

118TH CONGRESS
2D SESSION

S. 3635

To improve the President’s Cup Cybersecurity Competitions.

IN THE SENATE OF THE UNITED STATES

JANUARY 22, 2024

Mr. PETERS (for himself and Mr. BRAUN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To improve the President’s Cup Cybersecurity Competitions.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Industrial Control Sys-
5 tems Cybersecurity Competition Act”.

6 **SEC. 2. PRESIDENT’S CUP CYBERSECURITY COMPETITIONS.**

7 Section 7121(d) of the James M. Inhofe National De-
8 fense Authorization Act for Fiscal Year 2023 (6 U.S.C.
9 665m(d)) is amended—

10 (1) by striking paragraph (3);

1 (2) by redesignating paragraphs (1), (2), and
2 (4) as subparagraphs (A), (B), and (C), respectively,
3 and adjusting the margin accordingly;

4 (3) by striking “Each competition” and insert-
5 ing the following:

6 “(1) IN GENERAL.—Each competition”;

7 (4) in subparagraph (C) of paragraph (1), as so
8 redesignated, by striking “paragraphs (1), (2), or
9 (3)” and inserting “subparagraph (A) or (B)”; and

10 (5) by adding at the end the following:

11 “(2) BIENNIAL REQUIREMENTS.—Not less fre-
12 quently than every second competition, the competi-
13 tion shall incorporate categories demonstrating of-
14 fensive and defensive cyber operations involving—

15 “(A) information technology (as defined in
16 section 11101 of title 40, United States Code),
17 such as software reverse engineering and exploi-
18 tation, network operations, forensics, big data
19 analysis, cyber analysis, cyber defense, cyber ex-
20 ploitation, secure programming, and obfuscated
21 coding;

22 “(B) operational technology (as defined in
23 section 3 of the IoT Cybersecurity Improvement
24 Act of 2020 (15 U.S.C. 278g–3a)) or industrial
25 control systems (as defined in section 2220C of

1 the Homeland Security Act of 2002 (6 U.S.C.
2 665i)), such as knowledge of supervisory control
3 and data acquisition systems and the protocols
4 and communication methods used in these sys-
5 tems, detection of anomalies, and responding to
6 and recovering after incidents involving such
7 systems; or

8 “(C) any other category of technological
9 system requiring cybersecurity or information
10 security, as determined appropriate by the Di-
11 rector.”.

○