107TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
107–615

PROVIDING FOR CONSIDERATION OF H.R. 5005, HOMELAND SECURITY ACT OF 2002

JULY 25, 2002.—Referred to the House Calendar and ordered to be printed

---

Ms. PRYCE of Ohio, from the Committee on Rules, submitted the following

R E P O R T

[To accompany H. Res. 502]

The Committee on Rules, having had under consideration House Resolution 502, by a nonrecord vote, report the same to the House with the recommendation that the resolution be adopted.

SUMMARY OF PROVISIONS OF THE RESOLUTION

The resolution provides for the consideration of H.R. 5005, the Homeland Security Act of 2002, under a structured rule. The rule provides 90 minutes of general debate equally divided and controlled by the chairman and ranking minority member of the Select Committee on Homeland Security. The rule waives all points of order against consideration of the bill.

The rule provides that the amendment in the nature of a substitute recommended by the Select Committee on Homeland Security now printed in the bill shall be considered as an original bill for the purpose of amendment and shall be considered as read. The rule waives all points of order against the bill, as amended.

The rule provides that no amendment to the committee amendment in the nature of a substitute shall be in order except those printed in this report and amendments en bloc described in section 3 of the resolution.

The rule provides that each amendment printed in this report may be offered only in the order printed in this report, may be offered only by a Member designated in this report, shall be considered as read, shall be debatable for the time specified in this report equally divided and controlled by the proponent and an opponent, shall not be subject to amendment, and shall not be subject to a demand for division of the question in the House or in the Committee of the Whole, except as specified in section 4 of the resolution. The rule waives all points of order against the amendments

printed in this report or amendments en bloc described in section 3 of the resolution.

The rule provides that it shall be in order at any time for the chairman of the Select Committee on Homeland Security or his designee to offer amendments en bloc consisting of amendments printed in this report not earlier disposed of or germane modifications of any such amendment.

The rule provides that amendments en bloc offered pursuant to the rule shall be considered as read (except that modifications shall be reported), shall be debatable for 20 minutes equally divided and controlled by the chairman and ranking minority member of the Select Committee on Homeland Security or their designees, shall not be subject to amendment, and shall not be subject to a demand for division of the question in the House or in the Committee of the Whole.

The rule further provides that for the purpose of inclusion in such amendments en bloc, an amendment printed in the form of a motion to strike may be modified to the form of a germane perfecting amendment to the text originally proposed to be stricken.

The rule provides that the original proponent of an amendment included in such amendments en bloc may insert a statement in the Congressional Record immediately before the disposition of the amendments en bloc.

The rule provides that the Chairman of the Committee of the Whole may recognize for consideration of any amendment printed in the report out of the order printed, but not sooner than one hour after the chairman of the Select Committee on Homeland Security or his designee announces from the floor a request to that effect. Finally, the rule provides one motion to recommit with or without instructions.

The waiver of all points or order against the consideration of the bill includes a waiver of clause 4(a) of rule XIII (requiring a three-day layover of the committee report), which is needed because H. Rept. 107–609 was filed by the Select Committee on Homeland Security on the calendar day of Wednesday, July 24, and the bill may be considered by the House as early as Thursday, July 25. The waiver of all points of order against consideration of the bill and against the committee amendment in the nature of a substitute includes a waiver of section 306 of the Congressional Budget Act (prohibiting consideration of legislation within the jurisdiction of the Committee on the Budget unless reported by the Budget Committee). The waiver of all points of order against the committee amendment in the nature of a substitute includes a waiver of clause 4 of rule XXI (prohibiting appropriations in legislative bills), which is needed because provisions contained in section 811 of the committee amendment are in violation of this rule.

SUMMARY OF AMENDMENTS MADE IN ORDER UNDER THE RULE

Oberstar/Costello/Roemer #56: Retains FEMA as an independent agency with responsibility for natural disaster preparedness, response, and recovery. (20 minutes)

Young (AK) #64: Restores the Federal Emergency Management Agency as an entity. Ensures that FEMA carries out all of its statutory missions, not just those related to homeland security. Continues FEMA's role as the lead agency for the Federal Response

Plan established under Executive Order 12148 and 12656. (20 minutes)

Waxman #94: Codifies and strengthens the White House Office of Homeland Security which was established by executive order in October, 2001. Defines the functions of the Office. The head of the Office is appointed by the President with advice and consent of the Senate. Specifically subjects the Office and its Director to oversight by Congress. (40 minutes)

Cox #52: Provides specific, illustrative examples of the types of critical cybersecurity infrastructure which the Undersecretary for Information Analysis and Infrastructure Protection must develop a plan to protect. (10 minutes)

Israel #18: Creates an Advisory Committee for the Undersecretary for Science and Technology. (10 minutes)

Rivers #16: Creates an Office of Inquires within the Department of Science and Technology which would act as a point of entry for individuals or companies seeking guidance on how to pursue proposals to develop or deploy products that would contribute to homeland security. (10 minutes)

Woolsey #19: Adds a new section to the bill creating a Homeland Security Institute as a federally-funded research and development center. (10 minutes)

Cardin #27: Preserves the existing Customs Service as a "distinct entity" within the DHS. The amendment does not affect the bill's provisions which protect certain revenue and trade act enforcement functions of the Customs Service. (10 minutes)

Hunter #60: Sense of Congress that completion of the San Diego Border Fence Project is a priority of DHS. (10 minutes)

Ose #7: Requires the Under Secretary of Management to develop a plan, within one year, to consolidate and co-locate regional and field offices in each of the cities with an existing regional or field office transferred to the DHS. (10 minutes)

Velazquez/Issa/Wilson #49: Ensures that the Department of Homeland Security has procurement goals for small business that are no less than the statutory minimum. Ensures that those employees responsible for this goal attainment have a corresponding criteria in their performance evaluations. (10 minutes)

Hastings (FL) #2: Adds a new section to title VII that directs the Secretary to comply with laws protecting equal employment opportunity and provides whistle blower protections. States that nothing in the Act shall be construed as exempting the DHS from the requirements that are applicable to all other executive agencies. (10 minutes)

Rogers (KY) #87: Ensures that if the Federal Law Enforcement Training Center is transferred to the Department of Justice, the Department of Justice will not alter the operations of the Center. (10 minutes)

Rogers (KY) #41: Grants permissive authority to the DHS Secretary for the creation of a Joint Interagency Homeland Security Taskforce. (10 minutes)

Rush #25: Establishes within the Office of the Secretary an office to oversee and coordinate developmental programs for and relationships with states and local governments. (10 minutes)

Shays/Watson #23: Requires biennial reports to Congress on the status of homeland security preparedness, including a report on

each state. Requires a report to Congress, within one year of enactment, ensuring the maintenance of core functions transferred to the DHS and recommending statutory changes to facilitate implementation of the reorganization effort. (10 minutes)

Shays #85: Similar to the Morella amendment approved by the Government Reform Committee, except for an additional section stating that the provisions of the amendment would not apply where the President determines in writing that such application would have a substantial adverse impact on the Department's ability to protect homeland security. (20 minutes)

Morella #40: Allows existing employees transferred into DHS, who have the same job responsibilities, to still belong to a union. If their responsibilities changed so they were directly involved in the war on terrorism, they could be exempted from being part of a union by the President. Those employees or units that did not have union representation before the transfer would not be granted any extra protections by this amendment. (20 minutes)

Quinn #82: Clarifies workers rights in section 761. (20 minutes)

Waxman/Frost #95: Deletes the entire human resources which exempt employees of the new Department from Title 5. Provides that federal employees transferred to the new agency could not have their pay reduced. Strengthens whistleblower protections. (20 minutes)

Armey #69: En Bloc Manager's Amendment. Technical amendments requested by Energy and Commerce Committee. Technical amendments requested by Science Committee. Technical correction regarding Oil Spill Liability Trust Fund requested by Transportation and Infrastructure Committee. Technical amendments relating to DHS privacy officer. Technical correction relating to biological agent registration function requested by Agriculture Committee. An amendment to create a program to encourage and support innovative solutions to enhance homeland security (requested by Mr. Davis and Ms. Harman). An amendment to enhance nonfederal cybersecurity activities of Under Secretary for Information Analysis and Infrastructure Protection (requested by Science Committee). An amendment to establish "NET Guard" program to promote volunteer activities in support of information technology protection activities (requested by Science Committee). An amendment striking section 814 (relating to incidental transfers by the Director of OMB) requested by Appropriations Committee. A Technical correction to section 761 to insert a proper reference. An amendment inserting sense of Congress provision reaffirming the Posse Comitatus Act. An amendment clarifying that this Act preempts no state or local law, except that any preemption authority vested in agencies or officials transferred to DHS shall be transferred to DHS. An amendment inserting text of "Federal Information Security management Act of 2002" (recommended by Committee on Government Reform at request of Mr. Davis), which creates a new Title XI to address Federal information security. Transfers to the DHS the computer information security standards currently promulgated by the Secretary of Commerce and permanently reauthorizes the agency-wide risk management information security approach in the Government Information Security Reform Act of 2000 (GISRA) and eliminates GISRA's two-year sunset. Second, it would strengthen reforms initiated by the existing GISRA by clarifying

terms, correcting mistakes, and streamlining requirements. Requires the development, promulgation, and compliance with minimum mandatory management controls for securing information. Includes Amendments to subtitle F of title VII (relating to liability management) intended to clarify availability of liability protections afforded by this title. An amendment inserting a new section to reinstate liability cap for aviation screening companies. A clarification responsibilities of the DHS and the DHS Counternarcotics Officer with regard to narcotics interdiction. A clarification of the eligibility criteria for participation in certain extramural research programs of the Department. Includes technical amendment to section 766, regarding regulatory authority. New section expressing the sense of Congress regarding funding of trauma systems. (40 minutes)

Turner #88: Indemnifies companies who sell anti-terrorism technologies to the federal government, as well as, state and local governments, in a manner similar to the protection afforded under P.L. 85–804. (40 minutes)

Oberstar/Menendez #55: Strikes sec. 409 of the bill (Extension of Airline Baggage Screening Deadline). (45 minutes)

Schakowsky/Kucinich/Mink #51: Strikes subtitle C of section VII. Strikes section 762 from the bill and replaces with language that provides remedies for retaliation against whistleblowers. (30 minutes)

Davis, Tom #83: Expands the existing FOIA exemption in the homeland security legislation to other federal agencies as the Secretary of Homeland Security determines as appropriate. (20 minutes)

Chambliss/Harman/Shays/Menendez #9: Directs that critical threat information be shared between federal law enforcement and intelligence agencies with state and local personnel, including granting security clearances to appropriate state and local personnel. Directs the President to develop procedures by which federal agencies will share homeland security information with state and local personnel and vice versa. Requires that any information that is shared must not be used for any unauthorized purpose and the procedures must ensure the security and confidentiality of the information as well as the removal or deletion of obsolete or erroneous information. Protects information collected by the census. Allows certain types of information to be shared with appropriate state and local offices consistent with guidelines issued by the Attorney General and Director of Central Intelligence. (20 minutes)

Weldon (FL) #54: Amends sections 402 and 403 of the bill to transfer the visa office from the Department of State to the DHS. Provides for a two-year transition period during which the Foreign Service Officers issuing visas would be detailed to the DHS while new DHS personnel are trained and deployed abroad. Preserves the Secretary of State's authority to deny a visa based in the national interest of the U.S. Prohibits judicial review of consular decisions to refuse a visa. (20 minutes)

TEXT OF AMENDMENTS MADE IN ORDER

1. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE OBERSTAR OF MINNESOTA, OR HIS DESIGNEE, DEBATABLE FOR 20 MINUTES

Strike section 402(5) of the bill (and redesignate subsequent paragraphs accordingly).

