I

115TH CONGRESS
1ST SESSION

H. R. 945

To codify the objective of Presidential Policy Directive 21 to improve critical infrastructure security and resilience, 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 codify the objective of Presidential Policy Directive 21 to improve critical infrastructure security and resilience, 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 ''Terrorism Prevention and Critical Infrastructure Protection Act of 2017''.

SEC. 2. FINDINGS.

The Congress finds the following:

(1) The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary

to strengthen and maintain secure, functioning, and resilient critical infrastructure, including assets, networks, and systems, that are vital to public confidence and the Nation's safety, prosperity, and well-being.

(2) The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyber space, and governance constructs that involve multilevel authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

(3) Critical infrastructure must be secured against terrorist attacks, and must be designed and maintained in such a way as to withstand and recover quickly in the event of an attack. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery efforts.

SEC. 3. POLICY.

(a) SECURITY AND RESILIENCE.—The Secretary of Homeland Security shall work with critical infrastructure owners and operators and SLTTs to take proactive steps 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. Such efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt terrorism threats, and hasten response and recovery efforts related to critical infrastructure.

(b) 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 on which the Nation depends.

(c) INTEGRATED, HOLISTIC APPROACH.—

(1) RESEARCH TASK FORCE.—The Secretary shall establish a research task force to conduct research into the best means and methods to address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect critical

infrastructure's interconnectedness and interdependency.

(2) DUTIES OF THE RESEARCH TASK FORCE.—The research task force shall provide the Secretary with—

(A) a list of critical infrastructure;

(B) the degree the critical infrastructure is reliant upon other infrastructure;

(C) the cyber preparedness of suppliers, contractors, or service providers of critical infrastructure;

(D) programs, projects, or professional development for persons responsible for the security and operation of critical infrastructure; and

(E) vulnerabilities and threats that are found in software systems, firewalls, applications, and methods of accessing systems.

(3) MEMBERSHIP.—The research task force shall consist of 19 members appointed by the Secretary. The Secretary shall appoint one member to represent each of—

(A) the National Institutes of Standards and Technology;

(B) the Association of Computing Machinery;

(C) IEEE (formerly the Institute of Electrical and Electronic Engineers);

(D) Carnegie Mellon Cylabs;

(E) the Edison Electric Institute;

(F) the National Telecommunication and Information Administration;

(G) the Utilities Telecom Council;

(H) the US Oil and Gas Association;

(I) the American Chemistry Council;

(J) the American Fuel and Petrochemical Manufacturers;

(K) the Pharmaceutical Research Manufacturers of America; and

(L) the National Oceanic and Atmospheric Administration.

(4) REPORT.—The research task force shall provide a research report to the Secretary on its findings and recommendations 180 days after its establishment.

(5) CRITICAL INFRASTRUCTURE DEFINED.—In this subsection, the term ''critical infrastructure'' means infrastructure of—

(A) energy capture, refining, manufacturing, and delivery systems;

(B) transportation and transportation systems;

(C) water and sewer capture, processing, and delivery systems;

(D) healthcare systems, with respect to preventing threats to the quality and safety of medicines, medical devices, and delivery of life-saving health care services;

(E) food production, processing, and delivery systems;

(F) virtual and physical communication systems;

(G) financial systems; and

(H) the electricity grid.

(d) STRATEGIC IMPERATIVES.—

(1) IN GENERAL.—The Secretary shall establish the Strategic Research Imperatives Program, which shall have the responsibility of leading the Department of Homeland Security's Federal civilian agency approach to strengthen critical infrastructure security and resilience.

(2) DUTIES.—The duties of the program are the following:

(A) Collect data, refine and clarify functional relationships across the Federal Govern-

ment to advance the national unity of effort to strengthen critical infrastructure, terrorism prevention, security, and resilience.

(B) Investigate effective measures that support information exchange by identifying baseline data and systems requirements for the Federal Government.

(C) Recommend methods to implement an integration and analysis function to inform planning and operations decisions regarding the protection of critical infrastructure from terrorist threats.

(e) GUIDANCE.—The Secretary of Homeland Security shall make available research findings and guidance to Federal civilian department and agency heads (or their designees) for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure to assist in the prevention, mediation, and recovery from terrorism events.

SEC. 4. ROLES AND RESPONSIBILITIES.

