

115TH CONGRESS
2D SESSION

S. 3182

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.

IN THE SENATE OF THE UNITED STATES

JUNE 28, 2018

Mr. SASSE introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

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,*

3 **SECTION 1. SHORT TITLE.**

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

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

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

7 (1) in subsection (e)(1)—

8 (A) in subparagraph (G), by striking
 9 “and;” after the first semicolon;

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

12 (C) by adding at the end the following new
 13 subparagraph:

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

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

20 (3) by inserting after subsection (e) the fol-
 21 lowing new subsection:

22 “(f) INDUSTRIAL CONTROL SYSTEMS.—The Center
 23 shall maintain capabilities to identify and address threats
 24 and vulnerabilities to products and technologies intended
 25 for use in the automated control of critical infrastructure

1 processes. In carrying out this subsection, the Center
2 shall—

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

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

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

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

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

23 (b) REPORT TO CONGRESS.—Not later than 180 days
24 after the date of enactment of this Act, and every 6
25 months thereafter during the subsequent 4-year period,

1 the National Cybersecurity and Communications Integra-
2 tion Center shall provide to the Committee on Homeland
3 Security of the House of Representatives and the Com-
4 mittee on Homeland Security and Governmental Affairs
5 of the Senate a briefing on the industrial control systems
6 capabilities of the Center under subsection (f) of section
7 227 of the Homeland Security Act of 2002 (6 U.S.C.
8 148), as added by subsection (a).

○