In section 501(1) of the bill, strike ", major disasters, and other emergencies".

In the matter preceding subparagraph (A) of section 501(3) of the bill, strike "and major disasters".

In section 501(3)(D) of the bill, strike "or major disaster".

In section 501(4) of the bill—

(1) strike "and major disasters";

(2) strike "or major disasters"; and

(3) strike "or disasters".

In section 501(5) of the bill, strike "and disasters".

Strike section 501(6) of the bill and insert the following:

(6) In consultation with the Director of the Federal Emergency Management Agency, consolidating existing Federal Government emergency response plans for terrorist attacks into the Federal Response Plan referred to in section 506(b).

In section 502(1) of the bill, strike the text after "(1)" and preceding "Integrated" and insert "The".

At the end of title V of the bill, insert the following (and conform the table of contents of the bill accordingly):

SEC. 506. ROLE OF FEDERAL EMERGENCY MANAGEMENT AGENCY.

(a) IN GENERAL.—The functions of the Federal Emergency Management Agency include, but are not limited to, the following:

(1) All functions and authorities prescribed by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(2) Carrying out its mission to reduce the loss of life and property and protect the Nation from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program—

(A) of mitigation, by taking sustained actions to reduce or eliminate long-term risk to people and property from hazards and their effects;

(B) of preparedness, by building the emergency management profession to prepare effectively for, mitigate against, respond to, and recover from any hazard by planning, training, and exercising;

(C) of response, by conducting emergency operations to save lives and property through positioning emergency equipment and supplies, through evacuating potential victims, through providing food, water, shelter, and medical care to those in need, and through restoring critical public services;

(D) of recovery, by rebuilding communities so individuals, businesses, and governments can function on their own, return to normal life, and protect against future hazards; and

(E) of increased efficiencies, by coordinating efforts relating to preparedness and response activities to maximize efficiencies.

(b) FEDERAL RESPONSE PLAN.—

(1) ROLE OF FEMA.—Notwithstanding any other provision of this Act, the Federal Emergency Management Agency shall remain the lead agency for the Federal Response Plan established under Executive Order 12148 (44 Fed. Reg. 43239) and Executive Order 12656 (53 Fed. Reg. 47491).

(2) REVISION OF RESPONSE PLAN.—Not later than 60 days after the date of enactment of this Act, the Director of the Federal Emergency Management Agency shall revise the Federal Response Plan to reflect the establishment of and incorporate the Department.

(3) MEMORANDUM OF UNDERSTANDING.—Not later than 60 days after the date of enactment of this Act, the Secretary and the Director of the Federal Emergency Management Agency shall adopt a memorandum of understanding to address the roles and responsibilities of their respective agencies under this title.

---

2. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE YOUNG OF ALASKA, OR HIS DESIGNEE, DEBATABLE FOR 20 MINUTES

Strike section 402(5) of the bill (and redesignate subsequent paragraphs accordingly).

In section 502(1) of the bill, strike "Except as provided in section 402, the" and insert "The".

At the end of title 5 of the bill, add the following (and conform the table of contents of the bill accordingly):

SEC. 506. ROLE OF FEDERAL EMERGENCY MANAGEMENT AGENCY.

(a) IN GENERAL.—The functions of the Federal Emergency Management Agency include, but are not limited to, the following:

(1) All functions and authorities prescribed by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(2) Carrying out its mission to reduce the loss of life and property and protect the Nation from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program—

(A) of mitigation, by taking sustained actions to reduce or eliminate long-term risk to people and property from hazards and their effects;

(B) of preparedness, by building the emergency management profession to prepare effectively for, mitigate against, respond to, and recover from any hazard by planning, training, and exercising;

(C) of response, by conducting emergency operations to save lives and property through positioning emergency equipment and supplies, through evacuating potential victims, through providing food, water, shelter, and medical care to those in need, and through restoring critical public services;

(D) of recovery, by rebuilding communities so individuals, businesses, and governments can function on their own, return to normal life, and protect against future hazards; and

(E) of increased efficiencies, by coordinating efforts relating to preparedness and response activities to maximize efficiencies.

(b) FEDERAL RESPONSE PLAN.—

(1) ROLE OF FEMA.—Notwithstanding any other provision of this Act, the Federal Emergency Management Agency shall remain the lead agency for the Federal Response Plan established under Executive Order 12148 (44 Fed. Reg. 43239) and Executive Order 12656 (53 Fed. Reg. 47491).

(2) REVISION OF RESPONSE PLAN.—Not later than 60 days after the date of enactment of this Act, the Director of the Federal Emergency Management Agency shall revise the Federal Response Plan to reflect the establishment of and incorporate the Department.

---

3. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE WAXMAN OF CALIFORNIA, OR HIS DESIGNEE, DEBATABLE FOR 40 MINUTES

At the end of the bill add the following new title:

TITLE XI—OFFICE OF HOMELAND SECURITY

SEC. 1101. ESTABLISHMENT.

(a) IN GENERAL.—There is established in the Executive Office of the President an Office of Homeland Security.

(b) DIRECTOR.—The head of the Office shall be the Director of Homeland Security, who shall be appointed by the President with advice and consent of the Senate.

SEC. 1102. MISSION.

As provided in Executive Order 13228, the mission of the Office of Homeland Security is to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.

SEC. 1103. FUNCTIONS.

As provided in Executive Order 13228, the functions of the Office of Homeland Security shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. Such functions shall include—

(1) working with executive departments and agencies, State and local governments, and private entities to ensure the adequacy of the national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats or attacks within the United States and periodically reviewing and coordinating revisions to that strategy as necessary;

(2) identifying priorities and coordinating efforts for collection and analysis of information regarding threats of terrorism

against the United States, including ensuring that all executive departments and agencies that have intelligence collection responsibilities have sufficient technological capabilities and resources and that, to the extent permitted by law, all appropriate and necessary intelligence and law enforcement information relating to homeland security is disseminated to and exchanged among appropriate executive departments and agencies;

(3) coordinating national efforts to prepare for and mitigate the consequences of terrorist threats or attacks within the United States, including coordinating Federal assistance to State and local authorities and nongovernmental organizations to prepare for and respond to terrorist threats or attacks and ensuring the readiness and coordinated deployment of Federal response teams to respond to terrorist threats or attacks;

(4) coordinating efforts to prevent terrorist attacks within the United States;

(5) coordinating efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks;

(6) coordinating efforts to respond to and promote recovery from terrorist threats or attacks within the United States;

(7) coordinating the domestic response efforts of all departments and agencies in the event of an imminent terrorist threat and during and in the immediate aftermath of a terrorist attack within the United States and acting as the principal point of contact for and to the President with respect to coordination of such efforts;

(8) in coordination with the Assistant to the President for National Security Affairs, reviewing plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership;

(9) coordinating the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States and coordinating the development of programs for educating the public about the nature of terrorist threats and appropriate precautions and responses; and

(10) encouraging and inviting the participation of State and local governments and private entities, as appropriate, in carrying out the Offices's functions.

SEC. 1104. ACCESS TO INFORMATION.

As provided in Executive Order 13288, executive agencies, shall, to the extent permitted by law, make available to the Office of Homeland Security all information relating to terrorist threats and activities within the United States.

SEC. 1105. BUDGET APPROVAL.

(a) AUTHORITY.—The Director of the Office of Homeland Security shall—

(1) review the budget requests submitted to the President by all executive agencies with homeland security responsibilities; and

(2) if a budget request fails to conform to the objectives set forth in the national strategy described in section 1102, may disapprove such budget request.

(b) EFFECT OF DISAPPROVAL.—In any case in which a budget request is disapproved under subsection (a)—

(1) the Director shall notify the appropriate Committees of Congress; and

(2) the President may not include such budget request in the annual budget submission to Congress unless the President makes an express determination that including such request is in the national interest.

SEC. 1106. ADMINISTRATION.

As provided in Executive Order 13288, the Office of Administration within the Executive Office of the President shall provide the Office of Homeland Security with such personnel, funding, and administrative support, to the extent permitted by law and subject to the availability of appropriations, as necessary to carry out the provisions of this title.

SEC. 1107. DETAIL AND ASSIGNMENT.

As provided in Executive Order 13288, the heads of executive agencies are authorized, to the extent permitted by law, to detail or assign personnel of such agencies to the Office of Homeland Security upon request of the Director of Homeland Security.

SEC. 1108. OVERSIGHT BY CONGRESS.

The establishment of the Office of Homeland Security within the Executive Office of the President shall not be construed as affecting access by Congress, or any committee of Congress, to—

(1) any information, document, or study in the possession of, or conducted by or at the direction of, the Director; or

(2) personnel of the Office.

---

4. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE COX OF CALIFORNIA, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

In section 201(5), insert the following before the period at the end: "including, but not limited to, 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".

---

5. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE ISRAEL OF NEW YORK, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of title III, insert the following new section:

SEC. 309. HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—There is established within the Department a Homeland Security Science and Technology Advisory Committee (in this section referred to as the "Advisory Committee"). The Advisory Committee shall make recommendations with respect to the activities of the Under Secretary for Science and Technology,

including identifying research areas of potential importance to the security of the Nation.

(b) MEMBERSHIP.—

(1) APPOINTMENT.—The Advisory Committee shall consist of 20 members appointed by the Under Secretary for Science and Technology, which shall include emergency first-responders or representatives of organizations or associations of emergency first-responders. The Advisory Committee shall also include representatives of citizen groups, including economically disadvantaged communities. The individuals appointed as members of the Advisory Committee—

(A) shall be eminent in fields such as emergency response, research, engineering, new product development, business, and management consulting;

(B) shall be selected solely on the basis of established records of distinguished service;

(C) shall not be employees of the Federal Government; and

(D) shall be so selected as to provide representation of a cross-section of the research, development, demonstration, and deployment activities supported by the Under Secretary for Science and Technology.

(2) NATIONAL RESEARCH COUNCIL.—The Under Secretary for Science and Technology may enter into an arrangement for the National Research Council to select members of the Advisory Committee, but only if the panel used by the National Research Council reflects the representation described in paragraph (1).

(c) TERMS OF OFFICE.—

(1) IN GENERAL.—Except as otherwise provided in this subsection, the term of office of each member of the Advisory Committee shall be 3 years.

(2) ORIGINAL APPOINTMENTS.—The original members of the Advisory Committee shall be appointed to three classes of three members each. One class shall have a term of one year, one a term of two years, and the other a term of three years.

(3) VACANCIES.—A member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed for the remainder of such term.

(d) ELIGIBILITY.—A person who has completed two consecutive full terms of service on the Advisory Committee shall thereafter be ineligible for appointment during the one-year period following the expiration of the second such term.

(e) MEETINGS.—The Advisory Committee shall meet at least quarterly at the call of the Chair or whenever one-third of the members so request in writing. Each member shall be given appropriate notice of the call of each meeting, whenever possible not less than 15 days before the meeting.

(f) QUORUM.—A majority of the members of the Advisory Committee not having a conflict of interest in the matter being considered by the Advisory Committee shall constitute a quorum.

