H. R. 4009

To direct the Secretary of Homeland Security to conduct comprehensive examinations of the human resource capabilities and needs, organizational structure, innovation and improvement plans, intelligence and information analysis capabilities and resources, infrastructure capabilities and resources, budget, and other elements of the homeland security program and policies of the United States.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 6, 2005

Mr. THOMPSON of Mississippi (for himself, Ms. HARMAN, Mr. LANGEVIN, Ms. ZOE LOFGREN of California, Ms. NORTON, Mr. PASCRELL, Mrs. CHRISTENSEN, Ms. JACKSON-Lee of Texas, Mr. DeFAZIO, Mr. MEEK of Florida, Mr. DICKS, Mr. ETHERIDGE, and Mrs. LOWEY) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Select Committee on Intelligence (Permanent Select) and Transportation and Infrastructure, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

A BILL

To direct the Secretary of Homeland Security to conduct comprehensive examinations of the human resource capabilities and needs, organizational structure, innovation and improvement plans, intelligence and information analysis capabilities and resources, infrastructure capabilities and resources, budget, and other elements of the homeland security program and policies of the United States.
Be it enacted by the Senate and House of Representa-
tives of the United States of America in Congress assembled,

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the

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

Sec. 1. Short title; table of contents.

TITLE I—DEPARTMENT OF HOMELAND SECURITY REFORMS

Sec. 102. Chief Intelligence Officer.
Sec. 103. Repeal of Directorate of Information Analysis and Infrastructure
Preparedness.
Sec. 104. Intra-agency task force on protection of unclassified but security-rel-
vant information provided by the private sector.
Sec. 105. Redesignation of Directorate.
Sec. 106. Establishment of Assistant Secretary for Preparedness.
Sec. 107. Establishment of Director and Deputy Director of Federal Emer-
gency Management Agency.
Sec. 108. Chief medical officer.
Sec. 109. Operations office.
Sec. 110. Authorities of the Privacy Officer of the Department of Homeland
Security.
Sec. 111. Greater accountability.
Sec. 112. Whistleblower protections.
Sec. 113. Office of Tribal Security.
Sec. 114. Assistant Secretary for Cybersecurity and Telecommunications.
Sec. 115. Assistant Secretary for Physical Infrastructure Security.
Sec. 116. Under Secretary for Policy.

TITLE II—SECURE HANDLING OF AMMONIUM NITRATE

Sec. 201. Short title.
Sec. 203. Definitions.
Sec. 204. Regulation of handling and purchase of ammonium nitrate.
Sec. 205. Enforcement.
Sec. 206. Administrative provisions.
Sec. 207. Civil liability.
Sec. 208. State law preemption.
TITLE I—DEPARTMENT OF
HOMELAND SECURITY REFORMS

SEC. 101. QUADRENNIAL HOMELAND SECURITY REVIEW.

(a) QUADRENNIAL HOMELAND SECURITY REVIEW.—Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding at the end the following new section:

“SEC. 104. QUADRENNIAL HOMELAND SECURITY REVIEW.

“(a) Review Required.—In any year following a year evenly divisible by 4, the Secretary, acting through the Under Secretary for Policy, shall conduct a comprehensive examination of the Department to be known as a Quadrennial Homeland Security Review.

“(b) Functions of Review.—The functions of the Quadrennial Homeland Security Review shall be the following:

“(1) To establish a 10-year homeland security strategy and policy program, to be known as the National Homeland Security Strategy, which shall be consistent with this Act.

“(2) To determine, with respect to the Department, each of the following:

“(A) Human resource capabilities and requirements.

“(B) Organizational structure.
“(C) Innovation and improvement plans.

“(D) Intelligence and information analysis capabilities and resources.

“(E) Infrastructure capabilities and resources.

“(F) Budget; technology resources, capabilities and requirements.

“(G) Any other elements required to support the National Homeland Security Strategy.

“(3) To identify, with respect to the Department, each of the following:

“(A) A budget plan, acquisition strategy, and procurement process to provide sufficient resources to successfully execute the responsibilities of the Department that are delineated in the National Homeland Security Strategy.

“(B) Any additional resources required to attain such responsibilities.

“(c) REPORT TO CONGRESS.—

“(1) REPORT.—The Secretary shall submit a report on each Quadrennial Homeland Security Review to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate. The report shall be submitted in the year
following the year in which the review is conducted, but not later than the date on which the President submits the budget for the next fiscal year to Congress under section 1105(a) of title 31, United States Code.

“(2) CONTENTS.—The report shall include the following:

“(A) The results of the Review, including a comprehensive discussion of the National Homeland Security Strategy and the structure best suited to implement it.

“(B) The assumed or defined homeland security interests of the United States that inform the National Homeland Security Strategy as defined in the review.

“(C) The threats to the assumed or defined homeland security interests of the United States examined for purposes of the review and any scenarios developed in the examination of such threats.

“(D) An explanation of any and all underlying assumptions used in the review.

“(E) The effect on human resource requirements and response capabilities, identified by type of threat, including conventional, nu-
clear, biological, chemical, radiological, and agri-
cultural threats, and by means of attack
through traditional and non-traditional means
or from traditional as well as non-traditional
sources.

“(F) The anticipated roles and responsibil-
ities of the agencies, components, and organiza-
tional elements of the Department, as outlined
in the National Homeland Security Strategy,
and the strength, capabilities, technology and
equipment necessary to assure that such agen-
cies, components, and organizational elements
can capably discharge such roles and respon-
sibilities.

“(G) An examination of any steps taken by
the Department to promote an “intelligence cul-
ture” among employees designed to develop
analyses specific to the overall mission of the
Department.

“(H) The strategic and tactical air, sea,
and ground transportation capabilities required
to support the National Homeland Security
Strategy.

“(I) The state of the physical infrastruc-
ture at border crossings and an examination of
the resources, personnel, and time necessary to assure that such border crossing are capable of supporting the mission of the Department, as outlined in the National Homeland Security Strategy.

“(J) The level of preparedness of first responders and an examination of the resources necessary to assure they are capable of fulfilling their responsibilities, as outlined in the National Homeland Security Strategy.

“(K) An examination of ports, airports, and other points of transshipment to determine the necessary resources to ensure adequate security and functioning, as outlined in the National Homeland Security Strategy.

“(L) An examination of the Nation’s rail and transit system to determine the necessary resources to ensure adequate security and functioning, as outlined in the National Homeland Security Strategy.

“(M) An examination and risk assessment of key resources and public and privately owned infrastructure and other facilities determined to present an increased security risk by the National Homeland Security Strategy.
“(N) An examination of the efforts of the Department to develop a consistent policy that encourages information sharing of unclassified but security-relevant information between the government and the private sector.

“(O) An examination of passenger and non-passenger modes of conveyance to ensure the adequacy of precautionary policies and measures to ensure the security of the general public.

“(P) An examination of the security of the computer systems and networks of the Federal Government to assure the adequacy of precautionary and protective devices.

“(Q) Any need for Department personnel or resources to be positioned outside the United States in order to support the National Homeland Security Strategy.

“(R) The extent to which domestic resources must be shifted in order to ensure that border crossings and ports of entry are adequately secured.

“(S) The effect of any technology anticipated to be available during the subsequent 8 years on the human resources capabilities,
costs, efficiencies, resources, and planning of the Department.

“(T) Any other matter the Secretary considers appropriate to include in the review.”.

(b) REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on any congressionally required reports which he views as duplicating the requirements under section 104 of the Homeland Security Act of 2002, as added by subsection (a).

