I

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.

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 Communications of Utilities from Terrorist Threats'' or the ''SCOUTS Act''.

SEC. 2. POLICY.

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

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

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

(c) INVESTIGATION OF BEST MEANS TO ENGAGE OWNERS AND OPERATORS.—The Secretary, in coordination with the sector-specific agencies, may investigate the best means for engaging sector-specific agencies in participation in a voluntary cybersecurity information sharing, emergency support, and emerging threat awareness program.

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

form the Department of Homeland Security of sector-specific challenges to cybersecurity, including regarding—

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

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

(e) GAO REPORT.—The Comptroller General of the United States shall report to the Congress by not later than 6 months after the date of the enactment of this Act on the views, experiences, and preferences of critical infrastructure owners and operators regarding the benefits of engaging in voluntary cybersecurity incident reporting, intelligence gathering, and technical support resources provided by the Department of Homeland Security.

(f) INTERNATIONAL PARTNERS.—The Secretary shall, in consultation with appropriate Federal agencies, establish terrorism prevention policy to engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States, or in its territorial waters, on which the Nation depends.

SEC. 3. STRATEGIC IMPERATIVES.

(a) RESEARCH AND REPORT ON THE MOST EFFICIENT MEANS FOR INFORMATION EXCHANGE BY IDENTI-

fying Baseline Data and Systems Requirements for the Federal Government.—The Secretary shall facilitate the timely exchange of terrorism threat and vulnerability information as well as information that allows for the development of a situational awareness capability for Federal civilian agencies during terrorist incidents. The goal of such facilitation is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.

(b) Implementation of an Integration and Analysis Function To Inform Planning and Operational Decisions Regarding the Protection of Critical Infrastructure From Terrorism Events.—The Secretary of Homeland Security shall implement an integration and analysis function for critical infrastructure that includes operational and strategic analysis on terrorism incidents, threats, and emerging risks. Such function shall include establishment by the Secretary of integration of data sharing capabilities with Fusion Centers that accomplish the following:

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

curity threat or incident information regarding individuals or service providers with access to or ongoing business relationships with critical infrastructure.

(2) Determine whether or how the National Protection and Programs Directorate and the National Cybersecurity and Communications Integration Center may work with Fusion Centers to report possible cybersecurity incidents.

(3) Determine a means for Fusion Centers to report availability of critical infrastructure to support local, State, Federal, tribal, and territorial law enforcement and the provision of basic public services after disruption events such as electric power brownouts and blackouts, accidents that disrupt service, and vandalism to or near facilities.

(4) Categorize and prioritize cybersecurity intake risk information based on relevance to critical infrastructure owners or operators in the area served by the Fusion Center.

(5) Establish an emerging threat hotline and secure online sector-specific cybersecurity incident reporting portal by which information may be disseminated through Fusion Centers.

(6) Develop, keep up to date, and make available a Federal agency directory of designated offices

or individuals tasked with responding to, mitigating, or assisting in recovery from cybersecurity incidents involving critical infrastructure and make the directory available on a voluntary basis to critical infrastructure owners and operators.

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

(8) Gather voluntary feedback from critical infrastructure owners and operators on the value, relevance, and timeliness of the information received, which shall include how they believe information and the means used to disseminate that information might be improved.

(9) Report to Congress every 2 years on the voluntary participation of critical infrastructure owners and operators in the programs established under this title.

(10) Implement a capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to—

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

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

(C) determine, through the voluntary cooperation of critical infrastructure owners and operators, the staffing and professional need for cybersecurity critical infrastructure protection with Fusion Centers;

(D) determine, through coordination with the sector-specific agencies, the agency staffing needed to support cybersecurity critical infrastructure protection and report the findings to Congress;

(E) research and report findings regarding the feasibility of exploring terrorist incident correlations between critical infrastructure damage, destruction, and diminished capacity, and what occurs during certain natural disasters;

(F) anticipate interdependencies and cascading impacts related to cyber telecommunications failures;

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

(H) evaluate interdependencies and cascading impacts related to electric grid failures;

(I) support post-terrorism incident management and restoration efforts related to critical infrastructure; and

(J) make recommendations on preventing the collapse or serious degrading of the telecommunication capability in an area impacted by a terrorism event.

(11) Support the Department of Homeland Security's ability to maintain and share, as a common Federal service, a near real-time situational awareness capability for critical infrastructure that includes actionable information about imminent terrorist threats, significant trends, and awareness of incidents that may impact critical infrastructure.

SEC. 4. DEFINITIONS.

For purposes of this Act:

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

tems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(2) RESILIENCE.—The term ''resilience'' means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. The term includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

(3) SECTOR-SPECIFIC AGENCY.—The term ''sector-specific agency'' means a Federal department or agency designated as a Sector-Specific Agency by Presidential Policy Directive 21, relating to Critical Infrastructure Security and Resilience.

(4) SECURITY.—The term ''security'' means reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of terrorist intrusions or attacks.

○