(g) CONFLICT OF INTEREST RULES.—The Advisory Committee shall establish rules for determining when one of its members has

a conflict of interest in a matter being considered by the Advisory Committee.

(h) REPORTS.—

(1) ANNUAL REPORT.—The Advisory Committee shall render an annual report to the Under Secretary for Science and Technology for transmittal to the Congress on or before January 31 of each year. Such report shall describe the activities and recommendations of the Advisory Committee during the previous year.

(2) ADDITIONAL REPORTS.—The Advisory Committee may render to the Under Secretary for transmittal to the Congress such additional reports on specific policy matters as it considers appropriate.

(i) FACA EXEMPTION.—Section 14 of the Federal Advisory Committee Act shall not apply to the Advisory Committee.

Amend the table of contents accordingly.

---

6. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE RIVERS OF MICHIGAN, OR HER DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of title III, insert the following new section:

SEC. 309. INQUIRIES.

(a) OFFICE.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish an office to serve as a point of entry for individuals or companies seeking guidance on how to pursue proposals to develop or deploy products that would contribute to homeland security. Such office shall refer those seeking guidance on Federal funding, regulation, acquisition, or other matters to the appropriate unit of the Department or to other appropriate Federal agencies.

(b) FUNCTIONS.—The Under Secretary for Science and Technology shall work in conjunction with the Technical Support Working Group (organized under the April, 1982, National Security Decision Directive Numbered 30) to—

(1) screen proposals described in subsection (a), as appropriate;

(2) assess the feasibility, scientific and technical merits, and estimated cost of proposals screened under paragraph (1), as appropriate;

(3) identify areas where existing technologies may be easily adapted and deployed to meet the homeland security agenda of the Federal Government; and

(4) develop and oversee the implementation of homeland security technology demonstration events, held at least annually, for the purpose of improving contact among technology developers, vendors, and acquisition personnel.

Amend the table of contents accordingly.

---

7. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE WOOLSEY OF CALIFORNIA, OR HER DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of title III, insert the following new section:

SEC. 309. HOMELAND SECURITY INSTITUTE.

(a) ESTABLISHMENT.—The Secretary shall establish a federally funded research and development center to be known as the "Homeland Security Institute" (in this section referred to as the "Institute").

(b) ADMINISTRATION.—The Institute shall be administered as a separate entity by the Secretary.

(c) DUTIES.—The duties of the Institute shall be determined by the Secretary, and may include the following:

(1) Systems analysis, risk analysis, and simulation and modeling to determine the vulnerabilities of the Nation's critical infrastructures and the effectiveness of the systems deployed to reduce those vulnerabiblities.

(2) Economic and policy analysis to assess the distributed costs and benefits of alternative approaches to enhancing security.

(3) Evaluation of the effectiveness of measures deployed to enhance the security of institutions, facilities, and infrastructure that may be terrorist targets.

(4) Identification of instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for field operators and first responders.

(5) Assistance for Federal agencies and departments in establishing testbeds to evaluate the effectiveness of technologies under development and to assess the appropriateness of such technologies for deployment.

(6) Design of metrics and use of those metrics to evaluate the effectiveness of homeland security programs throughout the Federal Government, including all national laboratories.

(7) Design of and support for the conduct of homeland security-related exercises and simulations.

(8) Creation of strategic technology development plans to reduce vulnerabilities in the Nation's critical infrastructure and key resources.

(d) CONSULTATION ON INSTITUTE ACTIVITIES.—In carrying out the duties described in subsection (c), the Institute shall consult widely with representatives from private industry, institutions of higher education, and nonprofit institutions.

(e) ANNUAL REPORTS.—The Institute shall transmit to the Secretary and the Congress an annual report on the activities of the Institute under this section.

Amend the table of contents accordingly.

---

8. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE CARDIN OF MARYLAND, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

In section 401(1), add the following at the end: "The functions, personnel, assets, and obligations of the Customs Service so transferred shall be maintained as a distinct entity within the Department.".

---

9. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE HUNTER OF CALIFORNIA, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of chapter 1 of subtitle B of title IV, add the following:

SEC. 416. SENSE OF CONGRESS REGARDING CONSTRUCTION OF FENCING NEAR SAN DIEGO, CALIFORNIA.

It is the sense of the Congress that completing the 14-mile border fence project required to be carried out under section 102(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note) should be a priority for the Secretary.

---

10. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE OSE OF CALIFORNIA, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of title VI add the following:

SEC. . CONSOLIDATION AND CO-LOCATION OF OFFICES.

Not later than 1 year after the date of the enactment of this Act, the Secretary shall develop and submit to the Congress a plan for consolidating and co-locating—

(1) any regional offices or field offices of agencies that are transferred to the Department under this Act, if such officers are located in the same municipality; and

(2) portions of regional and field offices of other Federal agencies, to the extent such offices perform functions that are transferred to the Secretary under this Act.

---

11. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE VELAZQUEZ OF NEW YORK, OR HER DESIGNEE, DEBATABLE FOR 10 MINUTES

In section 734 of the bill, insert before the first sentence the following:

(a) OFFICE OF SMALL AND DISADVANTAGED BUSINESS UTILIZATION.—

At the end of section 734 of the bill, add the following new subsection:

(b) SMALL BUSINESS PROCUREMENT GOALS.—

(1) IN GENERAL.—The Secretary shall annually establish goals for the participation by small business concerns, by small business concerns owned and controlled by service-disabled veterans, by qualified HUBZone small business concerns, by small business concerns owned and controlled by socially and economically disadvantaged individuals, and by small business concerns owned and controlled by women (as such terms are defined pursuant to the Small Business Act (15 U.S.C. 631 et seq.) and relevant regulations promulgated thereunder) in procurement contracts of the Department.

(2) DEPARTMENT GOALS NOT LESS THAN GOVERNMENT-WIDE GOALS.—Notwithstanding section 15(g) of the Small Business Act (15 U.S.C. 644(g)), each goal established under paragraph (1) shall be equal to or greater than the corresponding Government-wide goal established by the President under section 15(g)(1) of the Small Business Act (15 U.S.C. 644(g)(1)).

(3) INCENTIVE FOR GOAL ACHIEVEMENT.—Achievement of the goals established under paragraph (1) shall be an element in the performance standards for employees of the Department who have the authority and responsibility for achieving such goals.

---

12. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE HASTINGS OF FLORIDA, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of title VII, insert the following new section:

SEC. 7. REQUIREMENT TO COMPLY WITH LAWS PROTECTING EQUAL EMPLOYMENT OPPORTUNITY AND PROVIDING WHISTLEBLOWER PROTECTIONS.

Nothing in this Act shall be construed as exempting the Department from requirements applicable with respect to executive agencies—

(1) to provide equal employment protection for employees of the Department (including pursuant to the provisions in section 2302(b)(1) of title 5, United States Code, and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (Pub. L. 107–174)); or

(2) to provide whistleblower protections for employees of the Department (including pursuant to the provisions in section 2302(b)(8) of such title and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002).

---

13. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE KINGSTON OF GEORGIA, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Add at the end of subtitle G of title VII the following:

SEC. . FEDERAL LAW ENFORCEMENT TRAINING CENTER.

(a) IN GENERAL.—The transfer of an authority or an agency under this Act to the Department of Homeland Security does not affect training agreements already entered into with the Federal Law Enforcement Training Center with respect to the training of personnel to carry out that authority or the duties of that transferred agency.

(b) CONTINUITY OF OPERATIONS.—All activities of the Federal Law Enforcement Training Center transferred to the Department of Justice under this Act shall continue to be carried out at the locations such activities were carried out before such transfer.

---

14. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE ROGERS OF KENTUCKY, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the appropriate place in the bill, add the following new section:

SEC. . JOINT INTERAGENCY TASK FORCE.

(a) ESTABLISHMENT.—The Secretary may establish and operate a permanent Joint Interagency Homeland Security Task Force composed of representatives from military and civilian agencies of the United States Government for the purposes of anticipating terrorist threats against the United States and taking appropriate actions to prevent harm to the United States.

(b) STRUCTURE.—It is the sense of Congress that the Secretary should model the Joint Interagency Homeland Security Task Force on the approach taken by the Joint Interagency Task Forces for drug interdiction at Key West, Florida and Alameda, California, to the maximum extent feasible and appropriate.

---

15. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE RUSH OF ILLINOIS, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of subtitle G of title VII add the following:

SEC. 7 . OFFICE FOR STATE AND LOCAL GOVERNMENT COORDINATION.

(a) ESTABLISHMENT.—There is established within the Office of the Secretary the Office for State and Local Government Coordination, to oversee and coordinate departmental programs for and relationships with State and local governments.

(b) RESPONSIBILITIES.—The Office established under subsection (a) shall—

(1) coordinate the activities of the Department relating to state and local government;

(2) assess, and advocate for, the resources needed by State and local government to implement the national strategy for combating terrorism;

(3) provide State and local government with regular information, research, and technical support to assist local efforts at securing the homeland; and

(4) develop a process for receiving meaningful input from State and local government to assist the development of the national strategy for combating terrorism and other homeland security activities.

---

16. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE SHAYS OF CONNECTICUT, OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of subtitle G of title VII insert the following:

SEC. 7 . REPORTING REQUIREMENTS.

(a) BIENNIAL REPORTS.—Every 2 years the Secretary shall submit to Congress—

(1) a report assessing the resources and requirements of executive agencies relating to border security and emergency preparedness issues;

(2) a report certifying the preparedness of the United States to prevent, protect against, and respond to natural disasters, cyber attacks, and incidents involving weapons of mass destruction; and

(3) a report assessing the emergency preparedness of each State, including an assessment of each State's coordination with the Department with respect to the responsibilities specified in section 501.

(b) ADDITIONAL REPORT.—Not later than 1 year after the effective date of this Act, the Secretary shall submit to Congress a report—

(1) assessing the progress of the Department in—

(A) implementing this Act; and

(B) ensuring the core functions of each entity transferred to the Department are maintained and strengthened; and

(2) recommending any conforming changes in law necessary as a result of the enactment and implementation of this Act.

---

17. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE SHAYS OF CONNECTICUT, OR HIS DESIGNEE, DEBATABLE FOR 20 MINUTES

Page 189, after line 7, insert the following (and redesignate succeeding sections and references thereto accordingly):

SEC. 762. LABOR-MANAGEMENT RELATIONS.

(a) LIMITATION ON EXCLUSIONARY AUTHORITY.—

(1) IN GENERAL.—No agency or subdivision of an agency which is transferred to the Department pursuant to this Act shall be excluded from the coverage of chapter 71 of title 5, United States Code, as a result of any order issued under section 7103(b)(1) of such title 5 after June 18, 2002, unless—

(A) the mission and responsibilities of the agency (or subdivision) materially change; and

(B) a majority of the employees within such agency (or subdivision) have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

(2) EXCLUSIONS ALLOWABLE.—Nothing in paragraph (1) shall affect the effectiveness of any order to the extent that such order excludes any portion of an agency or subdivision of an agency as to which—

(A) recognition as an appropriate unit has never been conferred for purposes of chapter 71 of such title 5; or

(B) any such recognition has been revoked or otherwise terminated as a result of a determination under subsection (b)(1).