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 103 the following new item:

“Sec. 104. Quadrennial Homeland Security Review.”.

SEC. 102. CHIEF INTELLIGENCE OFFICER.

(a) ESTABLISHMENT AND TRANSFER OF CERTAIN FUNCTIONS OF UNDER SECRETARY FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.—Subtitle A of title II of such Act is amended by adding at the end the following new section:
“SEC. 203. OFFICE OF INTELLIGENCE AND ANALYSIS AND CHIEF INTELLIGENCE OFFICER.

“(a) Office of Intelligence and Analysis.—There shall be in the Department an Office of Intelligence and Analysis headed by a Chief Intelligence Officer, who shall be appointed by the President.

“(b) Transitional Rule.—The Assistant Secretary for Information Analysis appointed pursuant to Sec. 201(b)(1) of this Act shall serve as the Chief Intelligence Officer.

“(c) Responsibilities of Chief Intelligence Officer.—Subject to the direction and control of the Secretary, the responsibilities of the Chief Intelligence Officer shall be as follows:

“(1) To act as the principal intelligence advisor to the Secretary.

“(2) To represent the Secretary to the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))).

“(3) To access, receive, and analyze law enforcement information, intelligence information, and other information from other agencies of the Federal Government, State, local, and tribal government agencies (including law enforcement agencies), and
private sector entities, and to integrate such infor-
mation in order to—

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

“(B) detect and identify threats of ter-
rorism against the United States; and

“(C) understand such threats in light of
actual and potential vulnerabilities of the home-
land.

“(4) To ensure, pursuant to section 202, that
the relevant personnel of the Department have time-
ly and efficient access to any information necessary
to discharge their responsibilities under this section,
including obtaining such information from other
agencies of the Federal Government;

“(5) To identify the intelligence-gathering com-
ponents of the Department and, within each compo-
nent, to promote an understanding of the intel-
ligence function of that component;

“(6) To establish, in consultation with other
agencies of the Federal Government, State, local,
and tribal government agencies (including law en-
forcement and intelligence agencies), and private
sector entities, a Department-wide terrorist intel-
ligence matrix, to identify and describe—
“(A) individuals and organizations suspected of terrorist involvement; and

“(B) current and developing terrorist capabilities, methods, plans, tactics, and threats.

“(7) To create a coordinated process for collecting and managing intelligence to be used by the intelligence-gathering components of the Department for providing relevant information for purposes of the terrorist intelligence matrix and other information needs of the Department.

“(8) To administer the Homeland Security Advisory System, including—

“(A) exercising primary responsibility for public advisories related to threats to homeland security; and

“(B) in coordination with other agencies of the Federal Government, providing specific warning information and advice about appropriate protective measures and countermeasures, to State, local and tribal government agencies and authorities, the private sector, other entities, and the public.

“(9) To establish a streamlined process within the Department and the Office of Intelligence and Analysis to receive, integrate, and distribute threat
assessment information through the Homeland Security Advisory System;

“(10) To review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the Federal Government and between the Federal Government and State, local, and tribal government agencies and authorities.

“(11) 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, local, and tribal 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.

“(12) 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-re-
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.

“(13) To consult with State, local, and tribal 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;

“(14) 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.
“(15) To request additional information from other agencies of the Federal Government, State, local and tribal 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.

“(16) 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.

“(17) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State, local and tribal 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 homeland security-relevant information revealed in their ordi-
nary duties and the optimal utilization of information received from the Department.

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

“(19) To establish within the Office of Intelligence Analysis an internal continuity of operations (COOP) plan that—

“(A) assures that the capability exists to continue uninterrupted intelligence analysis, collection, and related functions during a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies, that is maintained at a high level of readiness and is capable of implementation with and without warning; and

“(B) includes plans and procedures governing succession to office within the Office of Intelligence and Analysis, including—

“(i) emergency delegations of authority (where permissible, and in accordance with applicable law);

“(ii) the safekeeping of vital resources, facilities, and records;
“(iii) the improvisation or emergency acquisition of vital resources necessary for the performance of operations of the Office; and

“(iv) the capability to relocate essential personnel and functions to and to sustain the performance of the operations of the Office at an alternate work site until normal operations can be resumed.

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

“(d) Consultation With Assistant Secretary for Physical Infrastructure Security.—Subject to the direction and control of the Secretary, the Chief Intelligence Officer shall consult with the Assistant Secretary for Physical Infrastructure Security on the following responsibilities:

“(1) To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies.
“(2) 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.

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

“(e) TRANSFER OF FUNCTIONS.—In accordance with title XV, there shall be transferred to the Chief Intelligence Officer the functions, personnel, assets, and liabilities of the Directorate for Information Analysis and Infrastructure Protection.

“(f) INTELLIGENCE THROUGH EMPLOYEES GENERATING RESOURCES FOR ANALYTICAL LEADERSHIP (INTEGRAL) PROGRAM.—

“(1) FINDINGS.—Congress finds the following:
“(A) It is of critical importance that the Department establish an ‘intelligence culture’ among all of its employees.

“(B) At its inception, the Department drew together 22 Federal agencies that are now united in a common homeland security mission.

“(C) Most of those agencies were not intelligence agencies and were instead primarily concerned with either law enforcement or the provision of services.

“(D) Many employees who once worked for those agencies still do not view themselves as either collectors of intelligence information or contributors to the Department’s intelligence information analysis efforts.

“(E) The Department lacks an intelligence culture in which individuals understand that they are an integral part of a chain in which even the most seemingly insignificant piece of data can lead to the unraveling of a terrorist threat.

“(2) INTEGRAL PROGRAM.—The Secretary, acting through the Chief Intelligence Officer and in coordination with appropriate Department personnel, shall establish a program to be known as the Intel-
that—

“(A) is based on evaluations of how employees, including intelligence analysts and law enforcement agents, can better collect, analyze, process, and report intelligence information relevant to the intelligence analysis employees of the Department, the Chief Intelligence Officer, the Office of Intelligence and Analysis, and the wider intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)));

“(B) provides training, employee exchanges, and other educational opportunities for employees to better develop an understanding of the value of the intelligence information they collect for the intelligence analysis employees of the Department;

“(C) provides guidance on how the information Department employees collect can be used by the intelligence analysis employees of the Department and on what type of intelligence information is most useful;
“(D) creates mechanisms by which employees can communicate the information they gather to the intelligence analysis employees of the Department; and

“(E) establishes strategies for employees to adapt their daily work habits to promote an intelligence culture within the Department.”.

(b) REPORTS.—

(1) REPORT ON OFFICE OF INTELLIGENCE AND ANALYSIS AND CHIEF INTELLIGENCE OFFICER.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the effectiveness and activities of the Office of Intelligence and Analysis and the Chief Intelligence Officer.

(2) REPORT ON INTEGRAL PROGRAM.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the development of the INTEGRAL program established under section 201(e)(4) of the Homeland Security Act of 2002 (6 U.S.C. 121(e)(4)).
(c) CONFORMING AMENDMENTS.—Such Act is amended—

(1) in section 103, by striking “An Under Secretary for Information Analysis and Infrastructure Protection” and inserting “A Chief Intelligence Officer”;

(2) in section 223, by striking “section 201” and inserting “section 203”; and

(3) by striking “Under Secretary for Information Analysis and Infrastructure Protection” each place it appears and inserting “Chief Intelligence Officer”.

(d) HEADING AMENDMENT.—The heading for subtitle A of title II of such Act is amended by striking “Directorate for Information Analysis and Infrastructure Protection” and inserting “Chief Intelligence Officer”.