(a) UNITY OF EFFORT.—

(1) IN GENERAL.—The Secretary shall establish and appoint a research working group that shall—

(A) study and make recommendations on how best to achieve and implement national

unity of effort to protect against terrorism threats, through investigation of strategic guidance from existing laws, Presidential policy directives, and Executive orders; and

(B) investigate the security and resilience of the Nation's information assurance components that provide protection against terrorism threats.

(2) IN-DEPTH APPROACH.—The research working group shall also consider research by subject-matter experts on cyber security in-depth approaches that study the following, and make recommendations thereon to the Secretary:

(A) The program of the Department of Homeland Security to secure Federal agencies and critical infrastructure to create resilient secure computer systems and networks.

(B) Cyber security preparedness of vendors, contractors, or nongovernment agency entities that provide computer-related support or services to critical infrastructure owners and operators as well as government agencies charged with securing them.

(C) Investigation of the feasibility of developing industry- or sector-specific computer emergency rapid response teams.

(D) The feasibility of the agency developing a guest visiting security researchers program to provide instruction to private sector and civilian agency personnel responsible for cyber security.

(3) MEMBERSHIP.—The research working group shall be comprised of individuals with expertise and day-to-day engagement from the sector-specific agency terrorism prevention, remediation, and response experts, as well as the specialized or support terrorism prevention capabilities of other Federal departments and agencies, as well as experts who engage in strong collaboration with critical infrastructure owners and operators and SLTTs, and academic researchers with in-depth knowledge in computing security.

(b) SECRETARY OF HOMELAND SECURITY.—

(1) IN GENERAL.—The Secretary of Homeland Security shall establish a research program to provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to

promote the security and resilience of the Nation's critical infrastructure from terrorist threats.

(2) ADDITIONAL ROLES AND RESPONSIBILITIES.—Additional roles and responsibilities for the Secretary of Homeland Security include the following:

(A) Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences of terrorist attacks, in coordination with SSAs and other Federal departments and agencies.

(B) Maintain national terrorism critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about potential terrorist trends, imminent terrorist threats, and the status of terrorist incidents that may impact critical infrastructure.

(C) In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators on terrorism prevention security protocols and facilitate access to and exchange of information and intelligence necessary to strengthen

the security and resilience of critical infrastructure.

(D) Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTTs and critical infrastructure owners and operators.

(E) Coordinate Federal Government responses to cyber or physical terrorism incidents affecting critical infrastructure consistent with statutory authorities.

(F) Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and terrorist attacks against critical infrastructure.

(G) Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies.

(H) Report annually to Congress on the status of national critical infrastructure efforts to meet the objectives of this section.

(c) SECTOR-SPECIFIC AGENCIES.—Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, the head of each SSA shall carry out the following roles and responsibilities for their respective sectors:

(1) Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities related to cyber security critical infrastructure protection from terrorism.

(2) Carry out terrorism incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations.

(3) Provide, support, or facilitate technical assistance and consultations for such sectors to identify vulnerabilities and help mitigate terrorism incidents, as appropriate.

(d) RESEARCH AND REPORT ON BEST PRACTICES FOR COORDINATING.—The Secretary shall conduct research and submit a report to Congress not later than 180 days after the date of the enactment of this Act on the best practices for coordinating with civilian agencies, private sector critical infrastructure owners, local, State, tribal, and territorial agencies, other relevant Federal depart-

ments and agencies, where appropriate with independent regulatory agencies, and SLTTs, as appropriate, to implement this Act.

SEC. 5. STRATEGIC IMPERATIVES.

(a) RESEARCH AND REPORT ON THE MOST EFFICIENT MEANS FOR INFORMATION EXCHANGE BY IDENTIFYING 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 2 national centers to accomplish the following:

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

(A) aid in prioritizing assets and managing risks to critical infrastructure;

(B) determine the staffing and professional need for cyber security critical infrastructure protection;

(C) determine the agency staffing needed and to support cyber security critical infrastructure protection and report the findings to Congress;

(D) 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;

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

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

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

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

(2) 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 affect critical infrastructure.

SEC. 6. PROTECTION OF PRIVACY AND CIVIL LIBERTIES.

(a) IN GENERAL.—The Secretary of Homeland Security shall support greater terrorism cyber security information sharing by civilian Federal agencies with the private sector that protects constitutional privacy and civil liberties rights. The heads of Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with

applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee terrorism program information sharing properly.

