114TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
1st Session } { 114–240

CRITICAL INFRASTRUCTURE PROTECTION ACT

AUGUST 4, 2015.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Homeland Security, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 1073]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 1073) to amend the Homeland Security Act of 2002 to secure critical infrastructure against electromagnetic threats, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	3
Background and Need for Legislation	3
Hearings	4
Committee Consideration	4
Committee Votes	5
Committee Oversight Findings	5
New Budget Authority, Entitlement Authority, and Tax Expenditures	5
Congressional Budget Office Estimate	5
Statement of General Performance Goals and Objectives	6
Duplicative Federal Programs	6
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits	6
Federal Mandates Statement	6
Preemption Clarification	6
Advisory Committee Statement	6
Applicability to Legislative Branch	7
Section-by-Section Analysis of the Legislation	7

49–006

Changes in Existing Law Made by the Bill, as Reported 9
Additional Views 19

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Critical Infrastructure Protection Act" or "CIPA".

SEC. 2. EMP PLANNING, RESEARCH AND DEVELOPMENT, AND PROTECTION AND PREPAREDNESS.

(a) IN GENERAL.—The Homeland Security Act of 2002 (6 U.S.C. 121) is amended—

(1) in section 2 (6 U.S.C. 101), by inserting after paragraph (6) the following:

"(6a) EMP.—The term 'EMP' means—

"(A) an electromagnetic pulse caused by intentional means, including acts of terrorism; and

"(B) a geomagnetic disturbance caused by solar storms or other naturally occurring phenomena.";

(2) in title V (6 U.S.C. 311 et seq.), by adding at the end the following:

"SEC. 526. NATIONAL PLANNING FRAMEWORKS AND EDUCATION.

"The Secretary, or the Secretary's designee, shall, to the extent practicable—

"(1) include in national planning frameworks the threat of EMP events; and

"(2) conduct outreach to educate owners and operators of critical infrastructure, emergency planners, and emergency response providers at all levels of government of the threat of EMP events.";

(3) in title III (6 U.S.C. 181 et seq.), by adding at the end of the following:

"SEC. 318. EMP RESEARCH AND DEVELOPMENT.

"(a) IN GENERAL.—In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other relevant agencies and departments of the Federal Government and relevant owners and operators of critical infrastructure, shall, to the extent practicable, conduct research and development to mitigate the consequences of EMP events.

"(b) SCOPE.—The scope of the research and development under subsection (a) shall include the following:

"(1) An objective scientific analysis of the risks to critical infrastructures from a range of EMP events.

"(2) Determination of the critical national security assets and vital civic utilities and infrastructures that are at risk from EMP events.

"(3) An evaluation of emergency planning and response technologies that would address the findings and recommendations of experts, including those of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack.

"(4) An analysis of technology options that are available to improve the resiliency of critical infrastructure to EMP.

"(5) The restoration and recovery capabilities of critical infrastructure under differing levels of damage and disruption from various EMP events."; and

(4) in section 201(d) (6 U.S.C. 121(d)), by adding at the end the following:

"(26)(A) Prepare and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate—

"(i) a recommended strategy to protect and prepare the critical infrastructure of the American homeland against EMP events, including from acts of terrorism; and

"(ii) biennial updates on the status of the recommended strategy.

"(B) The recommended strategy shall—

"(i) be based on findings of the research and development conducted under section 318;

"(ii) be developed in consultation with the relevant Federal sector-specific agencies (as defined under Homeland Security Presidential Directive–7) for critical infrastructures;

"(iii) be developed in consultation with the relevant sector coordinating councils for critical infrastructures; and

"(iv) include a classified annex as needed.

"(C) The Secretary may, if appropriate, incorporate the recommended strategy into a broader recommendation developed by the Department to help protect and prepare critical infrastructure from terrorism and other threats if, as incorporated, the strategy complies with subparagraph (B).".

