

COMMITTEE PRINT OF THE COMMITTEE ON ENERGY AND COMMERCE

(Showing the amendment to H.R. 1817, as reported by the
Committee on Homeland Security)

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Department of Home-
3 land Security Authorization Act for Fiscal Year 2006”.

4 **SEC. 2. TABLE OF CONTENTS.**

5 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Table of contents.

TITLE I—AUTHORIZATION OF APPROPRIATIONS

- Sec. 101. Department of Homeland Security.
- Sec. 102. Border patrol agents.
- Sec. 103. Departmental management and operations.
- Sec. 104. Critical infrastructure grants.
- Sec. 105. Research and development.
- Sec. 106. Border and transportation security.
- Sec. 107. State and local terrorism preparedness.
- Sec. 108. Authorization of appropriations for training of State and local personnel in border States performing immigration functions.

TITLE II—TERRORISM PREVENTION, INFORMATION SHARING,
AND RISK ASSESSMENT

Subtitle A—Terrorism Prevention

- Sec. 201. Terrorism Prevention Plan and related budget submission.
- Sec. 202. Consolidated background check process.

Subtitle B—Homeland Security Information Sharing and Analysis
Enhancement

- Sec. 211. Short title.
- Sec. 212. Provision of terrorism-related information to private sector officials.
- Sec. 213. Analytic expertise on the threats from biological agents and nuclear weapons.
- Sec. 214. Alternative analysis of homeland security information.
- Sec. 215. Assignment of information analysis and infrastructure protection functions.
- Sec. 216. Authority for disseminating homeland security information.
- Sec. 217. 9/11 Memorial Homeland Security Fellows Program.
- Sec. 218. Access to nuclear terrorism-related information.



- Sec. 219. Access of Assistant Secretary for Information Analysis to terrorism information.
- Sec. 220. Administration of the Homeland Security Information Network.
- Sec. 221. IAIP personnel recruitment.
- Sec. 222. Information collection requirements and priorities.
- Sec. 223. Homeland Security Advisory System.
- Sec. 224. Use of open-source information.
- Sec. 225. Full and efficient use of open-source information.

TITLE III—DOMESTIC PREPAREDNESS AND PROTECTION

Subtitle A—Preparedness and Protection

- Sec. 301. National terrorism exercise program.
- Sec. 302. Technology development and transfer.
- Sec. 303. Review of antiterrorism acquisitions.
- Sec. 304. Center of Excellence for Border Security.
- Sec. 305. Requirements relating to the Container Security Initiative (CSI).
- Sec. 306. Security of maritime cargo containers.
- Sec. 307. Security plan for general aviation at Ronald Reagan Washington National Airport.
- Sec. 308. Interoperable communications assistance.
- Sec. 309. Report to Congress on implementation of recommendations regarding protection of agriculture.

Subtitle B—Department of Homeland Security Cybersecurity Enhancement

- Sec. 311. Short title.
- Sec. 312. Assistant Secretary for Cybersecurity.
- Sec. 313. Cybersecurity defined.
- Sec. 314. Cybersecurity training programs and equipment.
- Sec. 315. Information security requirements and OMB responsibilities not affected.

Subtitle C—Security of public transportation systems

- Sec. 321. Security best practices.
- Sec. 322. Public awareness.

Subtitle D—Critical infrastructure prioritization

- Sec. 331. Critical infrastructure.
- Sec. 332. Security review.
- Sec. 333. Implementation report.
- Sec. 334. Protection of information.

TITLE IV—MISCELLANEOUS

- Sec. 401. Border security and enforcement coordination and operations.
- Sec. 402. GAO report to Congress.
- Sec. 403. Plan for establishing consolidated and colocated regional offices.
- Sec. 404. Plan to reduce wait times.
- Sec. 405. Denial of transportation security card.
- Sec. 406. Transfer of existing Customs Patrol Officers unit and establishment of new CPO units in the Bureau of Immigration and Customs Enforcement.



