II

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.

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 ''Cyber Sense Act of 2020''.

SEC. 2. CYBER SENSE PROGRAM.

(a) DEFINITIONS.—In this section:

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

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

(3) PROGRAM.—The term ''program'' means the voluntary Cyber Sense program established under subsection (b).

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Energy.

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

(c) PROGRAM REQUIREMENTS.—In carrying out subsection (b), the Secretary shall—

(1) establish a testing process under the program to test the cybersecurity of products and technologies intended for use in the bulk-power system, including products relating to industrial control sys-

tems and operational technologies, such as supervisory control and data acquisition systems;

(2) for products and technologies tested under the program, establish and maintain cybersecurity vulnerability reporting processes and a related database;

(3) provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to develop solutions to mitigate identified cybersecurity vulnerabilities in products and technologies tested under the program;

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

(5) develop guidance that is informed by analysis and testing results under the program for electric utilities for the procurement of products and technologies;

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

(7) oversee the testing of products and technologies under the program; and

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

(d) DISCLOSURE OF INFORMATION.—Any cybersecurity vulnerability reported pursuant to a process established under subsection (c)(2), the disclosure of which the Secretary reasonably foresees would cause harm to critical electric infrastructure, shall be considered to be critical electric infrastructure information for purposes of section 215A(d) of the Federal Power Act (16 U.S.C. 824o–1(d)).

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

○