(b) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of such Act is amended—

(1) by adding at the end of the items relating to title V the following:

"Sec. 526. National planning frameworks and education.";

and

(2) by adding at the end of the items relating to title III the following:

"Sec. 318. EMP research and development.".

(c) DEADLINE FOR RECOMMENDED STRATEGY.—The Secretary of Homeland Security shall submit the recommended strategy required under the amendment made by subsection (a)(4) by not later than one year after the date of the enactment of this Act.

(d) REPORT.—The Secretary shall submit a report to Congress by not later than 180 days after the date of the enactment of this Act describing the progress made in, and an estimated date by which the Department of Homeland Security will have completed—

(1) including EMP (as defined in the amendment made by subsection (a)(1)) threats in national planning frameworks;

(2) research and development described in the amendment made by subsection (a)(3);

(3) development of the comprehensive plan required under the amendment made by subsection (a)(4); and

(4) outreach to educate owners and operators of critical infrastructure, emergency planners and emergency response providers at all levels of government regarding the threat of EMP events.

SEC. 3. NO REGULATORY AUTHORITY.

Nothing in this Act, including the amendments made by this Act, shall be construed to grant any regulatory authority.

SEC. 4. NO NEW AUTHORIZATION OF APPROPRIATIONS.

This Act, including the amendments made by this Act, may be carried out only by using funds appropriated under the authority of other laws.

PURPOSE AND SUMMARY

The purpose of H.R. 1073 is to amend the Homeland Security Act of 2002 to secure critical infrastructure against electromagnetic threats, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

The Department of Homeland Security (DHS) has a responsibility to assess critical infrastructure resilience to a variety of threats, both man-made and natural. The mission of DHS is to ensure "a homeland that is safe, secure, and resilient against terrorism and other hazards." The threat of electromagnetic pulses (EMP), whether due to a nuclear weapon or solar flares, represents another high-consequence, low-probability threat, which has had little attention from the Department.

This measure requires the Secretary to assess both EMP threats in the context of other threat to determine the research and development needs to mitigate the threat and consequences of EMP events, develop strategic guidance for the Department, and conduct outreach to educate owners and operators of the critical infrastructure, emergency planners, and emergency response providers regarding the threat of EMP events.

Prior Legislation

In the 113th Congress, the Committee on Homeland Security considered H.R. 3410, the Critical Infrastructure Protection Act. The House passed H.R. 3410 under Suspension of the Rules on De-

cember 1, 2014, and the measure was referred to the Senate Committee on Homeland Security and Governmental Affairs.

HEARINGS

112th Congress

On September 12, 2012, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "The EMP Threat: Examining the Consequences." The Subcommittee received testimony from Hon. Trent Franks, a Representative in Congress from the 2nd District of Arizona; Mr. Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission; Mr. Brandon Wales, Director, Homeland Infrastructure Threat and Risk Analysis Center, Department of Homeland Security; Mr. Michael A. Aimone, Director, Business Enterprise Integration, Office of the Deputy Undersecretary of Defense for Installations and Environment, Office of Undersecretary of Defense for Acquisition, Technology, and Logistics, Department of Defense; and Dr. Chris Beck, President, Electric Infrastructure Security Council.

113th Congress

On May 8, 2014, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Electromagnetic Pulse (EMP): Threat to Critical Infrastructure." The Subcommittee received testimony from Hon. Trent Franks, a Representative in Congress from the Eighth District of Arizona; Dr. Peter Vincent Pry, Congressional EMP Commission, Congressional Strategic Posture Commission, Executive Director of the Task Force on National and Homeland Security; Dr. Michael J. Frankel, Senior Scientist, Penn State University, Applied Research Laboratory; and Dr. Chris Beck, Vice President, Policy and Strategic Initiatives, Electric Infrastructure Security Council.

COMMITTEE CONSIDERATION

The Committee met on June 23, 2015, to consider H.R. 1073, and ordered the measure to be reported to the House with a favorable recommendation, amended, by voice vote. The Committee took the following actions:

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. PERRY (#1); was AGREED TO, as amended, by voice vote.