1 **TITLE I—AUTHORIZATION OF**
2 **APPROPRIATIONS**

3 **SEC. 101. DEPARTMENT OF HOMELAND SECURITY.**

4 There is authorized to be appropriated to the Sec-
5 retary of Homeland Security for the necessary expenses
6 of the Department of Homeland Security for fiscal year
7 2006, \$34,152,143,000.

8 **SEC. 102. BORDER PATROL AGENTS.**

9 Of the amount authorized under section 101, there
10 is authorized to be appropriated for fiscal year 2006 for
11 border security and control between ports of entry, includ-
12 ing for the hiring of 2,000 border patrol agents in addition
13 to the number employed on the date of enactment of this
14 Act, and related training and support costs,
15 \$1,916,427,000.

16 **SEC. 103. DEPARTMENTAL MANAGEMENT AND OPER-**
17 **ATIONS.**

18 Of the amount authorized under section 101, there
19 is authorized to be appropriated for fiscal year 2006 for
20 departmental management and operations, \$634,687,000,
21 of which—

22 (1) \$44,895,000 is authorized for the Depart-
23 ment of Homeland Security Regions Initiative;

24 (2) \$4,459,000 is authorized for Operation In-
25 tegration Staff; and



1 (3) \$56,278,000 is authorized for Office of Se-
2 curity initiatives.

3 **SEC. 104. CRITICAL INFRASTRUCTURE GRANTS.**

4 Of the amount authorized under section 101, there
5 is authorized to be appropriated for fiscal year 2006 for
6 grants and other assistance to improve critical infrastruc-
7 ture protection, \$500,000,000.

8 **SEC. 105. RESEARCH AND DEVELOPMENT.**

9 Of the amount authorized under section 101, there
10 are authorized to be appropriated for fiscal year 2006—

11 (1) \$76,573,000 to support chemical counter-
12 measure development activities of the Directorate of
13 Science and Technology;

14 (2) \$197,314,000 to support a nuclear detec-
15 tion office and related activities of such directorate;

16 (3) \$10,000,000 for research and development
17 of technologies capable of countering threats posed
18 by man-portable air defense systems, including loca-
19 tion-based technologies and noncommercial aircraft-
20 based technologies; and

21 (4) \$10,600,000 for the activities of such direc-
22 torate conducted pursuant to subtitle G of title VIII
23 of the Homeland Security Act of 2002 (6 U.S.C.
24 441 et seq.).



1 **SEC. 106. BORDER AND TRANSPORTATION SECURITY.**

2 Of the amount authorized under section 101, there
3 are authorized to be appropriated for fiscal year 2006—

4 (1) \$826,913,000 for expenses related to
5 Screening Coordination and Operations of the Direc-
6 torate of Border and Transportation Security;

7 (2) \$100,000,000 for weapons of mass destruc-
8 tion detection technology of such directorate; and

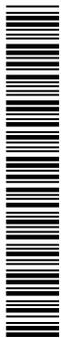
9 (3) \$133,800,000 for the Container Security
10 Initiative of such directorate.

11 **SEC. 107. STATE AND LOCAL TERRORISM PREPAREDNESS.**

12 Of the amount authorized under section 101, there
13 is authorized to be appropriated for fiscal year 2006—

14 (1) \$40,500,000 for the activities of the Office
15 for Interoperability and Compatibility within the Di-
16 rectorate of Science and Technology pursuant to sec-
17 tion 7303 of the Intelligence Reform and Terrorism
18 Prevention Act of 2004 (6 U.S.C 194); and

19 (2) \$1,000,000,000 for discretionary grants for
20 high-threat, high-density urban areas awarded by
21 the Office of State and Local Government Coordina-
22 tion and Preparedness.



