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.

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 ''DHS Industrial Control Systems Capabilities Enhancement Act of 2018''.

SEC. 2. CAPABILITIES OF NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS.

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

(1) in subsection (e)(1)—

(A) in subparagraph (G), by striking ''and;'' after the first semicolon;

(B) in subparagraph (H), by inserting ''and'' after the semicolon; and

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

''(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;'';

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

(3) by inserting after subsection (e) the following new subsection:

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

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

''(1) lead, in coordination with relevant sector specific agencies, Federal Government efforts to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

''(2) maintain cross-sector incident response capabilities to respond to industrial control system cybersecurity incidents;

''(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, and other industrial control system stakeholders to identify and mitigate vulnerabilities;

''(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, and other industrial control systems stakeholders; and

''(5) conduct such other efforts and assistance as the Secretary determines appropriate.''.

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

the National Cybersecurity and Communications Integration Center shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the industrial control systems capabilities of the Center under subsection (f) of section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148), as added by subsection (a).

○