(b) PROVISIONS RELATING TO BARGAINING UNITS.—

(1) LIMITATION RELATING TO APPROPRIATE UNITS.—Each unit which is recognized as an appropriate unit for purposes of chapter 71 of title 5, United States Code, as of the day before the effective date of this Act (and any subdivision of any such unit) shall, if such unit (or subdivision) is transferred to the Department pursuant to this Act, continue to be so recognized for such purposes, unless—

(A) the mission and responsibilities of such unit (or subdivision) materially change; and

(B) a majority of the employees within such unit (or subdivision) have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

(2) LIMITATION RELATING TO POSITIONS OR EMPLOYEES.—No position or employee within a unit (or subdivision of a unit) as to which continued recognition is given in accordance with paragraph (1) shall be excluded from such unit (or subdivision), for purposes of chapter 71 of such title 5, unless the primary job duty of such position or employee—

(A) materially changes; and

(B) consists of intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

In the case of any positions within a unit (or subdivision) which are first established on or after the effective date of this Act and any employees first appointed on or after such date, the preceding sentence shall be applied disregarding subparagraph (A).

(c) HOMELAND SECURITY.—Subsections (a), (b), and (d) of this section shall not apply in circumstances where the President determines in writing that such application would have a substantial adverse impact on the Department's ability to protect homeland security.

(d) COORDINATION RULE.—No other provision of this Act or of any amendment made by this Act may be construed or applied in a manner so as to limit, supersede, or otherwise affect the provisions of this section, except to the extent that it does so by specific reference to this section.

---

18. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE MORELLA OF MARYLAND, OR HER DESIGNEE, DEBATABLE FOR 20 MINUTES

In subtitle G of title VII of the bill, insert after section 761 the following (and redesignate succeeding sections and references thereto accordingly):

SEC. 762. LABOR-MANAGEMENT RELATIONS.

(a) LIMITATION ON EXCLUSIONARY AUTHORITY.—

(1) IN GENERAL.—No agency or subdivision of an agency which is transferred to the Department pursuant to this Act shall be excluded from the coverage of chapter 71 of title 5, United States Code, as a result of any order issued under section 7103(b)(1) of such title 5 after June 18, 2002, unless—

(A) the mission and responsibilities of the agency (or subdivision) materially change; and

(B) a majority of the employees within such agency (or subdivision) have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

(2) EXCLUSIONS ALLOWABLE.—Nothing in paragraph (1) shall affect the effectiveness of any order to the extent that such order excludes any portion of an agency or subdivision of an agency as to which—

(A) recognition as an appropriate unit has never been conferred for purposes of chapter 71 of such title 5; or

(B) any such recognition has been revoked or otherwise terminated as a result of a determination under subsection (b)(1).

(b) PROVISIONS RELATING TO BARGAINING UNITS.—

(1) LIMITATION RELATING TO APPROPRIATE UNITS.—Each unit which is recognized as an appropriate unit for purposes of chapter 71 of title 5, United States Code, as of the day before the effective date of this Act (and any subdivision of any such unit) shall, if such unit (or subdivision) is transferred to the Department pursuant to this Act, continue to be so recognized for such purposes, unless—

(A) the mission and responsibilities of such unit (or subdivision) materially change; and

(B) a majority of the employees within such unit (or subdivision) have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

(2) LIMITATION RELATING TO POSITIONS OR EMPLOYEES.—No position or employee within a unit (or subdivision of a unit) as to which continued recognition is given in accordance with paragraph (1) shall be excluded from such unit (or subdivision), for purposes of chapter 71 of such title 5, unless the primary job duty of such position or employee-

(A) materially changes; and

(B) consists of intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

In the case of any positions within a unit (or subdivision) which are first established on or after the effective date of this Act and any employees first appointed on or after such date, the preceding sentence shall be applied disregarding subparagraph (A).

(c) COORDINATION RULE.—No other provision of this Act or of any amendment made by this Act may be construed or applied in a manner so as to limit, supersede, or otherwise affect the provisions of this section, except to the extent that it does so by specific reference to this section.

---

19. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE QUINN OF NEW YORK, OR HIS DESIGNEE, DEBATABLE FOR 20 MINUTES

In section 761(a) of the bill, redesignate paragraphs (1) and (2) as paragraphs (2) and (3), respectively, and insert after the heading for subsection (a) the following:

(1) SENSE OF CONGRESS.—It is the sense of the Congress that—

(A) it is extremely important that employees of the Department be allowed to participate in a meaningful way in the creation of any human resources management system affecting them;

(B) such employees have the most direct knowledge of the demands of their jobs and have a direct interest in ensuring that their human resources management system is conducive to achieving optimal operational efficiencies;

(C) the 21st century human resources management system envisioned for the Department should be one that benefits from the input of its employees; and

(D) this collaborative effort will help secure our homeland.

In paragraph (4) of section 9701(b) of title 5, United States Code (as proposed to be added by section 761(a) of the bill), strike all that follows "by law" and insert "; and".

In section 9701 of title 5, United States Code (as proposed to be added by section 761(a) of the bill), redesignate subsection (e) as subsection (g) and insert after subsection (d) the following:

"(e) PROVISIONS TO ENSURE COLLABORATION WITH EMPLOYEE REPRESENTATIVES.—

"(1) IN GENERAL.—In order to ensure that the authority of this section is exercised in collaboration with, and in a manner that ensures the direct participation of employee representatives in the planning, development, and implementation of any human resources management system or adjustments under this section, the Secretary of Homeland Security and the Director of the Office of Personnel Management shall provide for the following:

"(A) NOTICE OF PROPOSAL, ETC.—The Secretary and the Director shall, with respect to any proposed system or adjustment—

"(i) provide to each employee representative representing any employees who might be affected, a written description of the proposed system or adjustment (including the reasons why it is considered necessary);

"(ii) give each representative at least 60 days (unless extraordinary circumstances require earlier action) to review and make recommendations with respect to the proposal; and

"(iii) give any recommendations received from any such representative under clause (ii) full and fair consideration in deciding whether or how to proceed with the proposal.

"(B) PRE-IMPLEMENTATION REQUIREMENTS.—If the Secretary and the Director decide to implement a proposal described in subparagraph (A), they shall before implementation—

"(i) give each employee representative details of the decision to implement the proposal, together with the information upon which the decision was based;

"(ii) give each representative an opportunity to make recommendations with respect to the proposal; and

"(iii) give such recommendations full and fair consideration, including the providing of reasons to an employee representative if any of its recommendations are rejected.

"(C) CONTINUING COLLABORATION.—If a proposal described in subparagraph (A) is implemented, the Secretary and the Director shall—

"(i) develop a method for each employee representative to participate in any further planning or development which might become necessary; and

"(ii) give each employee representative adequate access to information to make that participation productive.

"(2) PROCEDURES.—Any procedures necessary to carry out this subsection shall be established by the Secretary and the Director jointly. Such procedures shall include measures to ensure—

"(A) in the case of employees within a unit with respect to which a labor organization is accorded exclusive recognition, representation by individuals designated or from among individuals nominated by such organization;

"(B) in the case of any employees who are not within such a unit, representation by any appropriate organization which represents a substantial percentage of those employees or, if none, in such other manner as may be appropriate, consistent with the purposes of this subsection; and

"(C) the selection of representatives in a manner consistent with the relative numbers of employees represented by the organizations or other representatives involved.

"(f) PROVISIONS RELATING TO APPELLATE PROCEDURES.—

"(1) SENSE OF CONGRESS.—It is the sense of the Congress that—

"(A) employees of the Department of Homeland Security are entitled to fair treatment in any appeals that they bring in decisions relating to their employment; and

"(B) in prescribing regulations for any such appeals procedures, the Secretary of Homeland Security and the Director of the Office of Personnel Management—

"(i) should ensure that employees of the Department are afforded the protections of due process; and

"(ii) toward that end, should be required to consult with the Merit Systems Protection Board before issuing any such regulations.

"(2) REQUIREMENTS.—Any regulations under this section which relate to any matters within the purview of chapter 77—

"(A) shall be issued only after consultation with the Merit Systems Protection Board; and

"(B) shall ensure the availability of procedures which shall—

"(i) be consistent with requirements of due process; and

"(ii) provide, to the maximum extent practicable, for the expeditious handling of any matters involving the Department of Homeland Security.

---

20. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE WAXMAN OF CALIFORNIA, OR HIS DESIGNEE, DEBATABLE FOR 20 MINUTES

Strike section 761 and insert the following:

SEC. 761. HUMAN RESOURCES MANAGEMENT.

(a) AUTHORITY TO ADJUST PAY SCHEDULES.—

(1) IN GENERAL.—Notwithstanding any provision of title 5, United States Code, the Secretary may, under regulations prescribed jointly with the Director of the Office of Personnel Management, provide for such adjustments in rates of basic pay as may be necessary to address inequitable pay disparities among employees within the Department performing similar work in similar circumstances.

(2) APPLICABILITY.—No authority under paragraph (1) may be exercised with respect to any employee who serves in—

(A) an Executive Schedule position under subchapter II of chapter 53 of title 5, United States Code; or

(B) a position for which the rate of basic pay is fixed in statute by reference to a section or level under subchapter II of chapter 53 of such title 5.

(3) LIMITATIONS.—Nothing in this subsection shall constitute authority—

(A) to fix pay at a rate greater than the maximum amount of cash compensation allowable under section 5307 of title 5, United States Code, in a year; or

(B) to exempt any employee from the application of such section 5307.

(4) SUNSET PROVISION.—Effective 5 years after the effective date of this Act, all authority to issue regulations under this subsection (including regulations which would modify, supersede, or terminate any regulations previously issued under this subsection) shall cease to be available.

(b) SUSPENSION AND REMOVAL OF EMPLOYEES IN THE INTERESTS OF NATIONAL SECURITY.—The Secretary shall establish procedures consistent with section 7532 of title 5, United States Code, to provide for the suspension and removal of employees of the Department when necessary in the interests of national security or homeland security. Such regulations shall provide for written notice, hearings, and review similar to that provided by such section 7532.

(c) DEMONSTRATION PROJECT.—

(1) IN GENERAL.—Not later than 5 years after the effective date of this Act, the Secretary shall submit to Congress a proposal for a demonstration project, the purpose of which shall be to help attain a human resources management system which in the judgment of the Secretary is necessary in order to enable the Department best to carry out its mission.

(2) REQUIREMENTS.—The proposal shall—

(A) ensure that veterans' preference and whistleblower protection rights are retained;

(B) ensure that existing collective bargaining agreements and rights under chapter 71 of title 5, United States Code, remain unaffected;

(C) ensure the availability of such measures as may be necessary in order to allow the Department to recruit and retain the best persons possible to carry out its mission;

(D) include one or more performance appraisal systems which shall—

(i) provide for periodic appraisals of the performance of covered employees;

(ii) provide for meaningful participation of covered employees in the establishment of employee performance plans; and

(iii) use the results of performance appraisals as a basis for rewarding, reducing in grade, retaining, and removing covered employees; and

(E) contain recommendations for such legislation or other actions by Congress as the Secretary considers necessary.

(3) DEFINITION OF A COVERED EMPLOYEE.—For purposes of paragraph (2)(D), the term "covered employee" means a supervisor or management official (as defined in paragraphs (10) and (11) of section 7103(a) of title 5, United States Code, re-

spectively) who occupies a position within the Department which is in the General Schedule.

(d) MERIT SYSTEM PRINCIPLES.—All authorities under subsections (a) and (b) shall be exercised in a manner, and all personnel management flexibilities or authorities proposed under subsection (c) shall be, consistent with merit system principles under section 2301 of title 5, United States Code.