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

(1) by adding after the item relating to section 202 the following:

“Sec. 203. Chief Intelligence Officer.”

; and

(2) in the item relating to subtitle A of title II, by striking “Directorate for Information Analysis
and Infrastructure Protection” and inserting “Chief Intelligence Officer”.

SEC. 103. REPEAL OF DIRECTORATE OF INFORMATION ANALYSIS AND INFRASTRUCTURE PREPAREDNESS.

(a) REPEAL.—Section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) is repealed.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 201.

(c) CONFORMING AMENDMENT.—Section 510(d) of such Act is amended by striking “Directorate of Information Analysis and Infrastructure Preparedness” and inserting “Office of Intelligence and Analysis”.

SEC. 104. INTRA-AGENCY TASK FORCE ON PROTECTION OF UNCLASSIFIED BUT SECURITY-RELEVANT INFORMATION PROVIDED BY THE PRIVATE SECTOR.

(a) FINDINGS.—Congress finds the following:

(1) The vast majority of critical infrastructure located within the United States is privately owned.

(2) Securing this infrastructure from terrorist attack requires consistent policy and legislation that encourage the sharing of unclassified but security-
relevant information between the private sector and
the government.

(b) TASK FORCE.—The Secretary of the Department
of Homeland Security shall establish an intra-agency task
force to be comprised of the Chief Intelligence Officer of
the Department, the general counsel, the special assistant
to the Secretary (private sector), the officer for civil lib-
erties and civil rights, the privacy officer, and other appro-
priate personnel of the Department.

(c) STUDY.—The task force established under para-
graph (2) shall conduct a study of unclassified but secu-

rity-relevant information to—

(1) determine—

(A) what kind of information possessed by
the private sector is security-relevant but un-
classified information;

(B) how such information should be con-
trolled; and

(C) the significance of such information for
national security.

(2) propose a policy to encourage the sharing of
unclassified but security-relevant information be-
tween the private sector and government that—
(A) is sensitive to the public benefit of openness and which does not unnecessarily restrict public access to information;

(B) addresses private sector fears of business losses due to public disclosure of proprietary information, including disclosure through error, court documents, or public security announcements;

(C) addresses private sector fears of liability for disclosure; and

(D) addresses the fears of private citizens of inappropriate and overreaching government secrecy.

(d) REPORT.—Not later than 180 days after the date of the enactment of this Act, the task force shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report based on the study conducted under subsection (B).

SEC. 105. REDESIGNATION OF DIRECTORATE.

(a) IN GENERAL.—The Homeland Security Act of 2002 is amended—

(1) by striking “Directorate of Emergency Preparedness and Response” each place it appears and
inserting “Directorate of Preparedness and Response”;

(2) by striking “Under Secretary of Emergency Preparedness and Response” each place it appears and inserting “Under Secretary of Preparedness and Response”; and

(3) in the heading for title V, by striking “EMERGENCY”.

(b) CLERICAL AMENDMENT.—The item relating to title V in the table of contents in section 1(b) of such Act is amended by striking “Emergency”.

SEC. 106. ESTABLISHMENT OF ASSISTANT SECRETARY FOR PREPAREDNESS.

(a) ESTABLISHMENT.—Section 501 of the Homeland Security Act of 2002 (6 U.S.C. 311) is amended—

(1) in the section heading, by striking “UNDER SECRETARY FOR” and inserting “DIRECTORATE OF”;  

(2) by inserting “(a) ESTABLISHMENT OF DIRECTORATE; UNDER SECRETARY” before the first sentence; and

(3) by adding at the end the following: “(b) ASSISTANT SECRETARY.—
“(1) IN GENERAL.—There shall be in the Department an Assistant Secretary for Preparedness, who shall be appointed by the President.

“(2) RESPONSIBILITIES.—The Assistant Secretary for Preparedness shall perform such functions as were authorized to be performed by the Office for State and Local Government Coordination and Preparedness immediately before the enactment of the Department of Homeland Security Reform Act of 2005.

“(3) CONSULTATION WITH ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—The Assistant Secretary for Preparedness shall consult with the Assistant Secretary for Infrastructure Protection in the coordination and oversight of the following grant programs:

“(A) Buffer Zone Protection Program.

“(B) Transit Security Grant Program.

“(C) Intercity Passenger Rail Security Grant Program.

“(D) Truck Security Program.

“(E) Intercity Bus Security Program.

“(F) Port Security Grant Program.

“(4) PREPAREDNESS FOR TERRORISM.—In addition to the responsibilities under paragraph (2),
the Assistant Secretary for Preparedness shall have
the primary responsibility within the executive
branch of Government for the preparedness of the
United States for acts of terrorism, including—

“(A) coordinating preparedness efforts at
the Federal level, and working with all State,
local, tribal, parish, and private sector emer-
gency response providers on all matters per-
taining to combating terrorism, including train-
ing, exercises, and equipment support;

“(B) coordinating or, as appropriate, con-
solidating communications and systems of com-
munications relating to homeland security at all
levels of government;

“(C) directing and supervising terrorism
preparedness grant programs of the Federal
Government (other than those programs admin-
istered by the Department of Health and
Human Services) for all emergency response
providers;

“(D) incorporating the Strategy priorities
into planning guidance on an agency level for
the preparedness efforts of the Office for Do-
mestic Preparedness;
“(E) providing agency-specific training for agents and analysts within the Department, other agencies, and State and local agencies and international entities;

“(F) as the lead executive branch agency for preparedness of the United States for acts of terrorism, cooperating closely with the Federal Emergency Management Agency, which shall have the primary responsibility within the executive branch to prepare for and mitigate the effects of nonterrorist-related disasters in the United States;

“(G) assisting and supporting the Secretary, in coordination with other Directorates and entities outside the Department, in conducting appropriate risk analysis and risk management activities of State, local, and tribal governments consistent with the mission and functions of the Directorate;

“(H) those elements of the Office of National Preparedness of the Federal Emergency Management Agency which relate to terrorism, which shall be consolidated within the Department in the Office for Domestic Preparedness established under this section; and
“(I) helping to ensure the acquisition of interoperable communication technology by State and local governments and emergency response providers.

“(c) NATIONAL CAPITAL REGION COORDINATION.—The Under Secretary of Preparedness and Response shall have primary responsibility for oversight and coordination of Federal programs for and relationships with State, local, and regional authorities in the National Capital Region, as defined under section 2674(f)(2) of title 10, United States Code.

“(d) MILITARY LIAISON.—

“(1) ESTABLISHMENT.—There shall be in the Directorate of Preparedness and Response a Military Liaison, who shall be appointed by the President.

“(2) RESPONSIBILITIES.—The Military Liaison shall consult with the Secretary of Defense and coordinate the activities of the Directorate with the efforts of the Secretary of Defense to assist in preparedness and response with respect to hazards that threaten the loss of life and property in the United States.”.
(b) Clerical Amendment.—The table of contents in section 2 of such Act is amended by striking the item relating to section 501 and inserting the following:

“Sec. 501. Directorate of Preparedness and Response.”

(c) Elimination of Office for State and Local Government Coordination and Preparedness and Office for Domestic Preparedness.—


(2) Office for domestic preparedness.—Section 430 of the Homeland Security Act of 2002 (6 U.S.C. 238) is repealed.

(3) Clerical amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 430 and 801.

