targeted critical infrastructure owners and operators across the nation, seeking ransoms, information, attention, and in some cases, burrowing deeply into networks to preposition for future disruptive attacks.[2] Federal experts from across the Intelligence Community, CISA, and others have repeatedly called for more attention to be paid to the cyber threats faced by critical infrastructure and to provide additional federal support to the sectors most at risk.[3] Federal employee understanding of the technical nuances of protecting critical infrastructure, such as the OT and ICS systems, is a critical component of providing support and assistance to owners and operators across the nation.[4]

The 2024 ODNI Assessment found that "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks." Additionally, it found that Russia "maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States . . .". Iran's growing levels of expertise and willingness to conduct cyber operations against vulnerable, diverse targets further highlights the threats to critical infrastructure owners and operators. North Korea's "cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States . . .".[5] Additionally, cybercriminals and ransomware gangs have increased their attacks on critical infrastructure, using the threat of disruption of service to extort public utilities and manufacturing entities.[6]

Critical infrastructure sectors rely on both IT and OT or ICS to conduct daily operations, monitor systems and networks, and ensure the safety of operations.[7] OT and ICS are considered the backbone of most critical infrastructure entities and perform essential functions such as balancing electric grids, testing chemicals in

---

[1] Department of Homeland Security, Secure Cyberspace and Critical Infrastructure (www.dhs.gov/secure-cyberspace-and-critical-infrastructure) (accessed Mar. 26, 2024).

[2] *Major US, UK Water Companies Hit by Ransomware*, Security Week (Jan. 24, 2024) (www.securityweek.com/major-us-uk-water-companies-hit-by-ransomware/); *Terrifying hacks on critical infrastructure have arrived. America isn't ready*, The Hill (Dec. 12, 2023) (thehill.com/opinion/cybersecurity/4353922-terrifying-hacks-on-critical-infrastructure-have-arrived-america-isnt-ready/); *High-impact attacks on critical infrastructure climb 140%*, Security Intelligence (June 26, 2023) (securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/).

[3] Government Accountability Office, *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure* (GAO–23–106441) (Feb. 7, 2023).

[4] Government Accountability Office, *Improvements Needed in Addressing Risks to Operational Technology* (GAO–24–106576) (Mar. 7, 2024).

[5] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 11, 2024) (www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf).

[6] *Cyberattacks Wreaking Physical Disruption on the Rise*, Dark Reading (Apr. 2, 2024) (www.darkreading.com/ics-ot-security/cyberattacks-wreaking-physical-disruption-on-the-rise); National Security Agency, *Urgent Warning from Multiple Cybersecurity Organizations on Current Threat to OT Systems*, Press Release (May 1, 2024) (www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3761830/urgent-warning-from-multiple-cybersecurity-organizations-on-current-threat-to-o/).

[7] Cybersecurity and Infrastructure Security Agency, *Securing Industrial Control Systems: A Unified Initiative* (Jul. 2020) (www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf).

drinking water, and assembling vehicles in factories.[8] Historically and theoretically, successful attacks on OT and ICS can have an oversized impact on critical infrastructure compared to IT.[9] An example of a successful attack includes the 2015 Ukraine power grid attack which cut off power to a large number of customers in the middle of winter.[10] More recently, an Iranian-backed cyber group infiltrated water utility networks across the United States in a display of protest of the conflict in Gaza.[11]

In March 2024, the Government Accountability Office (GAO) published a report highlighting CISA's struggle to plan and respond to potential significant attacks across critical infrastructure systems, noting that there were very limited staff with OT/ICS-specific competency.[12] As part of these engagements with critical infrastructure, CISA and other federal employees must understand the nuances in operating and protecting IT, OT, and ICS.

A technical training opportunity for federal employees is the annual President's Cup Cybersecurity Competition. Established in 2019 by E.O. 13870, the competition trains, identifies, and rewards the best cybersecurity talent in the federal workforce, including military members.[13] CISA leads and hosts the annual competition as part of their mission to expand the size and capabilities of the cyber workforce, and the competition typically draws over a thousand participants. Participants are tested in a series of challenges following the National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The challenges include tasks related to cyber defense of networks, exploitation of systems, cyber forensics, and other technical skills.[14] Currently, the President's Cup Cybersecurity Competition does not require categories related to skills needed to defend OT or ICS networks and systems.[15]

This bill mandates the President's Cup Cybersecurity Competition to expand its parameters to include OT and ICS in addition to IT categories at least every other competition. This will ideally

---

[8] Microsoft CEE Multi-Country News Center, *Cyber risks to critical infrastructure are on the rise* (June 26, 2023) (news.microsoft.com/en-cee/2023/06/26/cyber-risks-to-critical-infrastructure-are-on-the-rise/).