(b) ENSURING INDEPENDENCE OF PRIVACY OFFICER.—

(1) IN GENERAL.—Section 222 of the Homeland Security Act of 2002 (6 U.S.C. 142) is amended—

(A) in subsection (a), by striking so much as precedes paragraph (1) and inserting the following:

''(a) IN GENERAL.—There shall be in the Department a Privacy Officer who shall be appointed by the President, by and with the advice and consent of the Senate. The Privacy Officer shall report directly to the Secretary, and shall have primary responsibility in the Department for privacy policy, including—'';

(B) by striking ''senior official appointed under subsection (a)'' each place it appears and inserting ''Privacy Officer'';

(C) in subsection (b)(1)(A), by striking ''senior official'' and inserting ''Privacy Officer'';

(D) in subsection (b)(1)(B), by striking ''senior official's'' and inserting ''Privacy Officer's'';

(E) in subsection (b)(1)(C), by striking ''senior official'' and inserting ''Privacy Officer'';

(F) in subsection (b)(1)(D), by striking ''senior official'' and inserting ''Privacy Officer'';

(G) in subsection (c)(2)(B), by striking ''senior official'' each place it appears and inserting ''Privacy Officer'';

(H) in the heading for subsection (c)(2)(B)(iii), by striking ''BY SENIOR OFFICIAL'';

(I) in subsection (d), by striking ''the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department'' and inserting ''individual appointed as Privacy Officer'';

(J) in the heading for subsection (e), by striking ''BY SENIOR OFFICIAL''; and

(K) in subsection (e)—

(i) by striking ''senior official'' and inserting ''Privacy Officer''; and

(ii) by striking ''senior official's'' each place it appears and inserting ''Privacy Officer''.

(2) CONTINUED SERVICE.—The senior official serving as the Privacy Officer of the Department of Homeland Security immediately before the enactment of this Act may continue to act as the Privacy Officer until a successor is appointed in accordance with the amendments made by this subsection.

SEC. 7. INNOVATION AND RESEARCH AND DEVELOPMENT.

The Secretary of Homeland Security may consult with other Federal departments and agencies to produce and submit to congressional oversight committees a report on how best to align federally funded research and development activities that seek to strengthen the security and resilience of the Nation's critical infrastructure, including—

(1) promoting research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;

(2) enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, and cascading effects on other sectors;

(3) facilitating initiatives to incentivize cyber security investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and

(4) prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

SEC. 8. IMPLEMENTATION BY DEPARTMENT OF HOMELAND SECURITY.

(a) CRITICAL INFRASTRUCTURE TERRORISM PREVENTION SECURITY AND COMPUTER NETWORK RESILIENCE FUNCTIONAL RELATIONSHIPS.—

(1) IN GENERAL.—Within 120 days after the date of the enactment of this Act, the Secretary of Homeland Security shall conduct research and develop a description of the functional relationships within the Department of Homeland Security and across the Federal Government related to critical infrastructure security and resilience. The description shall—

(A) include the roles and functions of the 2 national critical infrastructure centers and a discussion of the analysis and integration function;

(B) serve as a roadmap for critical infrastructure owners and operators and SLTTs to navigate the Federal Government's functions and primary points of contact assigned to those functions for critical infrastructure security and resilience against both physical and cyber threats; and

(C) include identification of every contact within the Federal Government for critical infrastructure protection security and resilience, by company and industry.

(2) COORDINATION.—The Secretary shall prepare a report on efforts to coordinate this effort with the SSAs and other relevant Federal departments and agencies.

(3) PROVISION TO PRESIDENT.—The Secretary shall provide the description, supported by agency-conducted research, to the President through the Assistant to the President for Homeland Security and Counterterrorism, and to the relevant congressional homeland security oversight committees.

(b) EVALUATION OF THE EXISTING PUBLIC-PRIVATE PARTNERSHIP MODEL.—

(1) IN GENERAL.—Within 150 days after the date of the enactment of this Act, the Secretary of

Homeland Security, in coordination with the SSAs, other relevant Federal departments and agencies, SLTTs, and critical infrastructure owners and operators, shall conduct an analysis of the existing public-private partnership model, evaluate its effectiveness, and recommend options for improving the effectiveness of the partnership in both the physical and cyber space.

