

115TH CONGRESS  
1ST SESSION

# H. R. 940

To secure communications of utilities from terrorist threats, and for other purposes.

---

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 7, 2017

Ms. JACKSON LEE introduced the following bill; which was referred to the Committee on Homeland Security

---

## A BILL

To secure communications of utilities from terrorist threats, 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 “Securing Communica-  
5 tions of Utilities from Terrorist Threats” or the  
6 “SCOUTS Act”.

7 **SEC. 2. POLICY.**

8 (a) SECURITY AND RESILIENCE.—The Secretary of  
9 Homeland Security, in coordination with the sector-spe-  
10 cific agencies, may work with critical infrastructure own-

1 ers and operators and State, local, tribal, and territorial  
2 entities to seek voluntary participation of such agencies  
3 to determine how the Department of Homeland Security  
4 can best serve the sector-specific cybersecurity needs to  
5 manage risk and strengthen the security and resilience of  
6 the Nation's critical infrastructure against terrorist at-  
7 tacks that could have a debilitating impact on national se-  
8 curity, economic stability, public health and safety, or any  
9 combination thereof.

10 (b) OBJECTIVES.—In implementing subsection (a),  
11 the Secretary shall seek to reduce vulnerabilities, minimize  
12 consequences, identify and disrupt terrorism threats, and  
13 hasten response and recovery efforts related to impacted  
14 critical infrastructures.

15 (c) INVESTIGATION OF BEST MEANS TO ENGAGE  
16 OWNERS AND OPERATORS.—The Secretary, in coordina-  
17 tion with the sector-specific agencies, may investigate the  
18 best means for engaging sector-specific agencies in partici-  
19 pation in a voluntary cybersecurity information sharing,  
20 emergency support, and emerging threat awareness pro-  
21 gram.

22 (d) LISTENING OPPORTUNITY.—The Secretary shall  
23 establish voluntary opportunities for sector-specific agen-  
24 cies and critical infrastructure owners and operators to in-

1 form the Department of Homeland Security of sector-spe-  
2 cific challenges to cybersecurity, including regarding—

3 (1) what needs they may have or may not have  
4 regarding critical infrastructure protection; and

5 (2) how the Department of Homeland Security  
6 is or is not helping to meet those needs that have  
7 been identified, through voluntary participation.

8 (e) GAO REPORT.—The Comptroller General of the  
9 United States shall report to the Congress by not later  
10 than 6 months after the date of the enactment of this Act  
11 on the views, experiences, and preferences of critical infra-  
12 structure owners and operators regarding the benefits of  
13 engaging in voluntary cybersecurity incident reporting, in-  
14 telligence gathering, and technical support resources pro-  
15 vided by the Department of Homeland Security.

16 (f) INTERNATIONAL PARTNERS.—The Secretary  
17 shall, in consultation with appropriate Federal agencies,  
18 establish terrorism prevention policy to engage with inter-  
19 national partners to strengthen the security and resilience  
20 of domestic critical infrastructure and critical infrastruc-  
21 ture located outside of the United States, or in its terri-  
22 torial waters, on which the Nation depends.

23 **SEC. 3. STRATEGIC IMPERATIVES.**

24 (a) RESEARCH AND REPORT ON THE MOST EFFI-  
25 CIENT MEANS FOR INFORMATION EXCHANGE BY IDENTI-

1 FYING BASELINE DATA AND SYSTEMS REQUIREMENTS  
2 FOR THE FEDERAL GOVERNMENT.—The Secretary shall  
3 facilitate the timely exchange of terrorism threat and vul-  
4 nerability information as well as information that allows  
5 for the development of a situational awareness capability  
6 for Federal civilian agencies during terrorist incidents.  
7 The goal of such facilitation is to enable efficient informa-  
8 tion exchange through the identification of requirements  
9 for data and information formats and accessibility, system  
10 interoperability, and redundant systems and alternate ca-  
11 pabilities should there be a disruption in the primary sys-  
12 tems.

13 (b) IMPLEMENTATION OF AN INTEGRATION AND  
14 ANALYSIS FUNCTION TO INFORM PLANNING AND OPER-  
15 ATIONAL DECISIONS REGARDING THE PROTECTION OF  
16 CRITICAL INFRASTRUCTURE FROM TERRORISM  
17 EVENTS.—The Secretary of Homeland Security shall im-  
18 plement an integration and analysis function for critical  
19 infrastructure that includes operational and strategic  
20 analysis on terrorism incidents, threats, and emerging  
21 risks. Such function shall include establishment by the  
22 Secretary of integration of data sharing capabilities with  
23 Fusion Centers that accomplish the following:

24 (1) Determine the appropriate role that Fusion  
25 Centers may fill in reporting data related to cyberse-

1 security threat or incident information regarding indi-  
2 viduals or service providers with access to or ongoing  
3 business relationships with critical infrastructure.

4 (2) Determine whether or how the National  
5 Protection and Programs Directorate and the Na-  
6 tional Cybersecurity and Communications Integra-  
7 tion Center may work with Fusion Centers to report  
8 possible cybersecurity incidents.

