I

115TH CONGRESS
2D SESSION

H. R. 5239

To require the Secretary of Energy to establish a voluntary Cyber Sense program to identify and promote cyber-secure products intended for use in the bulk-power system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 9, 2018

Mr. LATTA (for himself and Mr. MCNERNEY) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To require the Secretary of Energy to establish a voluntary Cyber Sense program to identify and promote cyber-secure products 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 2018''.

SEC. 2. CYBER SENSE.

(a) IN GENERAL.—The Secretary of Energy shall establish a voluntary Cyber Sense program to identify and

promote cyber-secure products intended for use in the bulk-power system, as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)).

(b) PROGRAM REQUIREMENTS.—In carrying out subsection (a), the Secretary of Energy shall—

(1) establish a Cyber Sense testing process to identify products and technologies intended for use in the bulk-power system that are cyber-secure, including products relating to industrial control systems, such as supervisory control and data acquisition systems;

(2) for products tested and identified as cyber-secure under the Cyber Sense 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 tested and identified as cyber-secure under the Cyber Sense program;

(4) biennially review products tested and identified as cyber-secure under the Cyber Sense program for cybersecurity vulnerabilities and provide analysis

with respect to how such products respond to and mitigate cyber threats;

(5) develop procurement guidance for electric utilities for products tested and identified as cyber-secure under the Cyber Sense program;

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

(7) establish procedures for disqualifying products that were tested and identified as cyber-secure under the Cyber Sense program but that no longer meet the qualifications to be identified cyber-secure products under such program;

(8) oversee Cyber Sense testing carried out by third parties; and

(9) consider incentives to encourage the use in the bulk-power system of products tested and identified as cyber-secure under the Cyber Sense program.

(c) DISCLOSURE OF INFORMATION.—Any cybersecurity vulnerability reported pursuant to the process established under subsection (b)(2), the disclosure of which the Secretary of Energy reasonably foresees would cause harm to critical electric infrastructure (as defined in section 215A of the Federal Power Act), shall be deemed to be

critical electric infrastructure information for purposes of section 215A(d) of the Federal Power Act.

(d) FEDERAL GOVERNMENT LIABILITY.—Nothing in this section shall be construed to authorize the commencement of an action against the United States Government with respect to the testing and identification of a product under the Cyber Sense program.

○