(2) CONTENTS.—The research and recommendations shall—

(A) consider options to streamline or automate (or both) processes for collaboration and exchange of terrorism-related information and to minimize duplication of effort;

(B) consider how the model for terrorism information exchange can be flexible and adaptable to meet the unique needs of individual critical infrastructure sectors while providing a focused, disciplined, and effective approach for the Federal Government to coordinate with the critical infrastructure owners and operators and with SLTTs governments; and

(C) result in recommendations to enhance partnerships to be approved for implementation by the President.

(c) IDENTIFICATION OF BASELINE DATA AND SYSTEMS REQUIREMENTS FOR THE FEDERAL GOVERNMENT TO ENABLE EFFICIENT INFORMATION EXCHANGE.—

(1) IN GENERAL.—Within 18 months after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the SSAs and other Federal departments and agencies, shall convene a team of researchers to identify baseline data and systems requirements—

(A) to enable the efficient exchange of terrorism information and intelligence relevant to strengthening the security and resilience of critical infrastructure; and

(B) for sharing of data and interoperability of systems to enable the timely exchange of terrorism or terrorist threat data and information to secure critical infrastructure and make it more resilient.

(2) EXPERTS INCLUDED.—The experts shall include representatives from—

(A) those entities that routinely possess information important to critical infrastructure security and resilience;

(B) those entities that determine and manage information technology systems used to exchange information; and

(C) those entities responsible for the security of information being exchanged.

(3) ANALYSIS.—Analysis by such team of experts shall include—

(A) interoperability with critical infrastructure partners;

(B) identification of key data and the information requirements of key Federal, SLTT, and private sector entities;

(C) availability, accessibility, and formats of data;

(D) the ability to exchange various classifications of information;

(E) the security of those systems to be used; and

(F) appropriate protections for individual privacy and civil liberties.

(4) PROVISION TO PRESIDENT.—The Secretary shall provide such analysis to the President through the Assistant to the President for Homeland Security and Counterterrorism, and to congressional homeland security oversight committees.

(d) DEVELOP A RESEARCH PROGRAM TO INFORM THE AGENCY OF A SITUATIONAL AWARENESS CAPABILITY FOR CRITICAL INFRASTRUCTURE.—Within 2 years after the date of the enactment of this Act, the Secretary of Homeland Security shall demonstrate a near real-time situational awareness, research-based pilot project for critical infrastructure that—

(1) includes threat streams and all-hazards information as well as vulnerabilities;

(2) provides the status of critical infrastructure and potential cascading effects;

(3) supports decisionmaking;

(4) disseminates critical information that may be needed to save or sustain lives, mitigate damage, or reduce further degradation of a critical infrastructure capability throughout an incident; and

(5) is available for and covers physical and cyber elements of critical infrastructure, and enables an integration of information as necessitated by an incident.

(e) UPDATE TO NATIONAL INFRASTRUCTURE PROTECTION PLAN.—

(1) IN GENERAL.—Within 18 months after the date of the enactment of this Act, the Secretary of Homeland Security shall provide to the President,

through the Assistant to the President for Homeland Security and Counterterrorism and the congressional homeland security oversight committees, a research report that outlines the National Infrastructure Protection Plan to address the implementation of this Act, the requirements of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.), and alignment with the National Preparedness Goal and System required by Presidential Policy Directive 8.

(2) CONTENTS.—The plan shall include—

(A) identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure against terrorist threats;

(B) the methods to be used to prioritize critical infrastructure in the event of a terrorism event that impacts multiple infrastructure systems;

(C) the protocols to be used to synchronize communication and actions within the Federal Government to effectively respond to critical infrastructure terrorist threats or events; and

(D) a metrics and analysis process to be used to measure the Nation's ability to manage

and reduce terrorism risks to critical infrastructure.

(3) RELATIONSHIP TO OTHER PROVISIONS.—The plan shall reflect the terrorism threat identification, prevention, mediation, and recovery relationships within the Department of Homeland Security and across the Federal Government identified under this Act and the updates to the public-private partnership model under this Act.

(4) ENERGY AND COMMUNICATION SYSTEMS.—The plan shall consider sector dependencies on energy and communications systems during a terrorism event, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems.

(5) COORDINATION.—The Secretary shall coordinate activities under this subsection with the SSAs, other relevant Federal departments and agencies, SLTTs, and critical infrastructure owners and operators.

(6) RESPONSE PLANS.—The plan shall include an analysis of the feasibility of developing terrorism response plans, based on research conducted on the resilience of critical infrastructure when faced with terrorism threats, that focus on action plans to

achieve a level of function and eventual recovery of full operability of critical infrastructure post-cyber attack.