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (#1) consisting of an amendment by *Mr. Payne*; was AGREED TO by voice vote.

Page 2, line 1, strike "Scenarios" and insert "Frameworks".
Page 2, line 3, insert "or the Secretary's designee" after "Secretary".
Page 2, line 4, strike "national planning scenarios" and insert "national planning frameworks".
Page 2, line 8, strike "responders" and insert "response providers".
Page 4, after line 23, strike "scenarios" and insert "frameworks".
Page 5, line 15, strike "scenarios" and insert "frameworks".
Page 5, line 23, strike "responders" and insert "response providers"

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 1073.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 1073, the Critical Infrastructure Protection Act, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 13, 2015.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1073, the Critical Infrastructure Protection Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

KEITH HALL.

Enclosure.

H.R. 1073—Critical Infrastructure Protection Act

H.R. 1073 would require the Department of Homeland Security (DHS) to undertake research and planning activities to mitigate the potential consequences of electromagnetic pulses—resulting from either intentional acts or natural causes—on critical infrastructure, such as public utilities and national security assets. The department is currently carrying out programs similar to those required by the bill, and CBO estimates that implementing H.R. 1073 would not significantly affect spending by DHS. Because enacting the legislation would not affect direct spending or revenues, pay-as-you-go procedures do not apply.

H.R. 1073 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

Statement of General Performance Goals and Objectives

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 1073 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

The Committee expects DHS to provide an appropriate assessment of the threat of electromagnetic pulse (EMP) events and to include such assessment in national planning scenarios. DHS shall develop a campaign to proactively educate owners and operators of critical infrastructure, emergency planners, and emergency responders at all levels of government of the threat of EMP events. The Committee expects DHS to conduct research and development to mitigate the consequences of EMP events and develop a comprehensive plan relating to intelligence and analysis to protect and prepare the critical infrastructure against EMP events

Duplicative Federal Programs

Pursuant to clause 3(c) of Rule XIII, the Committee finds that H.R. 1073 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

Federal Mandates Statement

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

Preemption Clarification

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 1073 does not preempt any State, local, or Tribal law.

Advisory Committee Statement

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that bill may be cited as the "Critical Infrastructure Protection Act" or "CIPA".

Section 2. EMP Planning, Research and Development, and Protection and Preparedness.

This section amends section 2 of the Homeland Security Act of 2002 to define EMP as: (a) an electromagnetic pulse caused by intentional means, including acts of terrorism, (b) a geomagnetic disturbance caused by solar storms or other naturally occurring phenomena.

The committee is aware of the concerns of industry in the possible confusion between pulses caused by intentional means, such as a high altitude nuclear weapon detonation, and those caused by natural phenomena such as solar storms. The magnitude and the temporal duration of the energy released are very different. Electromagnetic pulses caused by nuclear yield has a different waveform, typically described in the literature as E1, E2, and E3 forms, than the electromagnetic pulses caused by a geomagnetic disturbance, though we note that the later-time E3 of a nuclear generated pulse have many characteristics similar to the pulses caused by a geomagnetic disturbance. The intent of this definition is to keep these electromagnetic pulse initiating events distinct and separate, as well as the resulting impact on critical infrastructure such as the electric power grid. Regardless of the source event (nuclear yield or GMD), the Department of Homeland Security is to assess both types of events and the electromagnetic pulses generated, determine their impact to potential disturbances or outages to critical infrastructure, and suggest possible ways to mitigate these effects.

This section amends title V to require the Secretary to include the threat of EMP events in national planning frameworks and conduct outreach to educate critical infrastructure owners and operators, emergency planners, and emergency responders at all levels of government of the threat of EMP events.

