

115TH CONGRESS  
2D SESSION

# H. R. 5733

---

IN THE SENATE OF THE UNITED STATES

JUNE 26, 2018

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

---

## AN ACT

To amend the Homeland Security Act of 2002 to provide for the responsibility of the National Cybersecurity and Communications Integration Center to maintain capabilities to identify threats to industrial control systems, and for other purposes.

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

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “DHS Industrial Con-  
3 trol Systems Capabilities Enhancement Act of 2018”.

4 **SEC. 2. CAPABILITIES OF NATIONAL CYBERSECURITY AND**  
5 **COMMUNICATIONS INTEGRATION CENTER TO**  
6 **IDENTIFY THREATS TO INDUSTRIAL CON-**  
7 **TROL SYSTEMS.**

8 (a) IN GENERAL.—Section 227 of the Homeland Se-  
9 curity Act of 2002 (6 U.S.C. 148) is amended—

10 (1) in subsection (e)(1)—

11 (A) in subparagraph (G), by striking  
12 “and” after the semicolon;

13 (B) in subparagraph (H), by inserting  
14 “and” after the semicolon; and

15 (C) by adding at the end the following new  
16 subparagraph:

17 “(I) activities of the Center address the se-  
18 curity of both information technology and oper-  
19 ational technology, including industrial control  
20 systems;”;

21 (2) by redesignating subsections (f) through  
22 (m) as subsections (g) through (n), respectively; and

23 (3) by inserting after subsection (d) the fol-  
24 lowing new subsection:

25 “(f) INDUSTRIAL CONTROL SYSTEMS.—The Center  
26 shall maintain capabilities to identify and address threats

1 and vulnerabilities to products and technologies intended  
2 for use in the automated control of critical infrastructure  
3 processes. In carrying out this subsection, the Center  
4 shall—

5           “(1) lead, in coordination with relevant sector  
6 specific agencies, Federal Government efforts to  
7 identify and mitigate cybersecurity threats to indus-  
8 trial control systems, including supervisory control  
9 and data acquisition systems;

10           “(2) maintain cross-sector incident response ca-  
11 pabilities to respond to industrial control system cy-  
12 bersecurity incidents;

13           “(3) provide cybersecurity technical assistance  
14 to industry end-users, product manufacturers, and  
15 other industrial control system stakeholders to iden-  
16 tify and mitigate vulnerabilities;

17           “(4) collect, coordinate, and provide vulner-  
18 ability information to the industrial control systems  
19 community by, as appropriate, working closely with  
20 security researchers, industry end-users, product  
21 manufacturers, and other industrial control systems  
22 stakeholders; and

23           “(5) conduct such other efforts and assistance  
24 as the Secretary determines appropriate.”.

1 (b) REPORT TO CONGRESS.—Not later than 180 days  
2 after the date of the enactment of this Act, and every 6  
3 months thereafter during the subsequent 4-year period,  
4 the National Cybersecurity and Communications Integra-  
5 tion Center shall provide to the Committee on Homeland  
6 Security of the House of Representatives and the Com-  
7 mittee on Homeland Security and Governmental Affairs  
8 of the Senate a briefing on the industrial control systems  
9 capabilities of the Center under subsection (f) of section  
10 227 of the Homeland Security Act of 2002 (6 U.S.C.  
11 148), as added by subsection (a).

Passed the House of Representatives June 25, 2018.

Attest:

KAREN L. HAAS,

*Clerk.*