(d) Elimination of Office of National Capital Region Coordination.—

(1) Transfer of functions.—Effective as of the date of the enactment of this Act, there are transferred to the Directorate of Preparedness and Response the functions performed immediately before such transfer occurs by the Office of National Capital Region Coordination, pursuant to section
(2) REPEAL.—Section 882 of the Homeland Secu-


(3) CLERICAL AMENDMENT.—The table of con-

The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the item relating to section 882.

(4) CONFORMING AMENDMENT.—Section 102(c) of such Act is amended by striking “the Office of State and Local Coordination (established under section 801)” and inserting “the Under Secretary of Preparedness and Response”.

SEC. 107. ESTABLISHMENT OF DIRECTOR AND DEPUTY DIRECTOR OF FEDERAL EMERGENCY MANAGEMENT AGENCY.


(1) in the heading by striking “ROLE OF”;

(2) by redesignating subsections (a) and (b) as subsections (c) and (d), respectively; and

(3) by inserting before subsection (b), as so re-

designated, the following:

“(b) DIRECTOR.—
“(1) IN GENERAL.—The Federal Emergency Management Agency shall be headed by a Director who shall be an Assistant Secretary within the Preparedness and Response Directorate.

“(2) QUALIFICATION.—The Director shall be appointed by the President, by and with the advice and consent of the Senate, from among individuals who have extensive background in emergency or disaster-related management.

“(3) TERM OF OFFICE.—The term of office of an individual as Director shall be 5 years.

“(c) DEPUTY DIRECTOR.—There shall be a Deputy Director of the Federal Emergency Management Agency, who shall be appointed by the Director. The Deputy Director shall be a career Federal service employee.”.

(b) RATE OF PAY.—Chapter 53 of title 5, United States Code, is amended

(1) in section 5313 by adding at the end the following: “Director, Federal Emergency Management Agency.”; and

(2) in section 5314 by adding at the end the following: “Deputy Director, Federal Emergency Management Agency.”

(c) CLERICAL AMENDMENT.—The table of contents in section 2 of the Homeland Security Act of 2002 is
amended by striking the item relating to section 507 and inserting the following:

"Sec. 507. Federal Emergency Management Agency."

SEC. 108. CHIEF MEDICAL OFFICER.

(a) ESTABLISHMENT.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) is amended—

(1) by redesignating the second section 510 as section 511; and

(2) by adding at the end the following:

"SEC. 512. CHIEF MEDICAL OFFICER.

“(a) CHIEF MEDICAL OFFICER.—There is in the Directorate of Preparedness and Response a Chief Medical Officer who shall be an Assistant Secretary.

“(b) RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the responsibilities of the Chief Medical Officer shall include the following:

“(1) To coordinate activities related to emergency management system terrorism preparedness.

“(2) To serve as liaison to the emergency management system community.

“(3) To evaluate training programs and standards for emergency management system personnel related to terrorism preparedness.

“(4) To conduct periodic assessments into the needs and capabilities of emergency management
system providers, including governmental and non-
governmental providers.

“(5) To conduct periodic research into the num-
ber of emergency management system personnel, in-
cluding

“(A) governmental and nongovernmental
emergency management system personnel; and

“(B) emergency management system pro-
viders associated with fire departments or hos-
pitals.

“(6) To contribute to the development of mate-
rial threat assessments and material threat deter-
minations for Project BioShield.

“(7) To serve as a member of the Weapons of
Mass Destruction Medical Countermeasures sub-
committee of the National Science and Technology
Council and the White House Office of Science and
Technology Policy.

“(8) To consult with the Department of Health
and Human Services during the development of any
request for proposals under Project BioShield.

“(9) To be responsible for the oversight of the
Metropolitan Medical Response System.

“(10) To consult with the Secretary of Health
and Human Services and the Director of the Centers
for Disease Control and Prevention to ensure that
the public health infrastructure of the United States
is ready to respond to a mass casualty event or an
attack on the United States population involving a
biological, chemical, radiological, or nuclear weapon.

“(11) To develop and update guidelines to be
distributed to local authorities for medical plans for
responding to biological, chemical, radiological, or
nuclear weapon attacks.

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

(b) CLERICAL AMENDMENT.—The table of contents
in section 1(b) of the Homeland Security Act of 2002 is
amended by adding after the items relating to section 509
the following:

“Sec. 510. Procurement of security countermeasures for strategic national
stockpile.
“Sec. 511. Urban and other high risk area communications capabilities.
“Sec. 512. Chief Medical Officer.”.

SEC. 109. OPERATIONS OFFICE.

(a) SENSE OF CONGRESS REGARDING CONSOLIDA-
TION OF CBP AND ICE.—

(1) FINDINGS.—Congress finds that—

(A) the Bureau of Customs and Border
Protection (CBP) of the Department of Home-
land Security is responsible for managing, con-
trolling, and protecting the borders of the
United States, at and between United States ports of entry;

(B) U.S. Immigration and Customs Enforcement (ICE) of the Department of Homeland Security is the investigative and enforcement arm of the Department of Homeland Security responsible for hindering terrorism through the identification and resolution of violations and vulnerabilities in Federal immigration laws, customs laws, and air security laws;

(C) in the report titled “DHS 2.0 Rethinking The Department Of Homeland Security”, the Heritage Foundation recommended that a more efficient organization of border security which would be consistent with an effective homeland security program would require merging CBP and ICE;

(D) the current separation of CBP and ICE by the Department of Homeland Security has created organizational “turf battles” and inefficiency; and

(E) a combined entity containing components of CBP and ICE will bring together all of the tools for effective border and immigration enforcement.
(2) Sense of Congress.—It is the sense of Congress that the Bureau of Customs and Border Protection (CPB) and U.S. Immigration and Customs Enforcement (ICE), currently separate entities within the Department of Homeland Security, should be merged into a single operational unit within the Department of Homeland Security to better protect the borders of the United States and to conduct interior enforcement operations and investigations to increase homeland security.

(b) Report on the Functions of the Transportation Security Administration.—

(1) In general.—Within 120 days after the date of the enactment of this Act, the Secretary shall report to Congress the methodology and manner that the Transportation Security Administration will use to protect all modes of our Nation’s transportation systems from acts of terrorism.

(2) Requirements of report.—The report required under paragraph (1) shall set forth the following:

(A) Plans for the allocation of resources to manage risks, address threats, and enhance security across all transportation modes.
(B) The rationale for the allocation of resources that has resulted in non-aviation modes of transportation receiving fewer resources for security enhancements than aviation.

(C) A methodology to resolve the disparity in resource allocation across modes of transportation.

(D) Any structural and organizational changes necessary to ensure the effective operation and management of the Transportation Security Administration as a transportation security agency for all modes of transportation.

(E) A description of ongoing and planned research and development programs for all modes of transportation, including rail and transit security, that includes the funding for such programs and efforts that have occurred since March 11, 2004.

SEC. 110. AUTHORITIES OF THE PRIVACY OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.


(1) by striking “The Secretary shall establish” and inserting the following:
“(a) APPOINTMENT AND RESPONSIBILITIES.—The Secretary shall establish”; and

(2) by adding at the end the following new subsection:

“(b) AUTHORITY TO INVESTIGATE.—

“(1) IN GENERAL.—The senior official appointed under this section—

“(A) shall have access to any record, report, audit, review, document, paper, recommendation, or other material available to the Department relating to any program or operation for which the senior official has responsibility under this section;

“(B) shall make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the judgment of the senior official, necessary or desirable;

“(C) may require by subpoena the production, by persons other than Federal agencies, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the functions of the senior official under this section;
“(D) may administer to or take from any
person an oath, affirmation, or affidavit, whenever necessary to performance of the functions
of the senior official under this section; and

“(E) may take any other action authorized
to be taken by the Inspector General of the De-
partment, as necessary to require employees of
the Department to produce documents and an-
swer questions relevant to performance of the
functions of the senior official under this sec-
tion.

