

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.

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 2021”.

1 **SEC. 2. CAPABILITIES OF THE CYBERSECURITY AND INFRA-**  
2 **STRUCTURE SECURITY AGENCY TO IDENTIFY**  
3 **THREATS TO INDUSTRIAL CONTROL SYS-**  
4 **TEMS.**

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

7 (1) in subsection (e)(1)—

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

18 (2) by adding at the end the following new sub-  
19 section:

20 “(p) INDUSTRIAL CONTROL SYSTEMS.—The Director  
21 shall maintain capabilities to identify and address threats  
22 and vulnerabilities to products and technologies intended  
23 for use in the automated control of critical infrastructure  
24 processes. In carrying out this subsection, the Director  
25 shall—

1           “(1) lead Federal Government efforts, in con-  
2           sultation with Sector Risk Management Agencies, as  
3           appropriate, to identify and mitigate cybersecurity  
4           threats to industrial control systems, including su-  
5           pervisory control and data acquisition systems;

6           “(2) maintain threat hunting and incident re-  
7           sponse capabilities to respond to industrial control  
8           system cybersecurity risks and incidents;

9           “(3) provide cybersecurity technical assistance  
10          to industry end-users, product manufacturers, Sector  
11          Risk Management Agencies, other Federal agencies,  
12          and other industrial control system stakeholders to  
13          identify, evaluate, assess, and mitigate  
14          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, Sector Risk Management Agencies,  
20          other Federal agencies, and other industrial control  
21          systems stakeholders; and

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

24          (b) REPORT TO CONGRESS.—Not later than 180 days  
25          after the date of the enactment of this Act and every 6

1 months thereafter during the subsequent 4-year period,  
2 the Director of the Cybersecurity and Infrastructure Secu-  
3 rity Agency of the Department of Homeland Security shall  
4 provide to the Committee on Homeland Security and Gov-  
5 ernmental Affairs of the Senate and the Committee on  
6 Homeland Security of the House of Representatives a  
7 briefing on the industrial control systems capabilities of  
8 the Agency under section 2209 of the Homeland Security  
9 Act of 2002 (6 U.S.C. 659), as amended by subsection  
10 (a).

11 (c) GAO REVIEW.—Not later than two years after  
12 the date of the enactment of this Act, the Comptroller  
13 General of the United States shall review implementation  
14 of the requirements of subsections (e)(1)(I) and (p) of sec-  
15 tion 2209 of the Homeland Security Act of 2002 (6 U.S.C.  
16 659), as amended by subsection (a), and submit to the  
17 Committee on Homeland Security and Government Affairs  
18 of the Senate and the Committee on Homeland Security  
19 of the House of Representatives a report containing find-  
20 ings and recommendations relating to such implementa-  
21 tion. Such report shall include information on the fol-  
22 lowing:

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

1 land Security to lead Federal efforts to identify and  
2 mitigate cybersecurity threats to industrial control  
3 systems pursuant to subsection (p)(1) of such sec-  
4 tion 2209.

5 (2) The degree to which the Agency has ade-  
6 quate capacity, expertise, and resources to carry out  
7 threat hunting and incident response capabilities to  
8 mitigate cybersecurity threats to industrial control  
9 systems pursuant to subsection (p)(2) of such sec-  
10 tion 2209, as well as additional resources that would  
11 be needed to close any operational gaps in such ca-  
12 pabilities.

13 (3) The extent to which industrial control sys-  
14 tem stakeholders sought cybersecurity technical as-  
15 sistance from the Agency pursuant to subsection  
16 (p)(3) of such section 2209, and the utility and ef-  
17 fectiveness of such technical assistance.

18 (4) The degree to which the Agency works with  
19 security researchers and other industrial control sys-  
20 tems stakeholders, pursuant to subsection (p)(4) of  
21 such section 2209, to provide vulnerability informa-  
22 tion to the industrial control systems community.

○