9 (3) Determine a means for Fusion Centers to  
10 report availability of critical infrastructure to sup-  
11 port local, State, Federal, tribal, and territorial law  
12 enforcement and the provision of basic public serv-  
13 ices after disruption events such as electric power  
14 brownouts and blackouts, accidents that disrupt  
15 service, and vandalism to or near facilities.

16 (4) Categorize and prioritize cybersecurity in-  
17 take risk information based on relevance to critical  
18 infrastructure owners or operators in the area served  
19 by the Fusion Center.

20 (5) Establish an emerging threat hotline and  
21 secure online sector-specific cybersecurity incident  
22 reporting portal by which information may be dis-  
23 seminated through Fusion Centers.

24 (6) Develop, keep up to date, and make avail-  
25 able a Federal agency directory of designated offices

1 or individuals tasked with responding to, mitigating,  
2 or assisting in recovery from cybersecurity incidents  
3 involving critical infrastructure and make the direc-  
4 tory available on a voluntary basis to critical infra-  
5 structure owners and operators.

6 (7) Establish a voluntary incident access portal  
7 with the ability to allow users to determine the  
8 means, methods, and level of incident reporting that  
9 is sector-specific and relevant to the recipient as de-  
10 fined and controlled by the recipient.

11 (8) Gather voluntary feedback from critical in-  
12 frastructure owners and operators on the value, rel-  
13 evance, and timeliness of the information received,  
14 which shall include how they believe information and  
15 the means used to disseminate that information  
16 might be improved.

17 (9) Report to Congress every 2 years on the  
18 voluntary participation of critical infrastructure own-  
19 ers and operators in the programs established under  
20 this title.

21 (10) Implement a capability to collate, assess,  
22 and integrate vulnerability and consequence informa-  
23 tion with threat streams and hazard information  
24 to—

1 (A) evaluate the impact of cybersecurity  
2 and cyberphysical impacts of critical physical  
3 assets;

4 (B) aid in prioritizing assets and managing  
5 risks to critical infrastructure in impacted  
6 areas;

7 (C) determine, through the voluntary co-  
8 operation of critical infrastructure owners and  
9 operators, the staffing and professional need for  
10 cybersecurity critical infrastructure protection  
11 with Fusion Centers;

12 (D) determine, through coordination with  
13 the sector-specific agencies, the agency staffing  
14 needed to support cybersecurity critical infra-  
15 structure protection and report the findings to  
16 Congress;

17 (E) research and report findings regarding  
18 the feasibility of exploring terrorist incident cor-  
19 relations between critical infrastructure dam-  
20 age, destruction, and diminished capacity, and  
21 what occurs during certain natural disasters;

22 (F) anticipate interdependencies and cas-  
23 cading impacts related to cyber telecommuni-  
24 cations failures;

1 (G) recommend security and resilience  
2 measures for critical infrastructure prior to,  
3 during, and after a terrorism event or incident;

4 (H) evaluate interdependencies and cas-  
5 cading impacts related to electric grid failures;

6 (I) support post-terrorism incident man-  
7 agement and restoration efforts related to crit-  
8 ical infrastructure; and

9 (J) make recommendations on preventing  
10 the collapse or serious degrading of the tele-  
11 communication capability in an area impacted  
12 by a terrorism event.

13 (11) Support the Department of Homeland Se-  
14 curity’s ability to maintain and share, as a common  
15 Federal service, a near real-time situational aware-  
16 ness capability for critical infrastructure that in-  
17 cludes actionable information about imminent ter-  
18 rorist threats, significant trends, and awareness of  
19 incidents that may impact critical infrastructure.

20 **SEC. 4. DEFINITIONS.**

21 For purposes of this Act:

22 (1) **CRITICAL INFRASTRUCTURE.**—The term  
23 “critical infrastructure” means systems and assets,  
24 whether physical or virtual, so vital to the United  
25 States that the incapacity or destruction of such sys-



1       tems and assets would have a debilitating impact on  
2       security, national economic security, national public  
3       health or safety, or any combination of those mat-  
4       ters.

5           (2) RESILIENCE.—The term “resilience” means  
6       the ability to prepare for and adapt to changing con-  
7       ditions and withstand and recover rapidly from dis-  
8       ruptions. The term includes the ability to withstand  
9       and recover from deliberate attacks, accidents, or  
10      naturally occurring threats or incidents.

11          (3) SECTOR-SPECIFIC AGENCY.—The term “sec-  
12      tor-specific agency” means a Federal department or  
13      agency designated as a Sector-Specific Agency by  
14      Presidential Policy Directive 21, relating to Critical  
15      Infrastructure Security and Resilience.

16          (4) SECURITY.—The term “security” means re-  
17      ducing the risk to critical infrastructure by physical  
18      means or defense cyber measures to intrusions, at-  
19      tacks, or the effects of terrorist intrusions or at-  
20      tacks.

○