Defeated
8:8

FOT

AMENDMENT NO. 9 Calendar No.___

Purpose: To establish the Directorate for Information Analysis and Infrastructure Protection.

IN THE SENATE OF THE UNITED STATES — 107TH CONG., 2d Sess.

S. 2452

To establish the Department of National Homeland Security and the National Office for Combating Terrorism.

Referred to the Committee on _____
and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mr. THOMPSON

On page 40, line 5, strike all through page 55, line 15, and insert the following:

SEC. 132. DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.

(a) ESTABLISHMENT.— There is established a Directorate for Information Analysis and Infrastructure Protection for the purpose of supporting the mission of the Department as defined in this Act.

(b) UNDERSECRETARY AND ASSISTANT SECRETARIES.— The Directorate for Information Analysis and Infrastructure Protection shall be headed by the Under Secretary for Information Analysis and Infrastructure Protection, who shall be assisted by an Assistant Secretary for Information Analysis and an Assistant Secretary for Infrastructure Protection, each of which shall be appointed by the President, by and with the advice and the consent of the Senate.

(c) RESPONSIBILITIES OF DIRECTORATE OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.— The responsibilities of the Directorate of Information Analysis and Infrastructure Protection shall include —

(1) receiving and analyzing law enforcement information, intelligence, and other information in order to understand the nature and scope of the terrorist threat to the American homeland and to detect and identify potential threats of terrorism to the United States;

(2) ensuring the Directorate's timely and efficient access to information from United States Government agencies, state and local or foreign governments and private sector entities;

(3) entering into cooperative agreements as necessary, through the Secretary, to acquire such information;

(4) representing the Department in any interagency meetings to establish requirements and priorities in the collection of national intelligence;

(5) consulting with the Attorney General or his designee and other United States government officials to establish overall collection priorities, related to domestic threats, including terrorism to the homeland;

(6) establishing and utilizing, in conjunction with the Chief Information Officer of the Department, and in conjunction with appropriate officials at other United States Government agencies, a communications and information technology infrastructure adequate to carry out the mission of the Department;

(7) developing, in conjunction with the Chief Information Officer of the Department, and in conjunction with appropriate officials at other United States

Government agencies, appropriate software, hardware, and other information technology, and security and formatting protocols to ensure that United States Government databases and information technology systems containing information relevant to homeland security are compatible with the communications and information technology infrastructure referred to in paragraph (6), and that such systems comply with applicable federal laws and regulations concerning privacy and the prevention of unauthorized disclosure;

(8) ensuring, in conjunction with the Director of Central Intelligence, as head of the Intelligence Community as described in Section 102 of the National Security Act, and the Attorney General, that all material received by the Department is protected against unauthorized disclosure and is utilized by the Department only in the course and for the purposes of fulfillment of official duties, and is transmitted, retained, handled, and disseminated consistent with the authority of the Director of Central Intelligence to protect intelligence sources and methods from unauthorized disclosure under the National Security Act and related procedures or, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information;

(9) disseminating information derived from intelligence or other information relevant to potential terrorist threats to the United States, to United States Government entities, state and local governments, and private sector entities as appropriate in order to assist in deterring, preventing, and responding to terrorism against the United States;

(10) coordinating, or where appropriate, providing, training and other support as necessary to providers of information to the Department, or consumers of information from the Department, to allow them to identify and share information revealed in their ordinary duties or to utilize information from the Department, including training and

support under section 908 of the USA Patriot Act;

(11) receiving information from United States government agencies, including appropriate intelligence and law enforcement agencies, in order to comprehensively assess the vulnerabilities of key resources and critical infrastructures in the United States;

(12) integrating relevant information, intelligence analysis, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) to identify protective priorities and support protective measures by the Department, by other executive agencies, by State and local government personnel, agencies, and authorities, by the private sector, and by other entities to protect key resources and critical infrastructure in the United States;

(13) developing a comprehensive national plan for securing the key resources and critical infrastructure in the United States;

(14) establishing specialized research and analysis units for the purpose of processing intelligence to identify vulnerabilities and protective measures in —

(A) public health;

(B) food and water storage, production and distribution;

(C) commerce systems, including banking and finance;

(D) energy systems, including electric power and oil and gas production and storage;

(E) transportation systems, including pipelines;

(F) information and communication systems;

(G) continuity of government services; and

(H) other systems or facilities, the destruction or disruption of which could

cause substantial harm to health, safety, property, or the environment, as the Secretary may deem appropriate.

