

114TH CONGRESS
1ST SESSION

H. R. 85

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

JANUARY 6, 2015

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.

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 “Terrorism Prevention
5 and Critical Infrastructure Protection Act of 2015”.

6 **SEC. 2. FINDINGS.**

7 The Congress finds the following:

8 (1) The Nation’s critical infrastructure provides
9 the essential services that underpin American soci-
10 ety. Proactive and coordinated efforts are necessary

1 to strengthen and maintain secure, functioning, and
2 resilient critical infrastructure, including assets, net-
3 works, and systems, that are vital to public con-
4 fidence and the Nation's safety, prosperity, and well-
5 being.

6 (2) The Nation's critical infrastructure is di-
7 verse and complex. It includes distributed networks,
8 varied organizational structures and operating mod-
9 els (including multinational ownership), inter-
10 dependent functions and systems in both the phys-
11 ical space and cyber space, and governance con-
12 structs that involve multilevel authorities, respon-
13 sibilities, and regulations. Critical infrastructure
14 owners and operators are uniquely positioned to
15 manage risks to their individual operations and as-
16 sets, and to determine effective strategies to make
17 them more secure and resilient.

18 (3) Critical infrastructure must be secured
19 against terrorist attacks, and must be designed and
20 maintained in such a way as to withstand and re-
21 cover quickly in the event of an attack. Achieving
22 this will require integration with the national pre-
23 paredness system across prevention, protection, miti-
24 gation, response, and recovery efforts.

1 **SEC. 3. POLICY.**

2 (a) SECURITY AND RESILIENCE.—The Secretary of
3 Homeland Security shall work with critical infrastructure
4 owners and operators and SLTTs to take proactive steps
5 to manage risk and strengthen the security and resilience
6 of 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. Such efforts shall seek to reduce
10 vulnerabilities, minimize consequences, identify and dis-
11 rupt terrorism threats, and hasten response and recovery
12 efforts related to critical infrastructure.

13 (b) INTERNATIONAL PARTNERS.—The Secretary
14 shall, in consultation with appropriate Federal agencies,
15 establish terrorism prevention policy to engage with inter-
16 national partners to strengthen the security and resilience
17 of domestic critical infrastructure and critical infrastruc-
18 ture located outside of the United States on which the Na-
19 tion depends.

20 (c) INTEGRATED, HOLISTIC APPROACH.—

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

1 infrastructure's interconnectedness and interdepend-
2 ency.

3 (2) DUTIES OF THE RESEARCH TASK FORCE.—

4 The research task force shall provide the Secretary
5 with—

6 (A) a list of critical infrastructure;

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

9 (C) the cyber preparedness of suppliers,
10 contractors, or service providers of critical in-
11 frastructure;

12 (D) programs, projects, or professional de-
13 velopment for persons responsible for the secu-
14 rity and operation of critical infrastructure; and

15 (E) vulnerabilities and threats that are
16 found in software systems, firewalls, applica-
17 tions, and methods of accessing systems.

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

22 (A) the National Institutes of Standards
23 and Technology;

24 (B) the Association of Computing Machin-
25 ery;

1 (C) IEEE (formerly the Institute of Elec-
2 trical and Electronic Engineers);

3 (D) Carnegie Mellon Cylabs;

4 (E) the Edison Electric Institute;

5 (F) the National Telecommunication and
6 Information Administration;

7 (G) the Utilities Telecom Council;

8 (H) the US Oil and Gas Association;

9 (I) the American Chemistry Council;

10 (J) the American Fuel and Petrochemical
11 Manufacturers;

12 (K) the Pharmaceutical Research Manu-
13 facturers of America; and

14 (L) the National Oceanic and Atmospheric
15 Administration.

16 (4) REPORT.—The research task force shall
17 provide a research report to the Secretary on its
18 findings and recommendations 180 days after its es-
19 tablishment.

20 (5) CRITICAL INFRASTRUCTURE DEFINED.—In
21 this subsection, the term “critical infrastructure”
22 means infrastructure of—

23 (A) energy capture, refining, manufac-
24 turing, and delivery systems;

1 (B) transportation and transportation sys-
2 tems;

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

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

9 (E) food production, processing, and deliv-
10 ery systems;

11 (F) virtual and physical communication
12 systems;

13 (G) financial systems; and

14 (H) the electricity grid.

15 (d) STRATEGIC IMPERATIVES.—

16 (1) IN GENERAL.—The Secretary shall establish
17 the Strategic Research Imperatives Program, which
18 shall have the responsibility of leading the Depart-
19 ment of Homeland Security’s Federal civilian agency
20 approach to strengthen critical infrastructure secu-
21 rity and resilience.