This section amends title III of the Homeland Security Act of 2002 to require the Undersecretary of Science and Technology to conduct research and development to mitigate the consequences of EMP events. The research and development must include an objective scientific analysis of the risks to critical infrastructures from a range of EMP events; a determination of the national security assets and civic utilities and infrastructures at risk from EMP events; an evaluation of emergency planning and response technologies that would address the findings and recommendations of experts; an analysis of technology options available to improve the resiliency of critical infrastructure to EMP; and the restoration and

recovery capabilities of critical infrastructure under differing levels of damage and disruption from various EMP events.

This section amends section 201(d) by requiring a strategy to protect and prepare the critical infrastructure against EMP events. The strategy must be updated biennially. The strategy will be based on findings of the research and development conducted in title III; be developed in consultation with relevant Federal sector-specific agencies for critical infrastructures; be developed in consultation with the relevant sector coordinating councils; and include a classified annex as needed. The Secretary may incorporate the strategy into a broader recommendation to help protect and prepare critical infrastructure from terrorism and other threats. The strategy is due one year from the date of enactment.

This section requires the Secretary to report to Congress within 180 days of enactment on the progress made on the new requirements in this bill.

Section 3. No Regulatory Authority.

Consistent with Section 3, which provides that nothing in this Act shall be construed to grant any regulatory authority, the intent of the Committee is that the recommended strategy shall apply solely to planning, research and development, and other internal activities or recommendations of the Department, and should not be used or construed in a manner that would have the effect of imposing requirements or standards, either directly or indirectly, on the private sector.

Section 4. No New Authorization of Appropriations.

This section requires the Act to be carried out only by using funds appropriated under the authority of other laws.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

Sec. 318. EMP research and development.

* * * * * * *

TITLE V—NATIONAL EMERGENCY MANAGEMENT

* * * * * * *

Sec. 526. National planning frameworks and education.

* * * * * * *

SEC. 2. DEFINITIONS.

In this Act, the following definitions apply:

(1) Each of the terms "American homeland" and "homeland" means the United States.

(2) The term "appropriate congressional committee" means any committee of the House of Representatives or the Senate having legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.

(3) The term "assets" includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

(4) The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(5) The term "Department" means the Department of Homeland Security.

(6) The term "emergency response providers" includes Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency re-

sponse, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

(6a) EMP.—The term "EMP" means—

(A) an electromagnetic pulse caused by intentional means, including acts of terrorism; and

(B) a geomagnetic disturbance caused by solar storms or other naturally occurring phenomena.

(7) The term "executive agency" means an executive agency and a military department, as defined, respectively, in sections 105 and 102 of title 5, United States Code.

(8) The term "functions" includes authorities, powers, rights, privileges, immunities, programs, projects, activities, duties, and responsibilities.

(9) The term "intelligence component of the Department" means any element or entity of the Department that collects, gathers, processes, analyzes, produces, or disseminates intelligence information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence, as defined under section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)), except—

(A) the United States Secret Service; and

(B) the Coast Guard, when operating under the direct authority of the Secretary of Defense or Secretary of the Navy pursuant to section 3 of title 14, United States Code, except that nothing in this paragraph shall affect or diminish the authority and responsibilities of the Commandant of the Coast Guard to command or control the Coast Guard as an armed force or the authority of the Director of National Intelligence with respect to the Coast Guard as an element of the intelligence community (as defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(10) The term "key resources" means publicly or privately controlled resources essential to the minimal operations of the economy and government.

(11) The term "local government" means—

(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(C) a rural community, unincorporated town or village, or other public entity.

(12) The term "major disaster" has the meaning given in section 102(2) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(13) The term "personnel" means officers and employees.

(14) The term "Secretary" means the Secretary of Homeland Security.

(15) The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(16) The term "terrorism" means any activity that—

(A) involves an act that—

(i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and

(ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and

(B) appears to be intended—

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

(17)(A) The term "United States", when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

(B) Nothing in this paragraph or any other provision of this Act shall be construed to modify the definition of "United States" for the purposes of the Immigration and Nationality Act or any other immigration or nationality law.