“(2) ENFORCEMENT OF SUBPOENAS.—Any sub-
poena issued under paragraph (1)(C) shall, in the
case of contumacy or refusal to obey, be enforceable
by order of any appropriate United States district
court.

“(3) EFFECT OF OATHS.—Any oath, affirma-
tion, or affidavit administered or taken under para-
graph (1)(D) by or before an employee of the Pri-
vacy Office designated for that purpose by the senior
official appointed under subsection (a) shall have the
same force and effect as if administered or taken by
or before an officer having a seal of office.

“(c) TERM OF OFFICE.—The term of appointment of
a senior official under subsection (a) shall be 5 years.
“(d) REPORTS TO CONGRESS.—The senior official appointed under subsection (a) shall submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any officer or employee of the Department or the Office of Management and Budget.”

SEC. 111. GREATER ACCOUNTABILITY.

(a) ELIMINATION OF UNDER SECRETARY FOR MANAGEMENT.—

(1) TRANSFER OF FUNCTIONS.—Effective as of the date of the enactment of this Act, there are transferred to the Secretary the functions performed immediately before such transfer occurs by the Under Secretary for Management pursuant to section 701(b) of the the Homeland Security Act of 2002 (6 U.S.C. 341(b)).

(2) REPEAL.—Section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341) is repealed.

(b) AUTHORITY OF CHIEF FINANCIAL OFFICER OVER COMPONENT FINANCIAL OFFICERS.—Section 702 of such Act (15 U.S.C. 342) is amended by adding at the end the following new sentence: “The Chief Financial Officer shall exercise joint authority, with the component agency heads of the Department, over financial officers
in the component agencies and entities of the Depart-
ment.’’

(c) Authority of Chief Information Officer
Over Component Information Officers.—Section
703 of such Act (15 U.S.C. 343) is amended by adding
at the end the following new sentence: “The Chief Infor-
mation Officer shall exercise joint authority, with the com-
ponent agency heads of the Department, over information
officers in the component agencies and entities of the De-
partment.’’

(d) Authority of Chief Human Capital Officer
of Component Human Capital Officers.—Section
704 of such Act (6 U.S.C. 344) is amended by striking
“and” after “as the Secretary may direct” and inserting
the following: “. The Chief Human Capital Officer shall
exercise joint authority, with the component agency heads
of the Department, over human capital officers in the com-
ponent agencies and entities of the Department. The Chief
Human Capital Officer shall”.

(e) Business Transformation Officer.—Title
VII of such Act (6 U.S.C. 341 et seq.) is amended by add-
ing at the end the following new section:

“SEC. 707. BUSINESS TRANSFORMATION OFFICER.

“The Business Transformation Officer shall report to
the Secretary, or to another official of the Department,"
as the Secretary may direct. The Business Transformation Officer shall—

“(1) develop an overarching management integration strategy with recommendations and performance goals for the Department, in consultation with the Chief Procurement Officer, the Chief Human Capital Officer, the Chief Intelligence Officer, and any other appropriate official of the Department; and

“(2) report to the Secretary and the appropriate congressional committees of jurisdiction on a quarterly basis as to the progress of the management integration strategy of the Department.”.

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

(1) by striking the item relating to section 701;

and

(2) by inserting after the item relating to section 706 the following:

“Sec. 707. Business Transformation Officer.”.

SEC. 112. WHISTLEBLOWER PROTECTIONS.

(a) IN GENERAL.—No covered individual may be discharged, demoted, suspended, threatened, harassed, reprimanded, investigated, or in any other manner discriminated against (including by a denial, suspension, or revocation of a security clearance or by any other security
access determination) if such discrimination is due, in whole or in part, to any lawful act done, perceived to have been done, or intended to be done by the covered individual—

(1) to provide information, cause information to be provided, or otherwise assist in an investigation regarding any conduct which the covered individual reasonably believes constitutes a violation of any law, rule or regulation relating to national or homeland security, which the covered individual reasonably believes constitutes a threat to national or homeland security, or which the covered individual reasonably believes constitutes fraud, waste or mismanagement of Government funds intended to be used for national or homeland security, when the information or assistance is provided to or the investigation is conducted by—

(A) a Federal, State or local regulatory or law enforcement agency (including an office of Inspector General under the Inspector General Act of 1978);

(B) any Member of Congress, any committee of Congress, or the Government Accountability Office;
(C) a person with supervisory authority over the covered individual (or such other person who has the authority to investigate, discover, or terminate misconduct); or

(D) the Privacy Officer of the Department;

(2) to file, cause to be filed, testify, participate in, or otherwise assist in a proceeding or action filed or about to be filed relating to an alleged violation of any law, rule or regulation relating to national or homeland security; or

(3) to refuse to violate or assist in the violation of any law, rule, or regulation relating to national or homeland security.

(b) ENFORCEMENT ACTION.—

(1) IN GENERAL.—A covered individual who alleges discharge or other discrimination by any person in violation of subsection (a) may seek relief under subsection (c) by—

(A) filing a complaint with the Secretary of Labor; or

(B) if the Secretary has not issued a final decision within 180 days after the filing of the complaint and there is no showing that such delay is due to the bad faith of the claimant, bringing an action at law or equity for de novo
review in the appropriate district court of the United States, which shall have jurisdiction over such an action without regard to the amount in controversy.

(2) PROCEDURE.—

(A) In general.—An action under paragraph (1)(A) shall be governed under the rules and procedures set forth in section 42121(b) of title 49, United States Code.

(B) Exception.—Notification made under section 42121(b)(1) of title 49, United States Code, shall be made to the person named in the complaint and to the person’s employer.

(C) Burdens of proof.—An action brought under paragraph (1)(B) shall be governed by the legal burdens of proof set forth in section 42121(b) of title 49, United States Code.

(D) Statute of limitations.—An action under paragraph (1) shall be commenced not later than 1 year after the date on which the violation occurs.

(e) Remedies.—

(1) In general.—A covered individual prevailing in any action under subsection (b)(1) shall be
entitled to all relief necessary to make the covered individual whole.

(2) DAMAGES.—Relief for any action under paragraph (1) shall include—

(A) reinstatement with the same seniority status that the covered individual would have had, but for the discrimination;

(B) the amount of any back pay, with interest;

(C) compensation for any special damages sustained as a result of the discrimination, including litigation costs, expert witness fees, and reasonable attorney fees; and

(D) punitive damages in an amount not to exceed the greater of 3 times the amount of any compensatory damages awarded under this section.

(d) STATE SECRETS PRIVILEGE.—If, in any action brought under subsection (b)(1)(B), the Government asserts as a defense the privilege commonly referred to as the “state secrets privilege” and the assertion of such privilege prevents the plaintiff from establishing a prima facie case in support of the plaintiff’s claim, the court shall enter judgment for the plaintiff and shall determine the relief to be granted.
(c) **Criminal Penalties.**—

(1) **In general.**—It shall be unlawful for any person employing a covered individual to commit an act prohibited by subsection (a). Any person violating this paragraph shall be fined under title 18 of the United States Code, imprisoned not more than 10 years, or both.