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

24 (A) Collect data, refine and clarify func-
25 tional relationships across the Federal Govern-

1 ment to advance the national unity of effort to
2 strengthen critical infrastructure, terrorism pre-
3 vention, security, and resilience.

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

8 (C) Recommend methods to implement an
9 integration and analysis function to inform
10 planning and operations decisions regarding the
11 protection of critical infrastructure from ter-
12 rorist threats.

13 (e) GUIDANCE.—The Secretary of Homeland Secu-
14 rity shall make available research findings and guidance
15 to Federal civilian department and agency heads (or their
16 designees) for the identification, prioritization, assess-
17 ment, remediation, and security of their respective internal
18 critical infrastructure to assist in the prevention, medi-
19 ation, and recovery from terrorism events.

20 **SEC. 4. ROLES AND RESPONSIBILITIES.**

21 (a) UNITY OF EFFORT.—

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

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

1 unity of effort to protect against terrorism
2 threats, through investigation of strategic guid-
3 ance from existing laws, Presidential policy di-
4 rectives, and Executive orders; and

5 (B) investigate the security and resilience
6 of the Nation's information assurance compo-
7 nents that provide protection against terrorism
8 threats.

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

14 (A) The program of the Department of
15 Homeland Security to secure Federal agencies
16 and critical infrastructure to create resilient se-
17 cure computer systems and networks.

18 (B) Cyber security preparedness of ven-
19 dors, contractors, or nongovernment agency en-
20 tities that provide computer-related support or
21 services to critical infrastructure owners and
22 operators as well as government agencies
23 charged with securing them.

1 (C) Investigation of the feasibility of devel-
2 oping industry- or sector-specific computer
3 emergency rapid response teams.

4 (D) The feasibility of the agency devel-
5 oping a guest visiting security researchers pro-
6 gram to provide instruction to private sector
7 and civilian agency personnel responsible for
8 cyber security.

9 (3) MEMBERSHIP.—The research working
10 group shall be comprised of individuals with exper-
11 tise and day-to-day engagement from the sector-spe-
12 cific agency terrorism prevention, remediation, and
13 response experts, as well as the specialized or sup-
14 port terrorism prevention capabilities of other Fed-
15 eral departments and agencies, as well as experts
16 who engage in strong collaboration with critical in-
17 frastructure owners and operators and SLTTs, and
18 academic researchers with in-depth knowledge in
19 computing security.

20 (b) SECRETARY OF HOMELAND SECURITY.—

21 (1) IN GENERAL.—The Secretary of Homeland
22 Security shall establish a research program to pro-
23 vide strategic guidance, promote a national unity of
24 effort, and coordinate the overall Federal effort to

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

3 (2) ADDITIONAL ROLES AND RESPONSIBIL-
4 ITIES.—Additional roles and responsibilities for the
5 Secretary of Homeland Security include the fol-
6 lowing:

7 (A) Identify and prioritize critical infra-
8 structure, considering physical and cyber
9 threats, vulnerabilities, and consequences of ter-
10 rorist attacks, in coordination with SSAs and
11 other Federal departments and agencies.

12 (B) Maintain national terrorism critical in-
13 frastructure centers that shall provide a situa-
14 tional awareness capability that includes inte-
15 grated, actionable information about potential
16 terrorist trends, imminent terrorist threats, and
17 the status of terrorist incidents that may im-
18 pact critical infrastructure.

19 (C) In coordination with SSAs and other
20 Federal departments and agencies, provide
21 analysis, expertise, and other technical assist-
22 ance to critical infrastructure owners and oper-
23 ators on terrorism prevention security protocols
24 and facilitate access to and exchange of infor-
25 mation and intelligence necessary to strengthen

1 the security and resilience of critical infrastruc-
2 ture.

3 (D) Conduct comprehensive assessments of
4 the vulnerabilities of the Nation's critical infra-
5 structure in coordination with the SSAs and in
6 collaboration with SLTTs and critical infra-
7 structure owners and operators.

8 (E) Coordinate Federal Government re-
9 sponses to cyber or physical terrorism incidents
10 affecting critical infrastructure consistent with
11 statutory authorities.

12 (F) Support the Attorney General and law
13 enforcement agencies with their responsibilities
14 to investigate and prosecute threats to and ter-
15 rorist attacks against critical infrastructure.