(18) The term "voluntary preparedness standards" means a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs, such as the American National Standards Institute's National Fire Protection Association Standard on Disaster/Emergency Management and Business Continuity Programs (ANSI/NFPA 1600).

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Information and Analysis and Infrastructure Protection; Access to Information

SEC. 201. INFORMATION AND ANALYSIS AND INFRASTRUCTURE PROTECTION.

(a) INTELLIGENCE AND ANALYSIS AND INFRASTRUCTURE PROTECTION.—There shall be in the Department an Office of Intelligence and Analysis and an Office of Infrastructure Protection.

(b) UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS AND ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—

(1) OFFICE OF INTELLIGENCE AND ANALYSIS.—The Office of Intelligence and Analysis shall be headed by an Under Secretary for Intelligence and Analysis, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) CHIEF INTELLIGENCE OFFICER.—The Under Secretary for Intelligence and Analysis shall serve as the Chief Intelligence Officer of the Department.

(3) OFFICE OF INFRASTRUCTURE PROTECTION.—The Office of Infrastructure Protection shall be headed by an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President.

(c) DISCHARGE OF RESPONSIBILITIES.—The Secretary shall ensure that the responsibilities of the Department relating to information analysis and infrastructure protection, including those described in subsection (d), are carried out through the Under Secretary for Intelligence and Analysis or the Assistant Secretary for Infrastructure Protection, as appropriate.

(d) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS AND INFRASTRUCTURE PROTECTION.—The responsibilities of the Secretary relating to intelligence and analysis and infrastructure protection shall be as follows:

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 404o), in order to—

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis or assessments are provided by or produced by the Department) in order to—

(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal

Government, State, and local government agencies and authorities, the private sector, and other entities; and

(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private sector entity.

(4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

(6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

(7) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section.

(8) To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

(9) To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

(10) To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(11) To ensure that—

(A) any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this Act is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. 401 et seq.) and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

(12) To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(13) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(14) To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

(A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

(B) treat information in such databases in a manner that complies with applicable Federal law on privacy.

(15) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(16) To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

(17) To provide intelligence and information analysis and support to other elements of the Department.

(18) To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components.

(19) To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from

the President and, as applicable, the Director of National Intelligence.

(20) To establish a structure and process to support the missions and goals of the intelligence components of the Department.

(21) To ensure that, whenever possible, the Department—

(A) produces and disseminates unclassified reports and analytic products based on open-source information; and

(B) produces and disseminates such reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the Department produced and disseminated in a classified format.

(22) To establish within the Office of Intelligence and Analysis an internal continuity of operations plan.

(23) Based on intelligence priorities set by the President, and guidance from the Secretary and, as appropriate, the Director of National Intelligence—

(A) to provide to the heads of each intelligence component of the Department guidance for developing the budget pertaining to the activities of such component; and

(B) to present to the Secretary a recommendation for a consolidated budget for the intelligence components of the Department, together with any comments from the heads of such components.

(24) To perform such other duties relating to such responsibilities as the Secretary may provide.

(25) To prepare and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security in the House of Representatives, and to other appropriate congressional committees having jurisdiction over the critical infrastructure or key resources, for each sector identified in the National Infrastructure Protection Plan, a report on the comprehensive assessments carried out by the Secretary of the critical infrastructure and key resources of the United States, evaluating threat, vulnerability, and consequence, as required under this subsection. Each such report—

(A) shall contain, if applicable, actions or countermeasures recommended or taken by the Secretary or the head of another Federal agency to address issues identified in the assessments;

(B) shall be required for fiscal year 2007 and each subsequent fiscal year and shall be submitted not later than 35 days after the last day of the fiscal year covered by the report; and

(C) may be classified.

(26)(A) Prepare and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate—

(i) a recommended strategy to protect and prepare the critical infrastructure of the American homeland against EMP events, including from acts of terrorism; and

(ii) biennial updates on the status of the recommended strategy.