(e) REMEDIES FOR RETALIATION AGAINST WHISTLEBLOWERS.—Section 7211 of title 5, United States Code, is amended—

(1) by inserting "(a)" before "The right"; and

(2) by adding at the end the following:

"(b) Any employee aggrieved by a violation of subsection (a) may bring a civil action in the appropriate United States district court, within 3 years after the date on which such violation occurs, against any agency, organization, or other person responsible for the violation, for lost wages and benefits, reinstatement, costs and attorney fees, compensatory damages, and equitable, injunctive, or any other relief that the court considers appropriate. Any such action shall, upon request of the party bringing the action, be tried by the court with a jury.

"(c) The same legal burdens of proof in proceedings under subsection (b) shall apply as under sections 1214(b)(4)(B) and 1221(e) in the case of an alleged prohibited personnel practice described in section 2302(b)(8).

"(d) For purposes of this section, the term 'employee' means an employee (as defined by section 2105) and any individual performing services under a personal services contract with the Government (including as an employee of an organization).".

(f) NONREDUCTION IN PAY.—Nothing in this section shall, with respect to any employee who is transferred to the Department pursuant to this Act, constitute authority to reduce the rate of basic pay (including any comparability pay) payable to such employee below the rate last payable to such employee before the date on which such employee is so transferred.

In section 812(e)(1), strike "Act; and" and insert the following: "Act, except that the rules, procedures, terms, and conditions relating to employment in the Transportation Security Administration before the effective date of this Act may be applied only to the personnel employed by or carrying out the functions of the Transportation Security Administration.".

In section 812(e)(2), strike "except" and insert "Except".

---

21. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE ARMEY OF TEXAS, OR HIS DESIGNEE, DEBATABLE FOR 40 MINUTES

Page 13, line 20, strike "The Secretary" and insert "With respect to homeland security, the Secretary".

Page 22, line 13, strike "Under the direction of the Secretary, developing" and insert "Developing".

Page 24, lines 10 to 11, strike "and to other areas of responsibility described in section 101(b)".

Page 25, lines 9 to 10, strike "and to other areas of responsibility described in section 101(b)".

Page 24, line 12, strike "concerning infrastructure or other vulnerabilities" and insert "concerning infrastructure vulnerabilities or other vulnerabilities".

Page 25, lines 11 to 12, strike "concerning infrastructure or other vulnerabilities" and insert "concerning infrastructure vulnerabilities or other vulnerabilities".

Page 28, line 14, strike "(1) and (2)" and insert "(2) and (3)".

Page 19, line 16, strike "Director of Homeland Security" and insert "President".

Page 43, line 11, strike "the Congress" and insert "the appropriate congressional committees".

Page 142, line 2, insert "including" before "interventions".

Page 142, line 4, insert a comma after "asters".

In section 811(f)(1)—

(1) insert "or" before "Harbor"; and

(2) strike "or Oil Spill Liability Trust Fund".

In section 205(1), strike "information" the first place it appears.

In section 205(3) insert "and regulatory" after "legislative".

In section 302, strike paragraph (1) and redesignate the subsequent paragraphs in order as paragraphs (1) and (2).

In section 305(d), strike "section 302(2)(D)" and insert "302(1)(D)".

Strike section 906, and redesignate sections 907 through 913 as sections 906 through 912, respectively.

In section 301—

(1) in paragraph (8), strike "homeland security, including" and all that follows and insert "homeland security; and";

(2) strike paragraph (9); and

(3) redesignate paragraph (10) as paragraph (9).

In title III, add at the end the following section:

SEC. 309. TECHNOLOGY CLEARINGHOUSE TO ENCOURAGE AND SUPPORT INNOVATIVE SOLUTIONS TO ENHANCE HOMELAND SECURITY.

(a) ESTABLISHMENT OF PROGRAM.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish and promote a program to encourage technological innovation in facilitating the mission of the Department (as described in section 101).

(b) ELEMENTS OF PROGRAM.—The program described in subsection (a) shall include the following components:

(1) The establishment of a centralized Federal clearinghouse for information relating to technologies that would further the mission of the Department for dissemination, as appropriate, to Federal, State, and local government and private sector entities for additional review, purchase, or use.

(2) The issuance of announcements seeking unique and innovative technologies to advance the mission of the Department.

(3) The establishment of a technical assistance team to assist in screening, as appropriate, proposals submitted to the Secretary (except as provided in subsection (c)(2)) to assess the feasibility, scientific and technical merits, and estimated cost of such proposals, as appropriate.

(4) The provision of guidance, recommendations, and technical assistance, as appropriate, to assist Federal, State, and local government and private sector efforts to evaluate and im-

plement the use of technologies described in paragraph (1) or (2).

(5) The provision of information for persons seeking guidance on how to pursue proposals to develop or deploy technologies that would enhance homeland security, including information relating to Federal funding, regulation, or acquisition.

(c) MISCELLANEOUS PROVISIONS.—

(1) IN GENERAL.—Nothing in this section shall be construed as authorizing the Secretary or the technical assistance team established under subsection (b)(3) to set standards for technology to be used by the Department, any other executive agency, any State or local government entity, or any private sector entity.

(2) CERTAIN PROPOSALS.—The technical assistance team established under subsection (b)(3) shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

(3) COORDINATION.—In carrying out this section, the Secretary shall coordinate with the Technical Support Working Group (organized under the April 1982 National Security Decision Directive Numbered 30).

In title II, at the end of subtitle A add the following:

SEC. . ENHANCEMENT OF NON-FEDERAL CYBERSECURITY.

In carrying out the responsibilities under section 201, the Under Secretary for Information Analysis and Infrastructure Protection shall—

(1) as appropriate, provide to State and local government entities, and upon request to private entitites that own or operate critical information systems—

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; and

(2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems.

At the end of title II add the following:

SEC. . NET GUARD.

The Under Secretary for Information Analysis and Infrastructure Protection may establish a national technology guard, to be known as "NET Guard", comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

Strike section 814.

In section 761—

(1) in the proposed section 9701(b)(3)(D) strike "title" and insert "part"; and

(2) in the proposed section 9701(c), strike "title" and insert "part".

At the end of title VII, insert the following new section:

SEC. 774. SENSE OF CONGRESS REAFFIRMING THE CONTINUED IMPORTANCE AND APPLICABILITY OF THE POSSE COMITATUS ACT.

(a) FINDINGS.—The Congress finds the following:

(1) Section 1385 of title 18, United States Code (commonly known as the "Posse Comitatus Act"), prohibits the use of the Armed Forces as a posse comitatus to execute the laws except in cases and under circumstances expressly authorized by the Constitution or Act of Congress.

(2) Enacted in 1878, the Posse Comitatus Act was expressly intended to prevent United States Marshals, on their own initiative, from calling on the Army for assistance in enforcing Federal law.

(3) The Posse Comitatus Act has served the Nation well in limiting the use of the Armed Forces to enforce the law.

(4) Nevertheless, by its express terms, the Posse Comitatus Act is not a complete barrier to the use of the Armed Forces for a range of domestic purposes, including law enforcement functions, when the use of the Armed Forces is authorized by Act of Congress or the President determines that the use of the Armed Forces is required to fulfill the President's obligations under the Constitution to respond promptly in time of war, insurrection, or other serious emergency.

(5) Existing laws, including chapter 15 of title 10, United States Code (commonly known as the "Insurrection Act"), and the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.), grant the President broad powers that may be invoked in the event of domestic emergencies, including an attack against the Nation using weapons of mass destruction, and these laws specifically authorize the President to use the Armed Forces to help restore public order.

(b) SENSE OF CONGRESS.—The Congress reaffirms the continued importance of section 1385 of title 18, United States Code, and it is the sense of the Congress that nothing in this Act should be construed to alter the applicability of such section to any use of the Armed Forces as a posse comitatus to execute the laws.

Amend the heading for section 766 to read as follows:

SEC. 766. REGULATORY AUTHORITY AND PREEMPTION.

In section 766—

(1) before the first sentence insert the following: "(a) "REGULATORY AUTHORITY.—"; and

(2) at the end of the section add the following:

(b) PREEMPTION OF STATE OR LOCAL LAW.—Except as otherwise provided in this Act, this Act preempts no State or local law, except that any authority to preempt State or local law vested in any Federal agency or official transferred to the Department pursuant to this Act shall be transferred to the Department effective on the date of the transfer to the Department of that Federal agency or official.

Page 31, after line 5, insert the following:

SEC. 207. INFORMATION SECURITY.

In carrying out the responsibilities under section 201, the Under Secretary for Information Analysis and Infrastructure Protection shall—

(1) as appropriate, provide to State and local government entities, and, upon request, to private entities that own or operate critical information systems—

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; and

(2) as appropriate, provide technical assistance, upon request, to the private sector and with other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems.

At the end of the bill add the following new title:

TITLE XI—INFORMATION SECURITY

SEC. 1101. INFORMATION SECURITY.

(a) SHORT TITLE.—The amendments made by this title may be cited as the "Federal Information Security Management Act of 2002".

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, is amended to read as follows:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3531. Purposes

"The purposes of this subchapter are to—

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

"(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

"(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

"(4) provide a mechanism for improved oversight of Federal agency information security programs;

"(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation

that are designed, built, and operated by the private sector; and

"(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.".

"§ 3532. Definitions

"(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

"(b) ADDITIONAL DEFINITIONS.—As used in this subchapter—

"(1) the term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

"(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

"(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;

"(C) availability, which means ensuring timely and reliable access to and use of information; and

"(D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access;

"(2) the term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which—

"(A) involves intelligence activities;

"(B) involves cryptologic activities related to national security;

"(C) involves command and control of military forces;

"(D) involves equipment that is an integral part of a weapon or weapons system; or

"(E) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications);

"(3) the term 'information technology' has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

"(4) the term 'information system' means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes—

"(A) computers and computer networks;

"(B) ancillary equipment;

"(C) software, firmware, and related procedures;

"(D) services, including support services; and

"(E) related resources.".

"§ 3533. Authority and functions of the Director

"(a) The Director shall oversee agency information security policies and practices, by—

"(1) promulgating information security standards under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(2) overseeing the implementation of policies, principles, standards, and guidelines on information security;

"(3) requiring agencies, consistent with the standards promulgated under such section 5131 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

"(A) information collected or maintained by or on behalf of an agency; or

"(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

"(5) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) to enforce accountability for compliance with such requirements;

"(6) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3534(b);

"(7) coordinating information security policies and procedures with related information resources management policies and procedures; and

"(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

"(A) a summary of the findings of evaluations required by section 3535;

"(B) significant deficiencies in agency information security practices;

"(C) planned remedial action to address such deficiencies; and

"(D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(e)(7) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).".