(15) enhancing the sharing of information regarding cyber security and physical security of the United States, developing appropriate security standards, tracking vulnerabilities, proposing improved risk management policies, and delineating the roles of various Government agencies in preventing, defending, and recovering from attacks;

(16) acting as the Critical Information Technology, Assurance, and Security Officer of the Department and assuming the responsibilities carried out by the Critical Infrastructure Assurance Office and the National Infrastructure Protection Center;

(17) coordinating the activities of the Information Sharing and Analysis Centers to share information, between the public and private sectors, on threats, vulnerabilities, individual incidents, and privacy issues regarding United States homeland security;

(18) coordinating with the Department of State on cyber security issues with respect to international bodies and coordinating with appropriate agencies in helping to establish cyber security policy, standards, and enforcement mechanisms;

(19) establishing the necessary organizational structure within the Directorate to provide leadership and focus on both cyber security and physical security, and ensuring the maintenance of a nucleus of cyber security and physical security experts within the United States government;

(20) conducting risk assessments to determine the risk posed by specific kinds of terrorist attacks, the probability of successful attacks, and the feasibility of specific countermeasures;

(21) analyzing intelligence about the means terrorists are likely to use to exploit

vulnerabilities in the homeland security infrastructure;

(22) developing and conducting experiments, tests, and inspections to test weaknesses in homeland defenses;

(23) taking or seeking to effect necessary measures to protect the key resources and critical infrastructures in the United States, in coordination with other executive agencies and in cooperation with State and local government personnel, agencies, and authorities, the private sector, and other entities; and

(24) performing such other related lawful and appropriate duties as the Secretary shall assign.

(d) FUNCTIONS TRANSFERRED.— The authorities, functions, personnel, and assets of the following entities are transferred to the Department:

(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;

(3) the Computer Security Division of the National Institute of Standards and Technology;

(4) the National Infrastructure Simulation and Analysis Center of the Department of Energy;

(5) the Federal Computer Incident Response Center of the General Services Administration;

(6) the Energy Security and Assurance Program of the Department of Energy;

(7) the Critical Infrastructure Assurance Office of the Department of Commerce; and

(8) the Federal Protective Service of the General Services Administration

(e) ACCESS TO INFORMATION.—

(1) IN GENERAL.— the Secretary shall have access to, and United States government agencies shall provide, all reports, assessments, and analytical information relating to the capabilities, intentions, and activities of terrorists and terrorists organizations and to other areas of responsibility as described in this Act, and all information concerning infrastructure or other vulnerabilities of the United States, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any United States government agency, except as otherwise directed by the President. The Secretary shall also have access to, and United States government agencies shall provide, other information, whether or not such information has been analyzed, relating to the foregoing matters, including significant and credible threats of terrorism against the United States, that may be collected, possessed, or prepared by a United States government agency, as the President may further provide; and

(2) COOPERATIVE AGREEMENTS.— the Secretary shall enter into cooperative arrangements with other United States government agencies, state and local governments, and private entities as necessary to acquire such material on a regular or routine basis, including requests or arrangements involving broad categories of material.

(f) AUTHORIZATION TO SHARE LAW ENFORCEMENT

INFORMATION.— The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official for purposes of the information-sharing provisions of —

(1) the USA PATRIOT Act of 2001 (P.L. 107-56);

(2) section 2517 (6) of title 18, United States Code; and

(3) rule 6 (e) 3 (c) of the Federal Rules of Criminal Procedure.

(g) TREATMENT OF DIRECTORATE AS ELEMENT OF INTELLIGENCE COMMUNITY. — Section 3 (4) of the National Security Act of 1947 (50 U.S.C. 401a (3) (4)) is amended —

(1) in subparagraph (I), by striking "and" at end;

(2) by redesignating subparagraph (J) as subparagraph (K); and

(3) by inserting after subparagraph (I) the following new subparagraph (J):

"(J) elements of the Directorate for Information Analysis and Infrastructure Protection that primarily perform functions relating to the analysis and dissemination of foreign intelligence, as designated by the President or jointly by the Secretary of Homeland Security and the Director of Central Intelligence, *provided that*, notwithstanding any other provision of law, the Director of Central Intelligence may not exercise direction or control over elements of the Department of Homeland Security that primarily perform functions relating to the analysis of vulnerabilities, or protection against attack, of United States key resources and critical infrastructure."