1 **SEC. 108. AUTHORIZATION OF APPROPRIATIONS FOR**
2 **TRAINING OF STATE AND LOCAL PERSONNEL**
3 **IN BORDER STATES PERFORMING IMMIGRA-**
4 **TION FUNCTIONS.**

5 (a) **IN GENERAL.**—To carry out subsection (b), sub-
6 ject to such limitations as may be provided in Acts making
7 appropriations for Management and Administration for
8 U.S. Immigration and Customs Enforcement, there are
9 authorized to be appropriated from such amounts
10 \$40,000,000 for fiscal year 2006, to remain available until
11 September 30, 2007, for the purpose of enhancing the in-
12 tegrity of the border security system of the United States
13 against the threat of terrorism.

14 (b) **USE OF FUNDS.**—From amounts made available
15 under subsection (a), the Secretary of Homeland Security
16 may reimburse a State or political subdivision described
17 in subsection (c) for the expenses described in subsection
18 (d).

19 (c) **ELIGIBLE RECIPIENTS.**—A State, or a political
20 subdivision of a State, is eligible for reimbursement under
21 subsection (b) if the State or political subdivision—

22 (1) contains a location that is 30 miles or less
23 from a border or coastline of the United States;

24 (2) has entered into a written agreement de-
25 scribed in section 287(g) of the Immigration and
26 Nationality Act (8 U.S.C. 1357(g)) under which cer-



1 tain officers or employees of the State or subdivision
2 may be authorized to perform certain functions of
3 an immigration officer; and

4 (3) desires such officers or employees to receive
5 training from the Department of Homeland Security
6 in relation to such functions.

7 (d) EXPENSES.—The expenses described in this sub-
8 section are actual and necessary expenses incurred by the
9 State or political subdivision in order to permit the train-
10 ing described in subsection (c)(3) to take place, including
11 expenses such as the following:

12 (1) Costs of travel and transportation to loca-
13 tions where training is provided, including mileage
14 and related allowances for the use of a privately
15 owned automobile.

16 (2) Subsistence consisting of lodging, meals,
17 and other necessary expenses for the personal suste-
18 nance and comfort of a person required to travel
19 away from the person’s regular post of duty in order
20 to participate in the training.

21 (3) A per diem allowance paid instead of actual
22 expenses for subsistence and fees or tips to porters
23 and stewards.



1 (4) Costs of securing temporary replacements
2 for personnel traveling to, and participating in, the
3 training.

4 **TITLE II—TERRORISM PREVEN-**
5 **TION, INFORMATION SHAR-**
6 **ING, AND RISK ASSESSMENT**

7 **Subtitle A—Terrorism Prevention**

8 **SEC. 201. TERRORISM PREVENTION PLAN AND RELATED**
9 **BUDGET SUBMISSION.**

10 (a) DEPARTMENT OF HOMELAND SECURITY TER-
11 RORISM PREVENTION PLAN.—

12 (1) REQUIREMENTS.—Not later than 1 year
13 after the date of enactment of the Act, and on a reg-
14 ular basis thereafter, the Secretary of Homeland Se-
15 curity shall prepare and submit to the Committee on
16 Homeland Security of the House of Representatives
17 and the Committee on Homeland Security and Gov-
18 ernmental Affairs of the Senate a Department of
19 Homeland Security Terrorism Prevention Plan. The
20 Plan shall be a comprehensive and integrated plan
21 that includes the goals, objectives, milestones, and
22 key initiatives of the Department of Homeland Secu-
23 rity to prevent acts of terrorism on the United
24 States, including its territories and interests.



1 (2) CONTENTS.—The Secretary shall include in
2 the Plan the following elements:

3 (A) Identification and prioritization of
4 groups and subgroups that pose the most sig-
5 nificant threat of committing acts of terrorism
6 on the United States and its interests.

7 (B) Identification of the most significant
8 current, evolving, and long-term terrorist
9 threats to the United States and its interests,
10 including an evaluation of—

11 (i) the materials that may be used to
12 carry out a potential attack;

13 (ii) the methods that may be used to
14 carry out a potential attack; and

15 (iii) the outcome the perpetrators of
16 acts of terrorism aim to achieve.