"(b) Except for the authorities described in paragraphs (4) and (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

"§ 3534. Federal agency responsibilities

"(a) The head of each agency shall—

"(1) be responsible for—

"(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

"(i) information collected or maintained by or on behalf of the agency; and

"(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

"(i) information security standards promulgated by the Director under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441); and

"(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

"(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

"(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

"(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

"(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) for information security classifications and related requirements;

"(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

"(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

"(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

"(A) designating a senior agency information security officer who shall—

"(i) carry out the Chief Information Officer's responsibilities under this section;

"(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

"(iii) have information security duties as that official's primary duty; and

"(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

"(B) developing and maintaining an agencywide information security program as required by subsection (b);

"(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3533 of this title, and section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

"(E) assisting senior agency officials concerning their responsibilities under subparagraph (2);

"(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

"(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

"(b) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3533(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

"(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

"(2) policies and procedures that—

"(A) are based on the risk assessments required by subparagraph (1);

"(B) cost-effectively reduce information security risks to an acceptable level;

"(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

"(D) ensure compliance with—

"(i) the requirements of this subchapter;

"(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(iii) minimally acceptable system configuration requirements, as determined by the agency; and

"(iv) any other applicable requirements, including standards and guidelines for national security systems

issued in accordance with law and as directed by the President;

"(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

"(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

"(A) information security risks associated with their activities; and

"(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

"(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

"(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

"(B) may include testing relied on in a evaluation under section 3535;

"(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(7) procedures for detecting, reporting, and responding to security incidents, including—

"(A) mitigating risks associated with such incidents before substantial damage is done; and

"(B) notifying and consulting with, as appropriate—

"(i) law enforcement agencies and relevant Offices of Inspector General;

"(ii) an office designated by the President for any incident involving a national security system; and

"(iii) any other agency or office, in accordance with law or as directed by the President; and

"(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

"(c) Each agency shall—

"(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

"(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

"(A) annual agency budgets;

"(B) information resources management under subchapter 1 of this chapter;

"(C) information technology management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

"(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

"(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

"(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

"(G) internal accounting and administrative controls under section 3512 of title 31, United States Code, (known as the 'Federal Managers Financial Integrity Act'); and

"(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

"(A) as a material weakness in reporting under section 3512 of title 31, United States Code; and

"(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

"(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

"(A) the time periods, and

"(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

"(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

"(e) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

"§ 3535. Annual independent evaluation

"(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

"(2) Each evaluation by an agency under this section shall include—

"(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

"(B) an assessment (made on the basis of the results of the testing) of compliance with—

"(i) the requirements of this subchapter; and

"(ii) related information security policies, procedures, standards, and guidelines; and

"(C) separate presentations, as appropriate, regarding information security relating to national security systems.

"(b) Subject to subsection (c)—

"(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

"(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

"(c) For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

"(1) only by an entity designated by the agency head; and

"(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

"(d) The evaluation required by this section—

"(1) shall be performed in accordance with generally accepted government auditing standards; and

"(2) may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

"(e) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

"(f) Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

"(g)(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3533(a)(8).

"(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

"(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

"(h) The Comptroller General shall periodically evaluate and report to Congress on—

"(1) the adequacy and effectiveness of agency information security policies and practices; and

"(2) implementation of the requirements of this subchapter.

"§ 3536. National security systems

"The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

"(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

"(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

"(3) complies with the requirements of this subchapter.

"§ 3537. Authorization of appropriations

"There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

"§ 3538. Effect on existing law

"Nothing in this subchapter, section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441), or section 20 of the National Standards and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.".

(2) CLERICAL AMENDMENT.—The items in the table of sections at the beginning of such chapter 35 under the heading "SUBCHAPTER II" are amended to read as follows:

"3531. Purposes.
"3532. Definitions.
"3533. Authority and functions of the Director.
"3534. Federal agency responsibilities.
"3535. Annual independent evaluation.
"3536. National security systems.
"3537. Authorization of appropriations.
"3538. Effect on existing law.".

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3532(3) of title 44, United States Code.

(B) Section 2224 of title 10, United States Code, is amended—

(i) in subsection 2224(b), by striking "(b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1)" and inserting "(b) OBJECTIVES OF THE PROGRAM.—";

(ii) in subsection 2224(b), by striking "(2) the program shall at a minimum meet the requirements of section 3534 and 3535 of title 44, United States Code."; and

(iii) in subsection 2224(c), by inserting ", including through compliance with subtitle II of chapter 35 of title 44" after "infrastructure".

(2) ATOMIC ENERGY ACT OF 1954.—Nothing in this Act shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SEC. 1102. MANAGEMENT OF INFORMATION TECHNOLOGY.

Section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) is amended to read as follows:

"SEC. 5131. RESPONSIBILITIES FOR FEDERAL INFORMATION SYSTEMS STANDARDS.

"(a)(1)(A) Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

"(B) Standards promulgated under subparagraph (A) shall include—

"(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

"(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

"(C) Information security standards described under subparagraph (B) shall be compulsory and binding.

"(2) Standards and guidelines for national security systems, as defined under section 3532(3) of title 44, United States Code, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

"(b) The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards—

"(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

"(2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44, United States Code.

"(c)(1) The decision regarding the promulgation of any standard by the Director under subsection (a) shall occur not later than 6 months after the submission of the proposed standard to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

"(2) A decision by the Director to significantly modify, or not promulgate, a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), shall be made after the public is given an opportunity to comment on the Director's proposed decision.".

"(d) In this section, the term 'information security' has the meaning given that term in section 3532(b)(1) of title 44, United States Code.".

SEC. 1103. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), is amended by striking the text and inserting the following:

"(a) The Institute shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

"(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3532(b)(2) of title 44, United States Code);

"(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems; and

"(4) carry out the responsibilities described in paragraph (3) through the Computer Security Division.

"(b) The standards and guidelines required by subsection (a) shall include, at a minimum—

"(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

"(B) guidelines recommending the types of information and information systems to be included in each such category; and

"(C) minimum information security requirements for information and information systems in each such category;

"(2) a definition of and guidelines concerning detection and handling of information security incidents; and

"(3) guidelines developed in coordination with the National Security Agency for identifying an information system as a national security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

"(c) In developing standards and guidelines required by subsections (a) and (b), the Institute shall—

"(1) consult with other agencies and offices (including, but not limited to, the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security) to assure—

"(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

"(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

"(2) provide the public with an opportunity to comment on proposed standards and guidelines;

"(3) submit to the Director of the Office of Management and Budget for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441)—

"(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section; and

"(B) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section;

"(4) issue guidelines as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this Act;

"(5) ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions;

"(6) ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

"(7) use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products."

"(d) The Institute shall—

"(1) submit standards developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Director of the Office of Management and Budget for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(2) provide assistance to agencies regarding—

"(A) compliance with the standards and guidelines developed under subsection (a);

"(B) detecting and handling information security incidents; and

"(C) information security policies, procedures, and practices;

"(3) conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

"(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

"(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

"(6) evaluate security policies and practices developed for national security systems to assess potential application by agencies to strengthen information security;

"(7) periodically assess the effectiveness of standards and guidelines developed under this section and undertake revisions as appropriate;

"(8) solicit and consider the recommendations of the Information Security and Privacy Advisory Board, established by section 21, regarding standards and guidelines developed under subsection (a) and submit such recommendations to the Director of the Office of Management and Budget with such standards submitted to the Director; and

"(9) prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this section.

"(e) As used in this section—

"(1) the term 'agency' has the same meaning as provided in section 3502(1) of title 44, United States Code;

"(2) the term 'information security' has the same meaning as provided in section 3532(1) of such title;

"(3) the term 'information system' has the same meaning as provided in section 3502(8) of such title;

"(4) the term 'information technology' has the same meaning as provided in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

"(5) the term 'national security system' has the same meaning as provided in section 3532(b)(2) of such title.".

SEC. 1104. INFORMATION SECURITY AND PRIVACY ADVISORY BOARD.

Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4), is amended—

(1) in subsection (a), by striking "Computer System Security and Privacy Advisory Board" and inserting "Information Security and Privacy Advisory Board";

(2) in subsection (a)(1), by striking "computer or telecommunications" and inserting "information technology";

(3) in subsection (a)(2)—

(A) by striking "computer or telecommunications technology" and inserting "information technology"; and

(B) by striking "computer or telecommunications equipment" and inserting "information technology";

(4) in subsection (a)(3)—

(A) by striking "computer systems" and inserting "information system"; and

(B) by striking "computer systems security" and inserting "information security";

(5) in subsection (b)(1) by striking "computer systems security" and inserting "information security";

(6) in subsection (b) by striking paragraph (2) and inserting the following:

"(2) to advise the Institute and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including through review of proposed standards and guidelines developed under section 20; and";

(7) in subsection (b)(3) by inserting "annually" after "report";

(8) by inserting after subsection (e) the following new subsection:

"(f) The Board shall hold meetings at such locations and at such time and place as determined by a majority of the Board.";

(9) by redesignating subsections (f) and (g) as subsections (g) and (h), respectively; and

(10) by striking subsection (h), as redesignated by paragraph (9), and inserting the following:

"(h) As used in this section, the terms "information system" and "information technology" have the meanings given in section 20.".

SEC. 1105. TECHNICAL AND CONFORMING AMENDMENTS.

(a) COMPUTER SECURITY ACT.—Sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note) are repealed.

(b) FLOYD D. SPENCE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2001.—The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106–398) is amended by striking subtitle G of title X.

(c) PAPERWORK REDUCTION ACT.—(1) Section 3504(g) of title 44, United States Code, is amended—

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking "sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note)" and inserting "subchapter II of this title"; and

(ii) by striking the semicolon and inserting a period; and

(C) by striking paragraph (3).

(2) Section 3505 of such title is amended by adding at the end—

"(c)(1) The head of each agency shall develop and maintain an inventory of the information systems (including national security systems) operated by or under the control of such agency;

"(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency;

"(3) Such inventory shall be—

"(A) updated at least annually;

"(B) made available to the Comptroller General; and

"(C) used to support information resources management, including—

"(i) preparation and maintenance of the inventory of information resources under section 3506(b)(4);

"(ii) information technology planning, budgeting, acquisition, and management under section 3506(h), the Clinger-Cohen Act of 1996, and related laws and guidance;

"(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

"(iv) preparation of the index of major information systems required under section 552(g) of title 5, United States Code; and

"(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

"(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.".

(3) Section 3506(g) of such title is amended—

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking "the Computer Security Act of 1987 (40 U.S.C. 759 note)" and inserting "subchapter II of this title"; and

(ii) by striking the semicolon and inserting a period; and

(C) by striking paragraph (3).

SEC. 1106. CONSTRUCTION.

Nothing in this Act, or the amendments made by this Act, affects the authority of the National Institute of Standards and Technology or the Department of Commerce relating to the development and promulgation of standards or guidelines under paragraphs (1) and (2) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)).

In section 752(b)(1), strike "and extensive".

In section 752(b)(1), strike "and" and insert "or".

In section 752(b)(6), strike "evaluation" and insert "Evaluation".

At the end of section 752(b), insert:

(7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism.

In section 753(d)(1), insert "or other" after "liability".

In section 753(d)(3), strike "those products" and insert "anti-terrorism technology".

In section 753(d)(3), strike "product" and insert "anti-terrorism technology".

In section 754(a)(1), strike, "to non-federal" and insert "to Federal and non-Federal".

In section 754(a)(1), insert "and certified by the Secretary" after "section".

In section 755(1), strike "device, or technology designed, developed, or modified" and insert "equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured".

Page 182, line 2, strike "and" and insert "or".

At the end of subtitle G of title VII of the bill, add the following (and conform the table of contents of the bill accordingly):

SEC. 774. AIR TRANSPORTATION SAFETY AND SYSTEM STABILIZATION ACT AMENDMENTS.