(2) **Reporting requirement.**—The Department of Justice shall submit to Congress an annual report on the enforcement of paragraph (1). Each such report shall (A) identify each case in which formal charges under paragraph (1) were brought, (B) describe the status or disposition of each such case, and (C) in any actions under subsection (b)(1)(B) in which the covered individual was the prevailing party or the substantially prevailing party, indicate whether or not any formal charges under paragraph (1) have been brought and, if not, the reasons therefor.

(f) **Rights retained by covered individual.**—Nothing in this section shall be deemed to diminish the rights, privileges, or remedies of any covered individual under any Federal or State law, or under any collective bargaining agreement. The rights and remedies in this section may not be waived by any agreement, policy, form, or condition of employment.
(g) DEFINITIONS.—For purposes of this section—

(1) the term “covered individual” means an employee of—

(A) the Department of Homeland Security (which, for purposes of this section, includes the Transportation Security Administration);

(B) a Federal contractor or subcontractor; and

(C) an employer within the meaning of section 701(b) of the Civil Rights Act of 1964 (42 U.S.C. 2000e(b));

(2) the term “lawful” means not specifically prohibited by law, except that, in the case of any information the disclosure of which is specifically prohibited by law or specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs, any disclosure of such information to any Member of Congress, committee of Congress, or other recipient authorized to receive such information, shall be deemed lawful;

(3) the term “Federal contractor” means a person who has entered into a contract with the Department of Homeland Security;

(4) the term “employee” means—
(A) with respect to an employer referred to in paragraph (1)(A), an employee as defined by section 2105 of title 5, United States Code; and

(B) with respect to an employer referred to in subparagraph (A) or (B) of paragraph (1), any officer, partner, employee, or agent;

(5) the term “subcontractor”—

(A) means any person, other than the Federal contractor, who offers to furnish or furnishes any supplies, materials, equipment, or services of any kind under a contract with the Department of Homeland Security or a subcontract entered into in connection with such a contract; and

(B) includes any person who offers to furnish or furnishes general supplies to the Federal contractor or a higher tier subcontractor; and

(6) the term “person” means a corporation, partnership, State entity, business association of any kind, trust, joint-stock company, or individual.

(h) AUTHORIZATION OF FUNDS.—Of the amounts authorized under section 101, there is authorized to be appropriated amounts necessary for carrying out this sec-
tion. Except as provided in the preceding sentence, this section shall have no force or effect.

SEC. 113. OFFICE OF TRIBAL SECURITY.

The Homeland Security Act of 2002 (Public Law 107–296) is amended—

(1) by inserting after section 801 the following new section:

“SEC. 802. OFFICE OF TRIBAL SECURITY.

“(a) SHORT TITLE.—This section may be cited as the ‘Tribal Homeland Security Act’.

“(b) ESTABLISHMENT.—There is established within the Department of Homeland Security the Office of Tribal Security.

“(c) DIRECTOR.—The Office of Tribal Security shall be administered by a Director, who shall report to the Secretary of Homeland Security.

“(d) DUTIES.—The Director shall be responsible for coordinating relations between the Federal Government and federally recognized Indian tribes on issues relating to homeland security, which shall include the following duties:

“(1) Providing a point of contact within Department of Homeland Security which shall be responsible for—
“(A) meeting the broad and complex Federal responsibilities owed to federally recognized Indian tribes by the Department of Homeland Security; and

“(B) soliciting and, where appropriate, addressing the homeland security concerns of federally recognized Indian tribes and other parties interested in Indian affairs.

“(2) Communicating relevant policies of the Department of Homeland Security to federally recognized Indian tribes and the public.

“(3) Promoting internal uniformity of Department of Homeland Security policies relating to Indian country (as defined in section 1151 of title 18, United States Code).

“(4) Coordinating with the relevant offices within the Department and tribal governments to develop a comprehensive border security policy that addresses law enforcement, personnel, and funding issues in Indian country (as defined in section 1151 of title 18, United States Code) on the United States borders with Canada and with Mexico.

“(5) Coordinating with the Assistant Secretary for Infrastructure Protection and tribal governments to develop appropriate policies for infrastructure
protection on Indian lands, as well as information sharing mechanisms with tribal governments.

“(6) Coordinating with the relevant offices within the Department to help ensure that tribal governments are fully informed of, have access to, and may apply for all Department of Homeland Security grant opportunities for emergency response providers, and to develop and achieve preparedness goals for tribal governments that are consistent with national goals for terrorism preparedness, as determined by the Department.

“(7) Coordinating with the Director of Science and Technology to identify opportunities to conduct research and development of homeland security technologies or scientific understanding for tribal universities or private sector entities.

“(8) Coordinating with U.S. Citizenship and Immigration Services and other relevant entities within the Department of Homeland Security having immigration services- or enforcement-related functions to develop policies on issues related to citizenship and the movement of members of federally recognized Indian tribes across the United States border, taking into consideration the unique characteristics of certain federally recognized Indian tribes
with jurisdiction over lands adjacent to the Canadian
and Mexican borders.

“(9) Coordinating with other offices within the
Department of Homeland Security to develop and
implement sound policies regarding Indian country
(as defined in section 1151 of title 18, United States
Code) and tribal governments.”; and

(2) in the table of sections, by inserting after
the item relating to section 801 the following new
item:

“Sec. 802. Office of Tribal Security.”.

SEC. 114. ASSISTANT SECRETARY FOR CYBERSECURITY
AND TELECOMMUNICATIONS.

(a) IN GENERAL.—Title V of the Homeland Security
Act of 2002 (6 U.S.C. 311 et seq.), as amended by section
108, is further amended by adding at the end the following
new section:

“SEC. 513. ASSISTANT SECRETARY FOR CYBERSECURITY
AND TELECOMMUNICATIONS.

“(a) IN GENERAL.—There shall be in the Directorate
for Preparedness and Response a National Cybersecurity
Office, which shall be headed by an Assistant Secretary
for Cybersecurity and Telecommunications, who shall be
appointed by the President.

“(b) GENERAL AUTHORITY.—Subject to the direction
and control of the Secretary, the Assistant Secretary for
Cybersecurity and Telecommunications shall have primary authority within the Department for all critical infrastructure protection programs of the Department relating to cybersecurity, including with respect to policy formulation and program management.

“(c) RESPONSIBILITIES.—The Assistant Secretary for Cybersecurity and Telecommunications shall assist the Secretary in promoting national cybersecurity and telecommunications security and the responsibilities of the Assistant Secretary shall include the following duties:

“(1) To establish and manage—

“(A) a national cybersecurity response system that includes the ability to—

“(i) analyze the effect of cybersecurity threat information on national critical infrastructure; and

“(ii) aid in the detection and warning of attacks on cybersecurity infrastructure and in the restoration of such infrastructure in the aftermath of an attack;

“(B) a national cybersecurity threat and vulnerability reduction program to—

“(i) identify cybersecurity vulnerabilities that effect critical national infrastructure;
“(ii) perform vulnerability assessments on information technologies; and

“(iii) coordinate the mitigation of such vulnerabilities;

“(C) a national cybersecurity awareness and training program to promote cybersecurity awareness among the public and the private sectors and cybersecurity training and education programs;

“(D) a Government-wide cybersecurity program to coordinate and consult with Federal, State, and local governments to enhance their cybersecurity programs; and

“(E) a national security and international cybersecurity cooperation program to help foster Federal efforts to enhance international cybersecurity awareness and cooperation.

“(2) To coordinate with the private sector as appropriate and to promote cybersecurity information sharing, vulnerability assessment, and threat warning with respect to critical infrastructure.