[9] The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Information Technology and Operational Technology Convergence* (Aug. 23, 2022) (www.cisa.gov/sites/default/files/publications/NSTAC%20IT-OT%20Convergence%20Report_508%20Compliant_0.pdf); *1 in 4 Organizations Shut Down OT Operations Due to Cyberattacks: Survey,* Security Week (Mar. 20, 2024) (www.securityweek.com/1-in-4-organizations-shut-down-ot-operations-due-to-cyberattacks-survey/); *A Cyberattack on the U.S. Power Grid*, Council on Foreign Relations (April 2017) (backend-live.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf).

[10] Cybersecurity and Infrastructure Security Agency, *Cyber-Attack Against Ukrainian Critical Infrastructure* (July 20, 2021) (www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01); *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, Wired (Mar. 3, 2016) (www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/).

[11] *Breaches by Iran-Affiliated Hackers Spanned Multiple U.S. States, Federal Agencies Say*, AP News (Dec. 2, 2023) (apnews.com/article/hackers-iran-israel-water-utilities-critical-infrastructure-cisa-554b2aa969c8220016ab2ef94bd7635b); *Federal government investigating multiple hacks of US water utilities*, Politico (Nov. 28, 2023) (www.politico.com/news/2023/11/28/federal-government-investigating-multiple-hacks-of-us-water-utilities-00128977#:~:text=Politico%20Logo&text=The%20federal%20government%20is%20investigating,individuals%20familiar%20with%20the%20probes).

[12] Government Accountability Office, Cybersecurity: Improvements Needed in Addressing Risks to Operational Technology (GAO–24–106576) (Mar. 7, 2024) (https://www.gao.gov/assets/d24106576.pdf).

[13] Exec. Order No. 13870, 84 FR 20523 (May 2, 2019).

[14] Cybersecurity and Infrastructure Security Agency, *President's Cup FAQs* (www.cisa.gov/presidents-cup-faqs) (Accessed Mar. 26, 2024).

[15] Cybersecurity and Infrastructure Security Agency, President's Cup Cybersecurity Competition Challenge Repository (github.com/cisagov/prescup-challenges).

improve cybersecurity by training federal employees on OT and ICS in addition to IT, increasing employee familiarity with the nuances of these systems, and allowing employees to more quickly respond to cyber incidents across critical infrastructure. Without a skilled workforce, threat hunting and incident response services voluntarily provided by the federal government to critical infrastructure entities would be less effective during significant cyberattacks.[16]

III. Legislative History

Senator Gary C. Peters (D–MI) introduced S. 3635, the *Industrial Control Systems Cybersecurity Competition Act*, on January 22, 2024, with original cosponsor Senator Mike Braun (R–IN). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 3635 at a business meeting on January 31, 2024. At the business meeting, Senator Peters offered a substitute amendment to the bill along with a modification to the substitute amendment. The Peters substitute amendment as twice modified changed the bill to include spending caps on the competition, a requirement to submit reports to Congress before initiating a new competition, a sunset, and no new funding. The Committee adopted the modification to the Peters substitute amendment, and the Peters substitute amendment as modified, by unanimous consent, with Senators Peters, Carper, Hassan, Rosen, Ossoff, Paul, Lankford, Romney, Scott, and Marshall present.

The bill, amended by the Peters substitute amendment as twice modified, was ordered reported favorably by roll call vote of 9 yeas to 1 nay with Senators Peters, Carper, Hassan, Rosen, Ossoff, Lankford, Romney, Scott, and Marshall voting in the affirmative, and Senator Paul voting in the negative. Senators Sinema, Blumenthal, Butler, and Hawley voted yea by proxy, for the record only, and Senator Johnson voting in the negative by proxy, for the record only.

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

Section 1. Short title

This section establishes the short title of the bill as the "Industrial Control Systems Cybersecurity Competition Act."