The Air Transportation Safety and System Stabilization Act (49 U.S.C. 40101 note) is amended—

(1) in section 408 by striking the last sentence of subsection (c); and

(2) in section 402 by striking paragraph (1) and inserting the following:

"(1) AIR CARRIER.—The term 'air carrier' means a citizen of the United States undertaking by any means, directly or indirectly, to provide air transportation and includes employees and agents (including persons engaged in the business of providing air transportation security and their affiliates) of such citizen. For purposes of the preceding sentence, the term 'agent', as applied to persons engaged in the business of providing air transportation security, shall only include persons that have contracted directly with the Federal Aviation Administration on or after February 17, 2002, to provide such security, or are not debarred.".

Page 12, line 5, strike "and".

Page 12, line 9, strike the period and insert "; and".

Page 12, after line 9, insert the following:

(G) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

Page 195, line 16, after "terrorism." insert: "Such official shall—

(1) ensure the adequacy of resources within the Department for illicit drug interdiction; and

(2) serve as the United States Interdiction Coordinator for the Director of National Drug Control Policy.".

In section 307(b)(1)—

(1) strike "and" at the end of subparagraph (A);

(2) redesignate subparagraph (B) as subparagraph (C); and

(3) after subparagraph (A), insert the following new subparagraph:

(B) ensure that the research funded is of high quality, as determined through merit review processes developed under section 301(10); and

In section 766 of the bill, insert "sections 305(c) and 752(c) of" after "provided in".

Add at the end of title V of the bill the following section:

SEC. 506. SENSE OF CONGRESS REGARDING FUNDING OF TRAUMA SYSTEMS.

It is the sense of the Congress that States should give particular emphasis to developing and implementing the trauma care and burn center care components of the State plans for the provision of emergency medical services using funds authorized through Public Law 107–188 for grants to improve State, local, and hospital preparedness for and response to bioterrorism and other public health emergencies.

---

22. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE TURNER OF TEXAS, OR HIS DESIGNEE, DEBATABLE FOR 40 MINUTES

Strike subtitle F of title VII and insert the following:

Subtitle F—Risk Sharing and Indemnification

SEC. 751. RISK SHARING AND INDEMNIFICATION.

(a) DEFINITIONS.—Section 4 of the Office of Federal Procurement Policy Act (41 U.S.C. 403) is amended by adding at the end the following new paragraphs:

"(16) The term 'anti-terrorism technology and services' means any product, equipment, service or device, including information technology, system integration and any other kind of services (including support services) related to technology, designed, developed, modified or procured for the purpose of preventing, detecting, identifying, or otherwise deterring acts of terrorism.

"(17) The term 'act of terrorism,' means the calculated attack or threat of attack against persons, property or infrastructure to inculcate fear, intimidate or coerce a government, the civilian population, or any segment thereof, in the pursuit of political, religious or ideological grounds.

"(18) The term 'insurance carrier' means any corporation, association, society, order, firm, company, mutual, partnership, individual, aggregation of individuals, or any other legal entity that provides commercial property and casualty insurance. Such term includes any affiliates of a commercial insurance carrier.

"(19) The term 'liability insurance' means insurance for legal liabilities incurred by the insured resulting from—

"(A) loss of or damage to property of others;

"(B) ensuing loss of income or extra expense incurred because of loss of or damage to property of others;

"(C) bodily injury (including death) to persons other than the insured or its employees; or

"(D) loss resulting from debt or default of another.

"(20) The term 'homeland security procurement' means any procurement of anti-terrorism technology and services, as determined by the head of the agency, procured for the purpose of preventing, detecting, or otherwise deterring acts of terrorism.

"(21) The term 'information technology'—

"(A) means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information;

"(B) includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources; and

"(C) does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.".

(b) FEDERAL RISK SHARING AND INDEMNIFICATION.—The Office of Federal Procurement Policy Act is further amended by adding at the end the following new sections:

"SEC. 40. FEDERAL RISK SHARING AND INDEMNIFICATION.

"(a) When conducting a homeland security procurement the head of an agency may include in a contract an indemnification provision specified in subsection (e) if the head of the agency determines in writing that it is in the best interest of the Government to do so and determines that—

"(1) the anti-terrorism technology and services are needed to protect critical infrastructure services or facilities;

"(2) the anti-terrorism technology and services would be effective in facilitating the defense against acts of terrorism; and

"(3) the supplier of the anti-terrorism technology is unable to secure insurance coverage adequate to make the anti-terrorism technology and services available to the Government.

"(b) The head of the agency may exercise the authority in this section only if authorized by the Director of the Office of Management and Budget to do so.

"(c) In order to be eligible for an indemnification provision specified in this section, any entity that provides anti-terrorism technology and services to an agency identified in this Act shall obtain liability insurance of such types and in such amounts, to the maximum extent practicable as determined by the agency, to satisfy otherwise compensable third party claims resulting from an act of terrorism when anti-terrorism technologies and services have been deployed in defense against acts of terrorism.

"(d) An indemnification provision included in a contract under the authority of this section shall be without regard to other provisions of law relating to the making, performance, amendment or modification of contracts.

"(e)(1) The indemnification provision to be included in a contract under the authority of this section shall indemnify, in whole or in part, the contractor for liability, including reasonable expenses of litigation and settlement, that is not covered by the insurance required under subsection (c), for:

"(A) Claims by third persons, including employees of the contractor, for death, personal injury, or loss of, damage to, or loss of use of property, or economic losses resulting from an act of terrorism;

"(B) Loss of, damage to, or loss of use of property of the Government; and

"(C) Claims arising (i) from indemnification agreements between the contractor and a subcontractor or subcontractors, or (ii) from such arrangements and further indemnification arrangements between subcontractors at any tier, provided that all such arrangements were entered into pursuant to the terms of this section.

"(2) Liabilities arising out of the contractor's willful misconduct or lack of good faith shall not be entitled to indemnification under the authority of this section.

"(f) An indemnification provision included in a contract under the authority of this section shall be negotiated and signed by the agency contracting officer and an authorized representative of the contractor and approved by the head of the agency prior to the commencement of performance of the contract.

"(g) The authority conferred by this section shall be limited to the following agencies:

"(1) The Department of Homeland Security;
"(2) The Department of Agriculture;
"(3) The Department of Commerce;
"(4) The Department of Defense;
"(5) The Department of Energy;
"(6) The Department of Health and Human Services;
"(7) The Department of the Interior;
"(8) The Department of Justice;
"(9) The Department of State;
"(10) The Department of the Treasury;
"(11) The Department of Transportation;
"(12) The Federal Emergency Management Agency;
"(13) The Federal Reserve System;
"(14) The General Services Administration;
"(15) The National Aeronautics and Space Administration;
"(16) The Tennessee Valley Authority;
"(17) The U.S. Postal Service;
"(18) The Central Intelligence Agency;
"(19) The Architect of the Capitol; and
"(20) Any other agency designated by the Secretary of Homeland Security that engages in homeland security contracting activities.

"(h) If any suit or action is filed or any claim is made against the contractor for any losses to third parties arising out of an act of terrorism when its anti-terrorism technologies and services have been deployed such that the cost and expense of the losses may be indemnified by the United States under this section, the contractor shall—

"(1) immediately notify the Secretary and promptly furnish copies of all pertinent papers received;

"(2) authorize United States Government representatives to collaborate with counsel for the contractor's insurance carrier in settling or defending the claim when the amount of the liability claimed may exceed the amount of insurance coverage; and

"(3) authorize United States Government representatives to settle or defend the claim and to represent the contractor in or to take charge of any litigation, if required by the United States Government, when the liability is not insured.

The contractor may, at its own expense, be associated with the United States Government representatives in any such claim or litigation.".

(c) STATE AND LOCAL RISK SHARING AND INDEMNIFICATION.—(1) The Secretary may, upon the application of a State or local government, provide for indemnification of contractors who provide anti-terrorism technologies and services to State or local governments if the Secretary determines in writing that—

(A) it is in the best interest of the Government to do so;

(B) the State or local government is unable to provide the required indemnification; and

(C) the anti-terrorism technology and services are needed to protect critical infrastructure services or facilities, would be effective in facilitating the defense against acts of terrorism, and would not be reasonably available absent indemnification.

(2) The Secretary may exercise the authority in this subsection only if authorized by the Director of the Office of Management and Budget to do so.

(3) In order to be eligible for indemnification, any entity that provides anti-terrorism technology and services to a State or local government shall obtain liability insurance of such types and in such amounts to the maximum extent practicable, as determined by the Secretary, to satisfy otherwise compensable third party claims resulting from an act of terrorism when anti-terrorism technologies and services have been deployed in defense against acts of terrorism.

(4) The indemnification provided under the authority of this subsection shall indemnify, in whole or in part, the contractor for liability, including reasonable expenses of litigation and settlement, that is not covered by the insurance required under paragraph (3) for—

(A) claims by third persons, including employees of the contractor, for death, personal injury, or loss of, damage to, or loss of use of property, or economic losses resulting from an act of terrorism;

(B) loss of, damage to, or loss of use of property of the Government; and

(C) claims arising—

(i) from indemnification agreements between the contractor and a subcontractor or subcontractors; or

(ii) from such arrangements and further indemnification arrangements between subcontractors at any tier, provided that all such arrangements were entered into pursuant to the terms of this subsection.

Liabilities arising out of the contractor's willful misconduct or lack of good faith shall not be entitled to indemnification under the authority of this subsection.

(5) If any suit or action is filed or any claim is made against the contractor for any losses to third parties arising out of an act of terrorism when its anti-terrorism technologies and services have been deployed such that the cost and expense of the losses may be indemnified by the United States under this subsection, the contractor shall—

(A) immediately notify the Secretary and promptly furnish copies of all pertinent papers received;

(B) authorize United States Government representatives to collaborate with counsel for the contractor's insurance carrier in settling or defending the claim when the amount of the liability claimed may exceed the amount of insurance coverage; and

(C) authorize United States Government representatives to settle or defend the claim and to represent the contractor in or to take charge of any litigation, if required by the United States Government, when the liability is not insured.

The contractor may, at its own expense, be associated with the United States Government representatives in any such claim or litigation.

(6) In this subsection, the definitions in paragraphs (16) through (21) of section 4 of the Office of Federal Procurement Policy Act shall apply.

(c) IMPLEMENTING REGULATIONS.—Not later than 120 days after the date of the enactment of this Act, the Federal Acquisition Regulation shall be amended to ensure consistency between the Federal Acquisition Regulation and this section.

---

23. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE OBERSTAR OF MINNESOTA, OR HIS DESIGNEE, DEBATABLE FOR 45 MINUTES

Strike section 409 of the bill.
Redesignate section 410 of the bill as section 409.
Conform the table of contents of the bill accordingly.

---

24. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE SCHAKOWSKY OF ILLINOIS, OR HER DESIGNEE, DEBATABLE FOR 30 MINUTES

Strike subtitle C of title VII.
Strike section 762 and insert the following:

SEC. 762. REMEDIES FOR RETALIATION AGAINST WHISTLEBLOWERS.

Section 7211 of title 5, United States Code, is amended—

(1) by inserting "(a)" before "The right"; and

(2) by adding at the end the following:

"(b) Any employee aggrieved by a violation of subsection (a) may bring a civil action in the appropriate United States district court, within 3 years after the date on which such violation occurs, against any agency, organization, or other person responsible for the violation, for lost wages and benefits, reinstatement, costs and attorney fees, compensatory damages, and equitable, injunctive, or any other relief that the court considers appropriate. Any such action shall, upon request of the party bringing the action, be tried by the court with a jury.

"(c) The same legal burdens of proof in proceedings under subsection (b) shall apply as under sections 1214(b)(4)(B) and 1221(e) in the case of an alleged prohibited personnel practice described in section 2302(b)(8).

