117TH CONGRESS
1ST SESSION

S. 2439

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

IN THE SENATE OF THE UNITED STATES

JULY 22, 2021

Mr. PETERS (for himself, Mr. PORTMAN, Mr. RUBIO, and Mr. WARNER) 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 Cybersecurity and Infrastructure Security Agency 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 2021".

SEC. 2. CAPABILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS.

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (e)(1)—

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

(2) by adding at the end the following new subsection:

''(p) INDUSTRIAL CONTROL SYSTEMS.—The Director 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 Director shall—

''(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

''(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

''(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, 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, Sector Risk Management Agencies, other Federal agencies, 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 the enactment of this Act and every 6

months thereafter during the subsequent 4-year period, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a briefing on the industrial control systems capabilities of the Agency under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a).

(c) GAO REVIEW.—Not later than two years after the date of the enactment of this Act, the Comptroller General of the United States shall review implementation of the requirements of subsections (e)(1)(I) and (p) of section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a), and submit to the Committee on Homeland Security and Government Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report containing findings and recommendations relating to such implementation. Such report shall include information on the following:

(1) Any interagency coordination challenges to the ability of the Director of the Cybersecurity and Infrastructure Agency of the Department of Home-

land Security to lead Federal efforts to identify and mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(1) of such section 2209.

(2) The degree to which the Agency has adequate capacity, expertise, and resources to carry out threat hunting and incident response capabilities to mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(2) of such section 2209, as well as additional resources that would be needed to close any operational gaps in such capabilities.

(3) The extent to which industrial control system stakeholders sought cybersecurity technical assistance from the Agency pursuant to subsection (p)(3) of such section 2209, and the utility and effectiveness of such technical assistance.

(4) The degree to which the Agency works with security researchers and other industrial control systems stakeholders, pursuant to subsection (p)(4) of such section 2209, to provide vulnerability information to the industrial control systems community.

○