Section 2. President's cup cybersecurity competitions

Subsection (a) amends Section 7121 of the Homeland Security Act of 2002 (6 U.S.C. 665m) by striking subsection (d) paragraph (3), designating paragraphs (1), (2), and (4) as subparagraphs (A), (B), and (C), and striking "each competition". It adds a biennial requirement that the competition incorporate categories demonstrating offensive and defensive cyber operations involving information technology, operational technology or industrial control systems, or other categories of technology systems at determined appropriate. This subsection also provides for 20% caps on spending in items in subparagraph (A), (B), (C), and (D). Additionally, this

[16] Government Accountability Office, Cybersecurity: Improvements Needed in Addressing Risks to Operational Technology (GAO–24–106576) (Mar. 7, 2024) (https://www.gao.gov/assets/d24106576.pdf).

subsection adds a requirement that the Director cannot hold a competition until the report for the previous year has been submitted to Congress. This subsection also adds a sunset of 5 years to the competition.

Subsection (b) adds no additional funds allowed to be appropriated for the purpose of carrying out the amendments made by the bill.

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

S. 3635, Industrial Control Systems Cybersecurity Competition Act

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on January 31, 2024

By Fiscal Year, Millions of Dollars	2024	2024-2029	2024-2034
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	0	0

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2035?	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 2035?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

S. 3635 would add new categories to an awards competition for the federal cybersecurity workforce that is conducted by the Cybersecurity and Infrastructure Security Agency (CISA). The bill would expand the categories comprising CISA's awards program to include knowledge of cyber threats to systems that are used in the automated control of critical infrastructure processes (such as power generation and water treatment).

S. 3635 would not impose any new operating requirements on CISA, nor would it amend the cap on the total amount of money that can be awarded annually through the competition. As a result, CBO estimates that enacting the bill would not affect the federal budget.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Christina Hawley Anthony, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

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):

UNITED STATES CODE

* * * * * * *

TITLE 6—DOMESTIC SECURITY

* * * * * * *

CHAPTER 1—HOMELAND SECURITY ORGANIZATION

* * * * * * *

SUBCHAPTER XVIII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

SEC. 665m. PRESIDENT'S CUP CYBERSECURITY COMPETITION

(a) * * *
(b) * * *
(c) * * *
(d) COMPETITION PARAMETERS—

[Each competition**]** *(1) IN GENERAL.—Each Competition* shall incorporate the following elements:

[(1)**]***(A)* * * *

[(2)**]***(B)* * * *

[(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, or cyber-physical systems.**]**

[(4)**]***(C)* Any other elements related to [paragraphs (1), (2), or (3)] *subparagraph (A) or (B)*, as determined necessary by the Director.

(2) BIENNIAL REQUIREMENTS.—Not less frequently than every second competition, the competition shall incorporate categories demonstrating offensive and defensive cyber operations involving—

(A) information technology (as defined in section 11101 of title 40, United States Code), such as software reverse engineering and exploitation, network operations, forensics, big

data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, and obfuscated coding;

(B) operational technology (as defined in section 3 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a)) or industrial control systems (as defined in section 2220C of the Homeland Security Act of 2002 (6 U.S.C. 665i)), such as knowledge of supervisory control and data acquisition systems and the protocols and communication methods used in such systems, detection of anomalies, exploitation of operational technology or industrial control systems, and responding to and recovering after incidents involving operational technology or industrial control systems; or

(C) any other category of technological system requiring cybersecurity or information security, as determined appropriate by the Director.

(e) USE OF FUNDS.—

(1) IN GENERAL.—

In order to further the goals and objectives of the competition, the Director may use amounts made available to the Director for the competition for reasonable expenses for the following:

(A) Advertising, marketing, and promoting the competition, *which shall not exceed 20 percent of the amounts made available for the competition during any fiscal year.*

(B) Meals for participants and organizers of the competition if attendance at the meal during the competition is necessary to maintain the integrity of the competition, *which shall not exceed 20 percent of the amounts made available for the competition during any fiscal year.*

(C) Promotional items, including merchandise and apparel, *which shall not exceed 20 percent of the amounts made available for the competition during any fiscal year.*

(D) Consistent with section 4503 of title 5, necessary expenses for the honorary recognition of competition participants, including members of the uniformed services, *which shall not exceed 20 percent of the amounts made available for the competition during any fiscal year.*

* * * * * * *

(h) LIMITATION.—The Director may not hold an annual cybersecurity competition under this section for a year until after the Director submits the report required under subsection (g) with respect to the competition held under this section during the previous year.

(i) SUNSET.—The Director may not conduct a competition under the authority under this section on or after the first day of the first year that begins more than 5 years after the date of enactment of the Industrial Control Systems Cybersecurity Competition Act.

* * * * * * *

○