“(3) To coordinate with other directorates and offices within the Department on the cybersecurity aspects of their missions.
“(4) To coordinate with the Under Secretary for Policy to ensure that the national response plan developed pursuant to section 502(6) includes appropriate measures for the recovery of the cybersecurity elements of critical infrastructure.

“(5) To develop processes for information sharing with the private sector, consistent with section 214, that—

“(A) promote voluntary cybersecurity best practices, standards, and benchmarks that are responsive to rapid technology changes and to the security needs of critical infrastructure; and

“(B) consider roles of Federal, State, local, and foreign governments and the private sector, including the insurance industry and auditors.

“(6) To coordinate with the Chief Information Officer in establishing a secure information sharing architecture and information sharing processes, including with respect to the operation centers of the Department.

“(7) To consult with the Electronic Crimes Task Force of the United States Secret Service on private sector outreach and information activities.

“(8) To consult with the Director of the Office for Domestic Preparedness to ensure that realistic
cybersecurity scenarios are incorporated into tabletop and recovery exercises.

“(9) To consult and coordinate, as appropriate, with other Federal agencies on cybersecurity-related programs, policies, and operations.

“(10) To consult and coordinate within the Department and, where appropriate, with other relevant Federal agencies, on security of digital control systems, such as Supervisory Control and Data Acquisition systems.

“(d) AUTHORITY OVER THE NATIONAL COMMUNICATIONS SYSTEM.—The Assistant Secretary shall have primary authority within the Department over the National Communications System.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the items relating to title V the following new item:

“Sec. 513. Assistant Secretary for Cybersecurity and Telecommunications.”.

SEC. 115. ASSISTANT SECRETARY FOR PHYSICAL INFRASTRUCTURE SECURITY.

(a) IN GENERAL.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.), as amended by sections 108 and 114, is further amended by adding at the end the following new section:
"SEC. 514 ASSISTANT SECRETARY FOR PHYSICAL INFRASTRUCTURE SECURITY.

(a) In General.—There shall be in the Directorate for Preparedness and Response an Assistant Secretary for Physical Infrastructure Security, who shall be appointed by the President.

(b) Assistant Secretary for Physical Infrastructure Security.—

(1) Authority.—Subject to the direction and control of the Secretary, the Assistant Secretary for Physical Infrastructure Security shall have primary authority within the Department, including authority with respect to policy formulation and program management, for all physical critical infrastructure protection programs of the Department, including the following areas of responsibility:

(A) Agriculture.

(B) Food.

(C) Water.

(D) Public Health.

(E) Emergency Services.

(F) Government.

(G) Defense Industrial Base.

(H) Energy.

(I) Transportation.

(J) Banking and Finance.

“(L) Postal and Shipping.

“(M) National Icons and Monuments.

“(N) Commercial Assets.

“(O) Dams.

“(P) Nuclear Power Plants.

“(Q) Structures housing a significant number of people.

“(2) RESPONSIBILITIES.—The Assistant Secretary for Physical Infrastructure Security shall assist the Under Secretary for Preparedness and Response in discharging the responsibilities of the Under Secretary under this section. Subject to the direction and control of the Secretary, the responsibilities of the Assistant Secretary for Physical Infrastructure Security shall be as follows:

“(A) To establish and manage—

“(i) a national physical infrastructure security system to—

“(I) analyze the effect of physical infrastructure threats on the population, national economy, and other critical infrastructure; and
“(II) aid in the detection and warning of attacks on, and in the restoration of, physical security infrastructure in the aftermath of attacks on the national physical infrastructure;

“(ii) a national physical infrastructure vulnerability reduction program that identifies vulnerabilities of critical infrastructure, performs vulnerability assessments on infrastructure systems and technologies, and coordinates the mitigation of such vulnerabilities; and

“(iii) a program to coordinate and consult with Federal, State, and local governments to enhance their physical security programs.

“(B) To coordinate with other directorates and offices within the Department on infrastructure security.

“(C) To coordinate with the Under Secretary for Preparedness and Response to ensure that the National Response Plan developed pursuant to section 502(6) includes appropriate
measures for the recovery of the physical infra-
structure elements.

“(D) To develop processes for sharing in-
formation with state and local governments, 
and, if appropriate, the private sector, to—

“(i) promote voluntary infrastructure 
security best practices, standards, and 
benchmarks that are responsive to rapid 
technology changes and to the security 
needs of critical infrastructure; and 

“(ii) consider the roles of Federal, 
State, local, and foreign governments and 
the private sector, including the insurance 
industry and auditors.

“(E) To consult with the Under Secretary 
for Preparedness and Response to ensure that 
realistic infrastructure security scenarios are in-
corporated into tabletop and recovery exercises.

“(F) To consult and coordinate, as appro-
priate, with other Federal agencies on pro-
grams, policies, and operations related to infra-
structure security.

“(G) To advise the Under Secretary for 
Preparedness and Response on any regulatory
authority that is needed in order to fulfill the responsibilities listed in this section.

“(H) 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).

“(I) 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.

“(J) To recommend measures necessary to protect the key resources and critical infra-
structure 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.

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

“(3) Consultation with Chief Intelligence Officer.—Subject to the direction and control of the Secretary, the Assistant Secretary for Physical Infrastructure Security shall consult with the Chief Intelligence Officer on the following responsibilities:

“(A) To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies.

“(B) 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—
“(i) are compatible with one another
and with relevant information databases of
other agencies of the Federal Government;
and
“(ii) treat information in such data-
bases in a manner that complies with ap-
licable Federal law on privacy.
“(C) To coordinate with elements of the
intelligence community and with Federal, State,
and local law enforcement agencies, and the pri-
ivate sector, as appropriate.”.

(b) REPORTS REQUIRED.—

(1) REPORT ON CERTAIN VULNERABILITIES.—

(A) IN GENERAL.—Not later than Decem-
ber 30, 2005, the Assistant Secretary for Phys-
ical Infrastructure Security of the Department
of Homeland Security, in coordination with the
Chief Intelligence Officer of the Department of
Homeland Security and appropriate personnel
charged with infrastructure protection and
emergency preparedness and response for the
Department, shall submit to the President and
Congress a comprehensive report assessing the
vulnerabilities of the key resources and critical infrastructure of the United States.

   (B) METHODOLOGY.—The report shall be based on commonly accepted risk-assessment methodologies and shall prioritize vulnerabilities based upon actual and prospective threats so that appropriate protective and support measures can be taken. To the extent possible, the report should include not only a general prioritization of vulnerabilities but also a prioritization of vulnerabilities by resource and infrastructure sector.

   (c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the items relating to title V the following new item:

   “Sec. 514. Assistant Secretary for Physical Infrastructure Security.”.

SEC. 116. UNDER SECRETARY FOR POLICY.

Section 103(a) of such Act is amended—

   (1) by redesignating paragraphs (6) through (10) as paragraphs (7) through (11), accordingly; and

   (2) by inserting after paragraph (5) the following new paragraph (6):

   “(6) An Under Secretary for Policy.”.
TITLE II—SECURE HANDLING OF
AMMONIUM NITRATE

SEC. 201. SHORT TITLE.
This title may be cited as the “Secure Handling of
Ammonium Nitrate Act of 2005”.

SEC. 202. FINDINGS.
Congress finds the following:

(1) Although ammonium nitrate is an impor-
tant fertilizer used in agricultural production, in the
wrong hands, ammonium nitrate can be used to cre-
ate explosives and was so used in terrorist attacks
conducted in in Oklahoma City, Bali, and Istanbul.