16 (G) Coordinate with and utilize the exper-
17 tise of SSAs and other appropriate Federal de-
18 partments and agencies to map geospatially,
19 image, analyze, and sort critical infrastructure
20 by employing commercial satellite and airborne
21 systems, as well as existing capabilities within
22 other departments and agencies.

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

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

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

11 (2) Carry out terrorism incident management
12 responsibilities consistent with statutory authority
13 and other appropriate policies, directives, or regula-
14 tions.

15 (3) Provide, support, or facilitate technical as-
16 sistance and consultations for such sectors to iden-
17 tify vulnerabilities and help mitigate terrorism inci-
18 dents, as appropriate.

19 (d) RESEARCH AND REPORT ON BEST PRACTICES
20 FOR COORDINATING.—The Secretary shall conduct re-
21 search and submit a report to Congress not later than 180
22 days after the date of the enactment of this Act on the
23 best practices for coordinating with civilian agencies, pri-
24 vate sector critical infrastructure owners, local, State, trib-
25 al, and territorial agencies, other relevant Federal depart-

1 ments and agencies, where appropriate with independent
2 regulatory agencies, and SLTTs, as appropriate, to imple-
3 ment this Act.

4 **SEC. 5. STRATEGIC IMPERATIVES.**

5 (a) RESEARCH AND REPORT ON THE MOST EFFI-
6 CIENT MEANS FOR INFORMATION EXCHANGE BY IDENTI-
7 FYING BASELINE DATA AND SYSTEMS REQUIREMENTS
8 FOR THE FEDERAL GOVERNMENT.—The Secretary shall
9 facilitate the timely exchange of terrorism threat and vul-
10 nerability information as well as information that allows
11 for the development of a situational awareness capability
12 for Federal civilian agencies during terrorist incidents.
13 The goal of such facilitation is to enable efficient informa-
14 tion exchange through the identification of requirements
15 for data and information formats and accessibility, system
16 interoperability, and redundant systems and alternate ca-
17 pabilities should there be a disruption in the primary sys-
18 tems.

19 (b) IMPLEMENTATION OF AN INTEGRATION AND
20 ANALYSIS FUNCTION TO INFORM PLANNING AND OPER-
21 ATIONAL DECISIONS REGARDING THE PROTECTION OF
22 CRITICAL INFRASTRUCTURE FROM TERRORISM
23 EVENTS.—The Secretary of Homeland Security shall im-
24 plement an integration and analysis function for critical
25 infrastructure that includes operational and strategic

1 analysis on terrorism incidents, threats, and emerging
2 risks. Such function shall include establishment by the
3 Secretary of 2 national centers to accomplish the fol-
4 lowing:

5 (1) Implement a capability to collate, assess,
6 and integrate vulnerability and consequence informa-
7 tion with threat streams and hazard information
8 to—

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

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

14 (C) determine the agency staffing needed
15 and to support cyber security critical infrastruc-
16 ture protection and report the findings to Con-
17 gress;

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

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

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

4 (G) support post-terrorism incident man-
5 agement and restoration efforts related to crit-
6 ical infrastructure; and

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

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

18 **SEC. 6. PROTECTION OF PRIVACY AND CIVIL LIBERTIES.**

19 (a) IN GENERAL.—The Secretary of Homeland Secu-
20 rity shall support greater terrorism cyber security infor-
21 mation sharing by civilian Federal agencies with the pri-
22 vate sector that protects constitutional privacy and civil
23 liberties rights. The heads of Federal departments and
24 agencies shall ensure that all existing privacy principles,
25 policies, and procedures are implemented consistent with

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

4 (b) ENSURING INDEPENDENCE OF PRIVACY OFFI-
5 CER.—

6 (1) IN GENERAL.—Section 222 of the Home-
7 land Security Act of 2002 (6 U.S.C. 142) is amend-
8 ed—

9 (A) in subsection (a), by striking so much
10 as precedes paragraph (1) and inserting the fol-
11 lowing:

12 “(a) IN GENERAL.—There shall be in the Depart-
13 ment a Privacy Officer who shall be appointed by the
14 President, by and with the advice and consent of the Sen-
15 ate. The Privacy Officer shall report directly to the Sec-
16 retary, and shall have primary responsibility in the De-
17 partment for privacy policy, including—”;

18 (B) by striking “senior official appointed
19 under subsection (a)” each place it appears and
20 inserting “Privacy Officer”;

21 (C) in subsection (b)(1)(A), by striking
22 “senior official” and inserting “Privacy Offi-
23 cer”;