"(d) For purposes of this section, the term 'employee' means an employee (as defined by section 2105) and any individual performing services under a personal services contract with the Government (including as an employee of an organization).".

---

25. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE DAVIS OF VIRGINIA, OR HER DESIGNEE, DEBATABLE FOR 20 MINUTES

Strike paragraph (2) of section 772, and insert the following:

(2) COVERED FEDERAL AGENCY.—The term "covered Federal agency" means the Department of Homeland Security and any agency designated by the Department or with which the Department shares critical infrastructure information.

---

26. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE CHAMBLISS OF GEORGIA, OR HIS DESIGNEE, DEBATABLE FOR 20 MINUTES

At the end of title VII add the following new subtitle:

Subtitle H—Information Sharing

SEC. 780. SHORT TITLE.

This subtitle may be cited as the "Homeland Security Information Sharing Act".

SEC. 781. FINDINGS AND SENSE OF CONGRESS.

(a) FINDINGS.—The Congress finds the following:

(1) The Federal Government is required by the Constitution to provide for the common defense, which includes terrorist attack.

(2) The Federal Government relies on State and local personnel to protect against terrorist attack.

(3) The Federal Government collects, creates, manages, and protects classified and sensitive but unclassified information to enhance homeland security.

(4) Some homeland security information is needed by the State and local personnel to prevent and prepare for terrorist attack.

(5) The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information.

(6) Granting security clearances to certain State and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats among Federal, State, and local levels of government.

(7) Methods exist to declassify, redact, or otherwise adapt classified information so it may be shared with State and local personnel without the need for granting additional security clearances.

(8) State and local personnel have capabilities and opportunities to gather information on suspicious activities and terrorist threats not possessed by Federal agencies.

(9) The Federal Government and State and local governments and agencies in other jurisdictions may benefit from such information.

(10) Federal, State, and local governments and intelligence, law enforcement, and other emergency preparation and response agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks.

(11) Information systems, including the National Law Enforcement Telecommunications System and the Terrorist Threat Warning System, have been established for rapid sharing of classified and sensitive but unclassified information among Federal, State, and local entities.

(12) Increased efforts to share homeland security information should avoid duplicating existing information systems.

(b) SENSE OF CONGRESS.—It is the sense of Congress that Federal, State, and local entities should share homeland security information to the maximum extent practicable, with special emphasis on hard-to-reach urban and rural communities.

SEC. 782. FACILITATING HOMELAND SECURITY INFORMATION SHARING PROCEDURES.

(a) PROCEDURES FOR DETERMINING EXTENT OF SHARING OF HOMELAND SECURITY INFORMATION.—

(1) The President shall prescribe and implement procedures under which relevant Federal agencies—

(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;

(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) Such procedures shall not change the requirements and authorities to protect sources and methods.

(b) PROCEDURES FOR SHARING OF HOMELAND SECURITY INFORMATION.—

(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information.

(2) Each information sharing system through which information is shared under paragraph (1) shall—

(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;

(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—

(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of such information;

(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.

(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.

(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems—

(A) to access information shared with such personnel; and

(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.

(c) SHARING OF CLASSIFIED INFORMATION AND SENSITIVE BUT UNCLASSIFIED INFORMATION WITH STATE AND LOCAL PERSONNEL.—

(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (a).

(2) It is the sense of Congress that such procedures may include one or more of the following means:

(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.

(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.

(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.

(d) RESPONSIBLE OFFICIALS.—For each affected Federal agency, the head of such agency shall designate an official to administer this Act with respect to such agency.

(e) FEDERAL CONTROL OF INFORMATION.—Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.

(f) DEFINITIONS.—As used in this section:

(1) The term "homeland security information" means any information possessed by a Federal, State, or local agency that—

(A) relates to the threat of terrorist activity;

(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;

(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or

(D) would improve the response to a terrorist act.

(2) The term "intelligence community" has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(3) The term "State and local personnel" means any of the following persons involved in prevention, preparation, or response for terrorist attack:

(A) State Governors, mayors, and other locally elected officials.

(B) State and local law enforcement personnel and firefighters.

(C) Public health and medical professionals.

(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.

(E) Other appropriate emergency response agency personnel.

(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal government in procedures developed pursuant to this section.

(4) The term "State" includes the District of Columbia and any commonwealth, territory, or possession of the United States.

(g) CONSTRUCTION.—Nothing in this Act shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this Act to receive homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.

SEC. 783. REPORT.

(a) REPORT REQUIRED.—Not later than 12 months after the date of the enactment of this Act, the President shall submit to the congressional committees specified in subsection (b) a report on the implementation of section 782. The report shall include any recommendations for additional measures or appropriation requests, beyond the requirements of section 782, to increase the effectiveness of sharing of information between and among Federal, State, and local entities.

(b) SPECIFIED CONGRESSIONAL COMMITTEES.—The congressional committees referred to in subsection (a) are the following committees:

(1) The Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.

(2) The Select Committee on Intelligence and the Committee on the Judiciary of the Senate.

SEC. 784. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to carry out section 782.

SEC. 785. AUTHORITY TO SHARE GRAND JURY INFORMATION.

Rule 6(e) of the Federal Rules of Criminal Procedure is amended—

(1) in paragraph (2), by inserting ", or of guidelines jointly issued by the Attorney General and Director of Central Intelligence pursuant to Rule 6," after "Rule 6"; and

(2) in paragraph (3)—

(A) in subparagraph (A)(ii), by inserting "or of a foreign government" after "(including personnel of a state or subdivision of a state";

(B) in subparagraph (C)(i)—

(i) in subclause (I), by inserting before the semicolon the following: "or, upon a request by an attorney for the government, when sought by a foreign court or prosecutor for use in an official criminal investigation";

(ii) in subclause (IV)—

(I) by inserting "or foreign" after "may disclose a violation of State";

(II) by inserting "or of a foreign government" after "to an appropriate official of a State or subdivision of a State"; and

(III) by striking "or" at the end;

(iii) by striking the period at the end of subclause (V) and inserting "; or"; and

(iv) by adding at the end the following:

"(VI) when matters involve a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, to any appropriate federal, state, local, or foreign government official for the purpose of preventing or responding to such a threat."; and

(C) in subparagraph (C)(iii)—

(i) by striking "Federal";

(ii) by inserting "or clause (i)(VI)" after "clause (i)(V)"; and

(iii) by adding at the end the following: "Any state, local, or foreign official who receives information pursuant to clause (i)(VI) shall use that information only

consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.".

SEC. 786. AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION.

Section 2517 of title 18, United States Code, is amended by adding at the end the following:

"(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

"(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the At-

---

27. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE WELDON OF FLORIDA, OR HIS DESIGNEE, DEBATABLE FOR 20 MINUTES

At the end of section 402 (relating to functions transferred) insert the following:

(9) The Visa Office of the Bureau of Consular Affairs of the Department of State, including the functions of the Secretary of State, relating thereto.

In section 403 (relating to visa issuance) strike subsections (a) through (f) and insert the following (and redesignate subsection (g) as subsection (i)):

(a) AUTHORITY.—Notwithstanding the provisions of section 104 of the Immigration and Nationality Act (8 U.S.C. 1104) or any other law, the Secretary shall have exclusive authority to issue regulations with respect to, administer, and enforce the provisions of that

Act and all other immigration and nationality laws relating to the granting or refusal of visas.

(b) TRANSITION.—

(1) IN GENERAL; DETAILS.—During the 2-year period beginning on the effective date of this Act, there shall be a transition period. During this period consular officers (as defined in section 101(a)(9) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(9))) of the Department of State and other foreign service officers in the Visa Office, to the extent they are involved in the granting or refusal of visas or any other documents required for entry into the United States, shall be detailed to the Department of Homeland Security. A detail under this subsection may be terminated at any time by the Secretary.

(2) MAINTENANCE OF ROTATION PROGRAM.—During the transition period described in paragraph (1), the Secretary of State shall maintain and administer the current rotation program (at least at the employment level in existence on the date of enactment of this Act) under which foreign service officers are assigned functions involved in the adjudication, review, or processing of visa applications.

(3) TERMINATION OF TRANSITION PERIOD.—The transition period may be terminated within the 2-year period described in paragraph (1) by the Secretary after consultation with the Secretary of State.

(4) EXISTING EMPLOYEES OF VISA OFFICE.—Employees of the Visa Office who are not foreign service officers shall become employees of the Department of Homeland Security immediately upon the effective date of the transfer of the Visa Office to the Department under this title.

(c) TRAINING.—

(1) TRAINING PROGRAM.—The Secretary shall provide for the training of Department personnel involved in the adjudication, review, or processing of visa applications, specifically addressing the language skills, interview techniques, fraud detection techniques, and other skills to be used by such personnel.

(2) STUDY REGARDING USE OF FOREIGN NATIONALS.—During the transition period, the Secretary shall study the role of foreign nationals in the review and processing of visa applications, specifically addressing the following:

(A) The proper role, if any, of foreign nationals in such processing.

(B) Any security concerns involving the employment of foreign nationals.

(C) Whether there are cost-effective alternatives to the employment of foreign nationals.

(3) REPORT.—Not later than 2 years after the date of the enactment of this Act, the Secretary shall submit a report on the findings of the study under paragraph (2) to the Committee on Government Reform, Committee on the Judiciary, and Committee on International Relations of the House of Representatives and the Committee on Governmental Affairs, Committee on the Judiciary, and Committee on Foreign Relations of the Senate.

(d) LEGAL EFFECT.—

(1) IN GENERAL.—The transfer of authority to the Secretary in section 403(a) shall not be construed to modify—

(A) any ground for such refusal authorized by law (including grounds under sections 212 and 221(g) of such Act (8 U.S.C. 1182 and 1201(g)));

(B) the presumption of immigrant status established under section 214(b) of such Act (8 U.S.C. 1184(b)) or the effect of failure to establish eligibility for nonimmigrant status described in such section; or

(C) the burden of proof placed upon persons making application for a visa or any other document required for entry under section 291 of such Act (8 U.S.C. 1361) or the effect of failure to establish eligibility for such visa or other document described in such section.

(2) NONREVIEWABILITY.—No court shall have jurisdiction to review the granting or refusal of a visa by the Secretary or a designee of the Secretary.

(e) REFUSAL OF VISAS AT REQUEST OF SECRETARY OF STATE.—Upon request by the Secretary of State, the Secretary of Homeland Security shall refuse to issue a visa to an alien if the Secretary of State determines that such refusal is necessary or advisable in the interests of the United States.

(f) REVIEW OF PASSPORTS ISSUED TO AMERICANS OVERSEAS.—The Secretary shall have the authority to review requests for passports by citizens of the United States living or traveling overseas.

(g) CONFORMING AMENDMENTS.—Section 104 of the Immigration and Nationality Act (8 U.S.C. 1104) is amended as follows:

(1) In subsection (a), by striking "conferred upon consular officers" and inserting "conferred upon the Secretary of Homeland Security".

(2) In subsection (c)—

(A) in the first sentence, by striking ", a Visa Office,"; and

(B) in the second sentence, by striking "Directors of the Passport Office and the Visa Office" and inserting "Director of the Passport Office, and the head of the office of the Department of Homeland Security that administers the provisions of this Act and other immigration and nationality laws relating to the granting or refusal of visas,".

(3) By striking subsection (e).

○