I

115TH CONGRESS
1ST SESSION

H. R. 3855

To require a report on significant security risks of the national electric grid and the potential effect of such security risks on the readiness of the Armed Forces.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 27, 2017

Ms. ROSEN (for herself, Ms. STEFANIK, Mr. LIPINSKI, and Mr. FITZPATRICK) introduced the following bill; which was referred to the Committee on Armed Services

---

A BILL

To require a report on significant security risks of the national electric grid and the potential effect of such security risks on the readiness of the Armed Forces.

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 ''Securing the Electric Grid to Protect Military Readiness Act of 2017''.

SEC. 2. REPORT ON SIGNIFICANT SECURITY RISKS OF DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE.

(a) REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall, in coordination with the Director of National Intelligence, the Secretary of Energy, and the Secretary of Homeland Security, submit to the appropriate committees of Congress a report setting forth the following:

(1) Identification of significant security risks to defense critical electric infrastructure posed by significant malicious cyber-enabled activities.

(2) An assessment of the potential effect of the security risks identified pursuant to paragraph (1) on the readiness of the Armed Forces.

(3) An assessment of the strategic benefits derived from, and the challenges associated with, isolating military infrastructure from the national electric grid and the use of microgrids by the Armed Forces.

(4) Recommendations on actions to be taken—

(A) to eliminate or mitigate the security risks identified pursuant to paragraph (1); and

(B) to address the effect of those security risks on the readiness of the Armed Forces identified pursuant to paragraph (2).

(b) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) DEFINITIONS.—In this section:

(1) The term ''appropriate committees of Congress'' means—

(A) the congressional defense committees (as defined in section 101(a) of title 10, United States Code);

(B) the Committee on Energy and Natural Resources and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Energy and Commerce and the Committee on Homeland Security of the House of Representatives.

(2) The term ''defense critical electric infrastructure''—

(A) has the meaning given such term in section 215A(a) of the Federal Power Act (16 U.S.C. 824o–1(a)); and

(B) shall include any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility—

(i) designated by the Secretary of Defense as—

(I) critical to the defense of the United States; and

(II) vulnerable to a disruption of the supply of electric energy provided to such facility by an external provider; and

(ii) that is not owned or operated by the owner or operator of such facility.

(3) The term ''security risk'' shall have such meaning as the Secretary of Defense shall determine, in coordination with the Director of National Intelligence and the Secretary of Energy, for purposes of the report required by subsection (a).

(4) The term ''significant malicious cyber-enabled activities'' include—

(A) significant efforts—

(i) to deny access to or degrade, disrupt, or destroy an information and communications technology system or network; or

(ii) to exfiltrate, degrade, corrupt, destroy, or release information from such a system or network without authorization for purposes of—

(I) conducting influence operations; or

(II) causing a significant misappropriation of funds, economic resources, trade secrets, personal identifications, or financial information for commercial or competitive advantage or private financial gain;

(B) significant destructive malware attacks; and

(C) significant denial of service activities.

○