(2) The production, importation, storage, sale,
and distribution of ammonium nitrate affects inter-
state and intrastate commerce.

(3) It is necessary for the Secretary of Home-
land Security to regulate the production, storage,
sale, and distribution of ammonium nitrate on ac-
count of the prior use of ammonium nitrate to cre-
ate explosives used in acts of terrorism and the pre-
vent terrorists from acquiring ammonium nitrate to
create explosives.

SEC. 203. DEFINITIONS.
In this title:
(1) TITLE.—The term “this title” includes regulations issued under this title.

(2) AMMONIUM NITRATE.—The term “ammonium nitrate” means solid ammonium nitrate that is chiefly the ammonium salt of nitric acid and contains not less than 33 percent nitrogen, of which—

(A) 50 percent is in ammonium form; and

(B) 50 percent is in nitrate form.

(3) FACILITY.—The term “facility” means any site where ammonium nitrate is produced, stored, or held for distribution, sale, or use. The term includes—

(A) all buildings or structures used to produce, store, or hold ammonium nitrate for distribution, sale, or use at a single site; and

(B) multiple sites described in subparagraph (A), if the sites are—

(i) contiguous or adjacent; and

(ii) owned or operated by the same person.

(4) HANDLE.—The term “handle” means to produce, store, sell, or distribute ammonium nitrate.

(5) HANDLER.—The term “handler” means any person that produces, stores, sells, or distributes ammonium nitrate.
Purchaser.—The term “purchaser” means any person that purchases ammonium nitrate.

Terrorism.—The term “terrorism” has the meaning given that term in section 2(15) of the Homeland Security Act of 2002 (6 U.S.C. 101(15)).

Secretary.—The term “Secretary” means the Secretary of Homeland Security.

SEC. 204. REGULATION OF HANDLING AND PURCHASE OF AMMONIUM NITRATE.

(a) In General.—The Secretary may regulate the handling and purchase of ammonium nitrate to prevent the misappropriation or use of ammonium nitrate in an act of terrorism.

(b) Regulations.—The Secretary may promulgate regulations that require—

(1) handlers—

(A) to register facilities;

(B) to sell or distribute ammonium nitrate only to handlers and purchasers registered under this title; and

(C) to maintain records of sale or distribution that include the name, address, telephone number, and registration number of the imme-
mediate subsequent purchaser of ammonium nitrate; and

(2) purchasers to be registered.

(c) Use of Previously Submitted Information.—Prior to requiring a facility or handler to submit new information for registration under this section, the Secretary shall—

(1) request from the Attorney General, and the Attorney General shall provide, any information previously submitted to the Attorney General by the facility or handler under section 843 of title 18, United States Code; and

(2) at the election of the facility or handler—

(A) use the license issued under that section in lieu of requiring new information for registration under this section; and

(B) consider the license to fully comply with the requirement for registration under this section.

(d) Consultation.—In promulgating regulations under this section, the Secretary shall consult with the Secretary to Agriculture to ensure that the access of agricultural producers to ammonium nitrate is not unduly burdened.
(e) DATA CONFIDENTIALITY.—Notwithstanding section 552 of title 5, United States Code, or the USA PATRIOT ACT (Public Law 107–56; 115 Stat. 272) or an amendment made by that Act, the Secretary may not disclose to any person any information obtained from any facility, handler, or purchaser—

(1) regarding any action taken, or to be taken, at the facility or by the handler or purchaser to ensure the secure handling of ammonium nitrate; or

(2) that would disclose—

(A) the identity or address of any purchase of ammonium nitrate;

(B) the quantity of ammonium nitrate purchased; or

(C) the details of the purchase transaction.

(f) EXCEPTIONS TO DATA CONFIDENTIALITY.—The Secretary may disclose any information described in subsection (e)—

(1) to an officer or employee of the United States, or a person that has entered into a contract with the United States, who needs to know the information to perform the duties of the officer, employee, or person, or to a State agency pursuant to an arrangement under section 206, under appro-
priate arrangements to ensure the protection of the
information;

(2) to the public, to the extent the Secretary
specifically finds that disclosure of particular infor-
mation is required in the public interest; or

(3) to the extent required by order of a Federal
court in a proceeding in which the Secretary is a
party, under such protective measures as the court
may prescribe.

**SEC. 205. ENFORCEMENT.**

(a) **INSPECTIONS.**—The Secretary, without a war-
rant, may enter any place during business hours that the
Secretary believes may handle ammonium nitrate to deter-
mine whether the handling is being conducted in accord-
ance with this title.

(b) **PREVENTION OF SALE OR DISTRIBUTION
ORDER.**—In any case in which the Secretary has reason
to believe that ammonium nitrate has been handled other
than in accordance with this title, the Secretary may issue
a written order preventing any person that owns, controls,
or has custody of the ammonium nitrate from selling or
distributing the ammonium nitrate.

(e) **APPEAL PROCEDURES.**—

(1) **IN GENERAL.**—A person subject to an order
under subsection (b) may request a hearing to con-
test the order, under such administrative adjudication procedures as the Secretary may establish.

(2) Rescission.—If an appeal under paragraph (1) is successful, the Secretary shall rescind the order.

(d) In Rem Proceedings.—The Secretary may institute in rem proceedings in the United States district court for the district in which the ammonium nitrate is located to seize and confiscate ammonium nitrate that has been handled in violation of this title.

SEC. 206. ADMINISTRATIVE PROVISIONS.

(a) Cooperative Agreements.—The Secretary may enter into a cooperative agreement with the Secretary of Agriculture, or the head of any State department of agriculture or other State agency that regulates plant nutrients, to carry out this title, including cooperating in the enforcement of this title through the use of personnel or facilities.

(b) Delegation.—

(1) In General.—The Secretary may delegate to a State the authority to assist the Secretary in the administration and enforcement of this title.

(2) Delegation Required.—On the request of a Governor of a State, the Secretary shall delegate to the State the authority to carry out section
204 or 205, on a determination by the Secretary that the State is capable of satisfactorily carrying out that section.

(3) **FUNDING.**—If the Secretary enters into an agreement with a State under this subsection to delegate functions to the State, the Secretary shall provide to the State adequate funds to enable the State to carry out the functions.

(4) **INAPPLICABILITY.**—Notwithstanding any other provision of this subsection, this subsection does not authorize a State to carry out a function under section 204 or 205 relating to a facility or handler in the State that makes the election described in section 204(c)(2).

**SEC. 207. CIVIL LIABILITY.**

(a) **UNLAWFUL Acts.**—It is unlawful for any person—

(1) to fail to perform any duty required by this title;

(2) to violate the terms of registration under this title;

(3) to fail to keep any record, make any report, or allow any inspection required by this title; or

(4) to violate any sale or distribution order issued under this title.
(b) Penalties.—

(1) In general.—A person that violates this title may only be assessed a civil penalty by the Secretary of not more than $50,000 per violation.

(2) Notice and opportunity for a hearing.—No civil penalty shall be assessed under this title unless the person charged has been given notice and opportunity for a hearing on the charge in the county, parish, or incorporated city of residence of the person charged.

(c) Jurisdiction over actions for civil damages.—The district courts of the United States shall have exclusive jurisdiction over any action for civil damages against a handler for any harm or damage that is alleged to have resulted from the use of ammonium nitrate in violation of law that occurred on or after the date of enactment of this title.

Sec. 208. State law preemption.

This title preempts any State law that regulates the handling of ammonium nitrate to prevent the misappropriation or use of ammonium nitrate in an act of terrorism.