(B) The recommended strategy shall—

(i) be based on findings of the research and development conducted under section 318;

(ii) be developed in consultation with the relevant Federal sector-specific agencies (as defined under Homeland Security Presidential Directive–7) for critical infrastructures;

(iii) be developed in consultation with the relevant sector coordinating councils for critical infrastructures; and

(iv) include a classified annex as needed.

(C) The Secretary may, if appropriate, incorporate the recommended strategy into a broader recommendation developed by the Department to help protect and prepare critical infrastructure from terrorism and other threats if, as incorporated, the strategy complies with subparagraph (B).

(e) STAFF.—

(1) IN GENERAL.—The Secretary shall provide the Office of Intelligence and Analysis and the Office of Infrastructure Protection with a staff of analysts having appropriate expertise and experience to assist such offices in discharging responsibilities under this section.

(2) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(3) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(f) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the Office of Intelligence and Analysis and the Office of Infrastructure Protection in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

(2) COVERED AGENCIES.—The agencies referred to in this paragraph are as follows:

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The Defense Intelligence Agency.

(G) Any other agency of the Federal Government that the President considers appropriate.

(3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(4) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(g) FUNCTIONS TRANSFERRED.—In accordance with title XV, there shall be transferred to the Secretary, for assignment to the Office of Intelligence and Analysis and the Office of Infrastructure Protection under this section, the functions, personnel, assets, and liabilities of the following:

(1) The National Infrastructure Protection Center of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section), including the functions of the Attorney General relating thereto.

(2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.

(3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department, including the functions of the Secretary of Energy relating thereto.

(5) The Federal Computer Incident Response Center of the General Services Administration, including the functions of the Administrator of General Services relating thereto.

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 318. EMP RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other relevant agencies and departments of the Federal Government and relevant owners and operators of critical infrastructure, shall, to the extent practicable, conduct research and development to mitigate the consequences of EMP events.

(b) SCOPE.—The scope of the research and development under subsection (a) shall include the following:

(1) An objective scientific analysis of the risks to critical infrastructures from a range of EMP events.

(2) Determination of the critical national security assets and vital civic utilities and infrastructures that are at risk from EMP events.

(3) An evaluation of emergency planning and response technologies that would address the findings and recommendations of experts, including those of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack.

(4) An analysis of technology options that are available to improve the resiliency of critical infrastructure to EMP.

(5) The restoration and recovery capabilities of critical infrastructure under differing levels of damage and disruption from various EMP events.

* * * * * * *

TITLE V—NATIONAL EMERGENCY MANAGEMENT

* * * * * * *

SEC. 526. NATIONAL PLANNING FRAMEWORKS AND EDUCATION.

The Secretary, or the Secretary's designee, shall, to the extent practicable—

(1) include in national planning frameworks the threat of EMP events; and

(2) conduct outreach to educate owners and operators of critical infrastructure, emergency planners, and emergency response providers at all levels of government of the threat of EMP events.

* * * * * * *

ADDITIONAL VIEW OF RANKING MEMBER BENNIE G. THOMPSON

I am writing to associate myself with the views of many industry stakeholders on a core aspect of the bill—the definition of electromagnetic pulse.

While I am pleased that the report acknowledges industry concerns, I am disappointed that the bill does not distinguish an electromagnetic pulse (EMP) from a geomagnetic disturbance (GMD). An EMP event is manmade and expected to impact all microprocessors. A GMD is naturally-occurring and expected to impact primarily bulk power and communication systems.

Unfortunately, the definition in the bill merges and conflates the two. The definition has broad ramifications on how DHS uses its limited resources to carry out the new mandates under the bill. As a result of this conflation, DHS will now have to research, strategize, and develop educational materials on two very different low-probability threats that inherently demand radically different mitigation and response strategies.

BENNIE G. THOMPSON,
Ranking Member.