(f) NATIONAL CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE R&D PLAN.—Within 2 years after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy, the SSAs, the Department of Commerce, and other Federal departments and agencies, shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Security and Resilience Research and Development Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide research and development requirements and investments. The Secretary shall reissue the plan every 4 years after its initial issuance, and make interim updates as needed.

(g) CONSISTENCY IN PPD–1.—Policy coordination, dispute resolution, and periodic in-progress reviews for the implementation of this Act shall be carried out consistent with Presidential Policy Directive 1, including the use of interagency policy committees coordinated by the national security staff.

(h) RELATIONSHIP TO OTHER AUTHORITIES.—Nothing in this Act alters, supersedes, or impedes the authorities of Federal departments and agencies, including independent regulatory agencies, to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives, including the designation of critical infrastructure under such authorities.

SEC. 9. DESIGNATION OF CRITICAL INFRASTRUCTURE SECTORS AND SECTOR-SPECIFIC AGENCIES.

(a) DESIGNATION.—

(1) IN GENERAL.—For purposes of this Act, the Secretary of Homeland Security shall determine which critical infrastructure sectors and sector specific agencies for such sectors should be engaged in efforts to detect, deter, mitigate, and lead recovery efforts related to terrorist incidents.

(2) CULTIVATION OF RELATIONSHIPS.—The Secretary shall evaluate the appropriate relationships among Federal agencies, SSAs, SLTTs, and critical infrastructure owners and operators to establish the most effective defense against terrorist attacks.

(b) FUNCTION.—The Secretary shall provide institutional knowledge and specialized expertise to lead, facili-

tate, or support security and resilience programs and associated terrorism prevention activities with respect to sectors designated under subsection (a)(1).

(c) CHANGES.—The Secretary of Homeland Security shall periodically evaluate the need for and make changes to plans and evaluations made under this section. The Secretary shall consult with the Assistant to the President for Homeland Security and Counterterrorism and congressional homeland security oversight committees before changing the designation of a critical infrastructure sector or SSA for a sector.

(d) REPORTS.—The Secretary of Homeland Security shall seek periodic research reports on critical infrastructure protection from Federal agencies as considered necessary by the Secretary.

SEC. 10. EVALUATION OF ACHIEVEMENT OF OBJECTIVES.

(a) IN GENERAL.—The National Research Council, beginning 12 months after the date of enactment of this Act, shall evaluate how well the Department of Homeland Security is meeting the objectives of this Act.

(b) INCLUDED SUBJECTS.—The review shall include evaluation of—

(1) cyber security threats to critical infrastructure;

(2) the success of Department programs in implementing section 8; and

(3) the long-term vulnerabilities faced by the Department, other Federal agencies, and critical infrastructure managers and owners.

(c) COMPLETION.—The Council shall complete the review by not later than the end of the 18-month period beginning on the date of enactment of this Act, except that the Secretary of Homeland Security may extend such period.

(d) REPORT.—Upon the completion of the review, the Council shall submit to the Secretary a report on the findings of the review, including recommendations based on such findings.

SEC. 11. DEFINITIONS.

For purposes of this Act:

(1) ALL HAZARDS.—The term ''all hazards'' means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. The term includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

(2) COLLABORATION.—The term ''collaboration'' means the process of working together to achieve shared goals.

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

(4) FEDERAL DEPARTMENTS AND AGENCIES.—The term ''Federal departments and agencies'' means any authority of the United States that is an ''agency'' under section 3502(1) of title 44, United States Code, other than those considered to be independent regulatory agencies as defined in section 3502(5) of such title.

(5) NATIONAL ESSENTIAL FUNCTIONS.—The term ''national essential functions'' means that subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency.

(6) PRIMARY MISSION ESSENTIAL FUNCTIONS.—The term ''primary mission essential func-

tions'' means those Government functions that must be performed in order to support or implement the performance of the national essential functions before, during, and in the aftermath of an emergency.

(7) 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.

(8) SECTOR-SPECIFIC AGENCY; SSA.—The terms ''sector-specific agency'' and ''SSA'' mean the Federal department or agency designated under this Act for a critical infrastructure sector.

(9) SECURE; SECURITY.—The terms ''secure'' and ''security'' mean reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

(10) SLTT.—The term ''SLTT'' means State, local, tribal, and territorial entities.

○