1 (D) in subsection (b)(1)(B), by striking
2 “senior official’s” and inserting “Privacy Offi-
3 cer’s”;

4 (E) in subsection (b)(1)(C), by striking
5 “senior official” and inserting “Privacy Offi-
6 cer”;

7 (F) in subsection (b)(1)(D), by striking
8 “senior official” and inserting “Privacy Offi-
9 cer”;

10 (G) in subsection (c)(2)(B), by striking
11 “senior official” each place it appears and in-
12 serting “Privacy Officer”;

13 (H) in the heading for subsection
14 (c)(2)(B)(iii), by striking “BY SENIOR OFFI-
15 CIAL”;

16 (I) in subsection (d), by striking “the sen-
17 ior official appointed under subsection (a) or
18 transfers that senior official to another position
19 or location within the Department” and insert-
20 ing “individual appointed as Privacy Officer”;

21 (J) in the heading for subsection (e), by
22 striking “BY SENIOR OFFICIAL”; and

23 (K) in subsection (e)—

24 (i) by striking “senior official” and in-
25 serting “Privacy Officer”; and

1 (ii) by striking “senior official’s” each
2 place it appears and inserting “Privacy Of-
3 ficer”.

4 (2) CONTINUED SERVICE.—The senior official
5 serving as the Privacy Officer of the Department of
6 Homeland Security immediately before the enact-
7 ment of this Act may continue to act as the Privacy
8 Officer until a successor is appointed in accordance
9 with the amendments made by this subsection.

10 **SEC. 7. INNOVATION AND RESEARCH AND DEVELOPMENT.**

11 The Secretary of Homeland Security may consult
12 with other Federal departments and agencies to produce
13 and submit to congressional oversight committees a report
14 on how best to align federally funded research and devel-
15 opment activities that seek to strengthen the security and
16 resilience of the Nation’s critical infrastructure, includ-
17 ing—

18 (1) promoting research and development to en-
19 able the secure and resilient design and construction
20 of critical infrastructure and more secure accom-
21 panying cyber technology;

22 (2) enhancing modeling capabilities to deter-
23 mine potential impacts on critical infrastructure of
24 an incident or threat scenario, and cascading effects
25 on other sectors;

1 (3) facilitating initiatives to incentivize cyber
2 security investments and the adoption of critical in-
3 frastructure design features that strengthen all-haz-
4 ards security and resilience; and

5 (4) prioritizing efforts to support the strategic
6 guidance issued by the Secretary of Homeland Secu-
7 rity.

8 **SEC. 8. IMPLEMENTATION BY DEPARTMENT OF HOMELAND**
9 **SECURITY.**

10 (a) CRITICAL INFRASTRUCTURE TERRORISM PRE-
11 VENTION SECURITY AND COMPUTER NETWORK RESIL-
12 IENCE FUNCTIONAL RELATIONSHIPS.—

13 (1) IN GENERAL.—Within 120 days after the
14 date of the enactment of this Act, the Secretary of
15 Homeland Security shall conduct research and de-
16 velop a description of the functional relationships
17 within the Department of Homeland Security and
18 across the Federal Government related to critical in-
19 frastructure security and resilience. The description
20 shall—

21 (A) include the roles and functions of the
22 2 national critical infrastructure centers and a
23 discussion of the analysis and integration func-
24 tion;

1 (B) serve as a roadmap for critical infra-
2 structure owners and operators and SLTTs to
3 navigate the Federal Government's functions
4 and primary points of contact assigned to those
5 functions for critical infrastructure security and
6 resilience against both physical and cyber
7 threats; and

8 (C) include identification of every contact
9 within the Federal Government for critical in-
10 frastructure protection security and resilience,
11 by company and industry.

12 (2) COORDINATION.—The Secretary shall pre-
13 pare a report on efforts to coordinate this effort with
14 the SSAs and other relevant Federal departments
15 and agencies.

16 (3) PROVISION TO PRESIDENT.—The Secretary
17 shall provide the description, supported by agency-
18 conducted research, to the President through the As-
19 sistant to the President for Homeland Security and
20 Counterterrorism, and to the relevant congressional
21 homeland security oversight committees.

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

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

1 Homeland Security, in coordination with the SSAs,
2 other relevant Federal departments and agencies,
3 SLTTs, and critical infrastructure owners and oper-
4 ators, shall conduct an analysis of the existing pub-
5 lic-private partnership model, evaluate its effective-
6 ness, and recommend options for improving the ef-
7 fectiveness of the partnership in both the physical
8 and cyber space.

