

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.

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 “Securing the Electric  
5 Grid to Protect Military Readiness Act of 2017”.

1 **SEC. 2. REPORT ON SIGNIFICANT SECURITY RISKS OF DE-**  
2 **FENSE CRITICAL ELECTRIC INFRASTRUC-**  
3 **TURE.**

4 (a) REPORT REQUIRED.—Not later than 90 days  
5 after the date of the enactment of this Act, the Secretary  
6 of Defense shall, in coordination with the Director of Na-  
7 tional Intelligence, the Secretary of Energy, and the Sec-  
8 retary of Homeland Security, submit to the appropriate  
9 committees of Congress a report setting forth the fol-  
10 lowing:

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

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

17 (3) An assessment of the strategic benefits de-  
18 rived from, and the challenges associated with, iso-  
19 lating military infrastructure from the national elec-  
20 tric grid and the use of microgrids by the Armed  
21 Forces.

22 (4) Recommendations on actions to be taken—  
23 (A) to eliminate or mitigate the security  
24 risks identified pursuant to paragraph (1); and

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

4 (b) FORM OF REPORT.—The report required by sub-  
5 section (a) shall be submitted in unclassified form, but  
6 may include a classified annex.

7 (c) DEFINITIONS.—In this section:

8 (1) The term “appropriate committees of Con-  
9 gress” means—

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

13 (B) the Committee on Energy and Natural  
14 Resources and the Committee on Homeland Se-  
15 curity and Governmental Affairs of the Senate;  
16 and

17 (C) the Committee on Energy and Com-  
18 merce and the Committee on Homeland Secu-  
19 rity of the House of Representatives.

20 (2) The term “defense critical electric infra-  
21 structure”—

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

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

4 (i) designated by the Secretary of De-  
5 fense as—

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

8 (II) vulnerable to a disruption of  
9 the supply of electric energy provided  
10 to such facility by an external pro-  
11 vider; and

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

14 (3) The term “security risk” shall have such  
15 meaning as the Secretary of Defense shall deter-  
16 mine, in coordination with the Director of National  
17 Intelligence and the Secretary of Energy, for pur-  
18 poses of the report required by subsection (a).

19 (4) The term “significant malicious cyber-en-  
20 abled activities” include—

21 (A) significant efforts—

22 (i) to deny access to or degrade, dis-  
23 rupt, or destroy an information and com-  
24 munications technology system or network;

25 or

- 1                   (ii) to exfiltrate, degrade, corrupt, de-  
2                   stroy, or release information from such a  
3                   system or network without authorization  
4                   for purposes of—
- 5                   (I) conducting influence oper-  
6                   ations; or
- 7                   (II) causing a significant mis-  
8                   appropriation of funds, economic re-  
9                   sources, trade secrets, personal identi-  
10                  fications, or financial information for  
11                  commercial or competitive advantage  
12                  or private financial gain;
- 13                  (B) significant destructive malware at-  
14                  tacks; and
- 15                  (C) significant denial of service activities.

○