

116TH CONGRESS
2D SESSION

S. 4795

To require the Secretary of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, and for other purposes.

IN THE SENATE OF THE UNITED STATES

OCTOBER 1, 2020

Ms. ROSEN (for herself and Mr. HOEVEN) introduced the following bill; which was read twice and referred to the Committee on Energy and Natural Resources

A BILL

To require the Secretary of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, 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 “Cyber Sense Act of
5 2020”.

6 **SEC. 2. CYBER SENSE PROGRAM.**

7 (a) **DEFINITIONS.**—In this section:

1 (1) BULK-POWER SYSTEM.—The term “bulk-
2 power system” has the meaning given the term in
3 section 215(a) of the Federal Power Act (16 U.S.C.
4 824o(a)).

5 (2) CRITICAL ELECTRIC INFRASTRUCTURE.—
6 The term “critical electric infrastructure” has the
7 meaning given the term in section 215A(a) of the
8 Federal Power Act (16 U.S.C. 824o–1(a)).

9 (3) PROGRAM.—The term “program” means
10 the voluntary Cyber Sense program established
11 under subsection (b).

12 (4) SECRETARY.—The term “Secretary” means
13 the Secretary of Energy.

14 (b) ESTABLISHMENT.—The Secretary, in coordina-
15 tion with the heads of other relevant Federal agencies,
16 shall establish a voluntary Cyber Sense program to test
17 the cybersecurity of products and technologies intended
18 for use in the bulk-power system.

19 (c) PROGRAM REQUIREMENTS.—In carrying out sub-
20 section (b), the Secretary shall—

21 (1) establish a testing process under the pro-
22 gram to test the cybersecurity of products and tech-
23 nologies intended for use in the bulk-power system,
24 including products relating to industrial control sys-

1 tems and operational technologies, such as super-
2 visory control and data acquisition systems;

3 (2) for products and technologies tested under
4 the program, establish and maintain cybersecurity
5 vulnerability reporting processes and a related data-
6 base;

7 (3) provide technical assistance to electric utili-
8 ties, product manufacturers, and other electricity
9 sector stakeholders to develop solutions to mitigate
10 identified cybersecurity vulnerabilities in products
11 and technologies tested under the program;

12 (4) biennially review products and technologies
13 tested under the program for cybersecurity
14 vulnerabilities and provide analysis with respect to
15 how those products and technologies respond to and
16 mitigate cyber threats;

17 (5) develop guidance that is informed by anal-
18 ysis and testing results under the program for elec-
19 tric utilities for the procurement of products and
20 technologies;

21 (6) provide reasonable notice to, and solicit
22 comments from, the public prior to establishing or
23 revising the testing process under the program;

24 (7) oversee the testing of products and tech-
25 nologies under the program; and

1 (8) consider incentives to encourage the use of
2 analysis and results of testing under the program in
3 the design of products and technologies for use in
4 the bulk-power system.

5 (d) DISCLOSURE OF INFORMATION.—Any cybersecu-
6 rity vulnerability reported pursuant to a process estab-
7 lished under subsection (c)(2), the disclosure of which the
8 Secretary reasonably foresees would cause harm to critical
9 electric infrastructure, shall be considered to be critical
10 electric infrastructure information for purposes of section
11 215A(d) of the Federal Power Act (16 U.S.C. 824o–1(d)).

12 (e) FEDERAL GOVERNMENT LIABILITY.—Nothing in
13 this section authorizes the commencement of an action
14 against the United States with respect to the testing of
15 a product or technology under the program.

○