9 (2) CONTENTS.—The research and rec-
10 ommendations shall—

11 (A) consider options to streamline or auto-
12 mate (or both) processes for collaboration and
13 exchange of terrorism-related information and
14 to minimize duplication of effort;

15 (B) consider how the model for terrorism
16 information exchange can be flexible and adapt-
17 able to meet the unique needs of individual crit-
18 ical infrastructure sectors while providing a fo-
19 cused, disciplined, and effective approach for
20 the Federal Government to coordinate with the
21 critical infrastructure owners and operators and
22 with SLTTs governments; and

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

1 (c) IDENTIFICATION OF BASELINE DATA AND SYS-
2 TEMS REQUIREMENTS FOR THE FEDERAL GOVERNMENT
3 TO ENABLE EFFICIENT INFORMATION EXCHANGE.—

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

10 (A) to enable the efficient exchange of ter-
11 rorism information and intelligence relevant to
12 strengthening the security and resilience of crit-
13 ical infrastructure; and

14 (B) for sharing of data and interoperability
15 of systems to enable the timely exchange of ter-
16 rorism or terrorist threat data and information
17 to secure critical infrastructure and make it
18 more resilient.

19 (2) EXPERTS INCLUDED.—The experts shall in-
20 clude representatives from—

21 (A) those entities that routinely possess in-
22 formation important to critical infrastructure
23 security and resilience;

1 (B) those entities that determine and man-
2 age information technology systems used to ex-
3 change information; and

4 (C) those entities responsible for the secu-
5 rity of information being exchanged.

6 (3) ANALYSIS.—Analysis by such team of ex-
7 perts shall include—

8 (A) interoperability with critical infrastruc-
9 ture partners;

10 (B) identification of key data and the in-
11 formation requirements of key Federal, SLTT,
12 and private sector entities;

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

15 (D) the ability to exchange various classi-
16 fications of information;

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

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

21 (4) PROVISION TO PRESIDENT.—The Secretary
22 shall provide such analysis to the President through
23 the Assistant to the President for Homeland Secu-
24 rity and Counterterrorism, and to congressional
25 homeland security oversight committees.

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

8 (1) includes threat streams and all-hazards in-
9 formation as well as vulnerabilities;

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

12 (3) supports decisionmaking;

13 (4) disseminates critical information that may
14 be needed to save or sustain lives, mitigate damage,
15 or reduce further degradation of a critical infra-
16 structure capability throughout an incident; and

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

21 (e) UPDATE TO NATIONAL INFRASTRUCTURE PRO-
22 TECTION PLAN.—

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

1 through the Assistant to the President for Home-
2 land Security and Counterterrorism and the congres-
3 sional homeland security oversight committees, a re-
4 search report that outlines the National Infrastruc-
5 ture Protection Plan to address the implementation
6 of this Act, the requirements of title II of the Home-
7 land Security Act of 2002 (6 U.S.C. 121 et seq.),
8 and alignment with the National Preparedness Goal
9 and System required by Presidential Policy Directive
10 8.

11 (2) CONTENTS.—The plan shall include—

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

16 (B) the methods to be used to prioritize
17 critical infrastructure in the event of a ter-
18 rorism event that impacts multiple infrastruc-
19 ture systems;

20 (C) the protocols to be used to synchronize
21 communication and actions within the Federal
22 Government to effectively respond to critical in-
23 frastructure terrorist threats or events; and

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

1 and reduce terrorism risks to critical infrastruc-
2 ture.

3 (3) RELATIONSHIP TO OTHER PROVISIONS.—

4 The plan shall reflect the terrorism threat identifica-
5 tion, prevention, mediation, and recovery relation-
6 ships within the Department of Homeland Security
7 and across the Federal Government identified under
8 this Act and the updates to the public-private part-
9 nership model under this Act.

10 (4) ENERGY AND COMMUNICATION SYSTEMS.—

11 The plan shall consider sector dependencies on en-
12 ergy and communications systems during a ter-
13 rorism event, and identify pre-event and mitigation
14 measures or alternate capabilities during disruptions
15 to those systems.

16 (5) COORDINATION.—The Secretary shall co-
17 ordinate activities under this subsection with the
18 SSAs, other relevant Federal departments and agen-
19 cies, SLTTs, and critical infrastructure owners and
20 operators.

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

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

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

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

1 (h) RELATIONSHIP TO OTHER AUTHORITIES.—Noth-
 2 ing in this Act alters, supersedes, or impedes the authori-
 3 ties of Federal departments and agencies, including inde-
 4 pendent regulatory agencies, to carry out their functions
 5 and duties consistent with applicable legal authorities and
 6 other Presidential guidance and directives, including the
 7 designation of critical infrastructure under such authori-
 8 ties.

9 **SEC. 9. DESIGNATION OF CRITICAL INFRASTRUCTURE SEC-**
 10 **TORS AND SECTOR-SPECIFIC AGENCIES.**

11 (a) DESIGNATION.—

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

18 (2) CULTIVATION OF RELATIONSHIPS.—The
 19 Secretary shall evaluate the appropriate relation-
 20 ships among Federal agencies, SSAs, SLTTs, and
 21 critical infrastructure owners and operators to estab-
 22 lish the most effective defense against terrorist at-
 23 tacks.

24 (b) FUNCTION.—The Secretary shall provide institu-
 25 tional knowledge and specialized expertise to lead, facili-

1 tate, or support security and resilience programs and asso-
 2 ciated terrorism prevention activities with respect to sec-
 3 tors designated under subsection (a)(1).

4 (c) CHANGES.—The Secretary of Homeland Security
 5 shall periodically evaluate the need for and make changes
 6 to plans and evaluations made under this section. The Sec-
 7 retary shall consult with the Assistant to the President
 8 for Homeland Security and Counterterrorism and congres-
 9 sional homeland security oversight committees before
 10 changing the designation of a critical infrastructure sector
 11 or SSA for a sector.

12 (d) REPORTS.—The Secretary of Homeland Security
 13 shall seek periodic research reports on critical infrastruc-
 14 ture protection from Federal agencies as considered nec-
 15 essary by the Secretary.

16 **SEC. 10. EVALUATION OF ACHIEVEMENT OF OBJECTIVES.**

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

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

23 (1) cyber security threats to critical infrastruc-
 24 ture;

1 (2) the success of Department programs in im-
2 plementing section 8; and

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

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

11 (d) REPORT.—Upon the completion of the review, the
12 Council shall submit to the Secretary a report on the find-
13 ings of the review, including recommendations based on
14 such findings.

15 **SEC. 11. DEFINITIONS.**

16 For purposes of this Act:

17 (1) ALL HAZARDS.—The term “all hazards”
18 means a threat or an incident, natural or manmade,
19 that warrants action to protect life, property, the en-
20 vironment, and public health or safety, and to mini-
21 mize disruptions of government, social, or economic
22 activities. The term includes natural disasters, cyber
23 incidents, industrial accidents, pandemics, acts of
24 terrorism, sabotage, and destructive criminal activity
25 targeting critical infrastructure.

1 (2) COLLABORATION.—The term “collabora-
2 tion” means the process of working together to
3 achieve shared goals.

4 (3) CRITICAL INFRASTRUCTURE.—The term
5 “critical infrastructure” means systems and assets,
6 whether physical or virtual, so vital to the United
7 States that the incapacity or destruction of such sys-
8 tems and assets would have a debilitating impact on
9 security, national economic security, national public
10 health or safety, or any combination of those mat-
11 ters.

12 (4) FEDERAL DEPARTMENTS AND AGENCIES.—
13 The term “Federal departments and agencies”
14 means any authority of the United States that is an
15 “agency” under section 3502(1) of title 44, United
16 States Code, other than those considered to be inde-
17 pendent regulatory agencies as defined in section
18 3502(5) of such title.

19 (5) NATIONAL ESSENTIAL FUNCTIONS.—The
20 term “national essential functions” means that sub-
21 set of Government functions that are necessary to
22 lead and sustain the Nation during a catastrophic
23 emergency.

24 (6) PRIMARY MISSION ESSENTIAL FUNC-
25 TIONS.—The term “primary mission essential func-

1 tions” means those Government functions that must
2 be performed in order to support or implement the
3 performance of the national essential functions be-
4 fore, during, and in the aftermath of an emergency.

5 (7) 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 (8) SECTOR-SPECIFIC AGENCY; SSA.—The
12 terms “sector-specific agency” and “SSA” mean the
13 Federal department or agency designated under this
14 Act for a critical infrastructure sector.

15 (9) SECURE; SECURITY.—The terms “secure”
16 and “security” mean reducing the risk to critical in-
17 frastructure by physical means or defense cyber
18 measures to intrusions, attacks, or the effects of
19 natural or manmade disasters.

20 (10) SLTT.—The term “SLTT” means State,
21 local, tribal, and territorial entities.

○