17 (C) A prioritization of the threats identi-
18 fied under subparagraph (B), based on an as-
19 sessment of probability and consequence of such
20 attacks.

21 (D) A description of processes and proce-
22 dures that the Secretary shall establish to insti-
23 tutionalize close coordination between the De-
24 partment of Homeland Security and the Na-



1 tional Counter Terrorism Center and other ap-
2 propriate United States intelligence agencies.

3 (E) The policies and procedures the Sec-
4 retary shall establish to ensure the Department
5 gathers real-time information from the National
6 Counter Terrorism Center; disseminates this in-
7 formation throughout the Department, as ap-
8 propriate; utilizes this information to support
9 the Department's counterterrorism responsibil-
10 ities; integrates the Department's information
11 collection and analysis functions; and dissemi-
12 nates this information to its operational units,
13 as appropriate.

14 (F) A description of the specific actions
15 the Secretary shall take to identify threats of
16 terrorism on the United States and its inter-
17 ests, and to coordinate activities within the De-
18 partment to prevent acts of terrorism, with spe-
19 cial emphasis on prevention of terrorist access
20 to and use of weapons of mass destruction.

21 (G) A description of initiatives the Sec-
22 retary shall take to share critical terrorism pre-
23 vention information with, and provide terrorism
24 prevention support to, State and local govern-
25 ments and the private sector.



1 (H) A timeline, with goals and milestones,
2 for implementing the Homeland Security Infor-
3 mation Network, the Homeland Security Secure
4 Data Network, and other departmental infor-
5 mation initiatives to prevent acts of terrorism
6 on the United States and its interests, including
7 integration of these initiatives in the operations
8 of the Homeland Security Operations Center.

9 (I) Such other terrorism prevention-related
10 elements as the Secretary considers appro-
11 priate.

12 (3) CONSULTATION.—In formulating the Plan
13 the Secretary shall consult with—

14 (A) the Director of National Intelligence;

15 (B) the Director of the National Counter
16 Terrorism Center;

17 (C) the Attorney General;

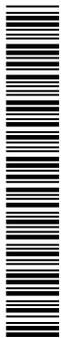
18 (D) the Director of the Federal Bureau of
19 Investigation;

20 (E) the Secretary of Defense;

21 (F) the Secretary of State;

22 (G) the Secretary of Energy;

23 (H) the Secretary of the Treasury; and



1 (I) the heads of other Federal agencies and
2 State, county, and local law enforcement agen-
3 cies as the Secretary considers appropriate.

4 (4) CLASSIFICATION.—The Secretary shall pre-
5 pare the Plan in both classified and nonclassified
6 forms.

7 (b) ANNUAL CROSSCUTTING ANALYSIS OF PROPOSED
8 FUNDING FOR DEPARTMENT OF HOMELAND SECURITY
9 PROGRAMS.—

10 (1) REQUIREMENT TO SUBMIT ANALYSIS.—The
11 Secretary of Homeland Security shall submit to the
12 Congress, concurrently with the submission of the
13 President’s budget for each fiscal year, a detailed,
14 crosscutting analysis of the budget proposed for the
15 Department of Homeland Security, by budget func-
16 tion, by agency, and by initiative area, identifying
17 the requested amounts of gross and net appropria-
18 tions or obligational authority and outlays for pro-
19 grams and activities of the Department for each of
20 the following mission areas:

21 (A) To prevent terrorist attacks within the
22 United States.

23 (B) To reduce the vulnerability of the
24 United States to terrorism.



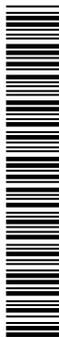
1 (C) To minimize the damage, and assist in
2 the recovery, from terrorist attacks that do
3 occur within the United States.

4 (D) To carry out all functions of the agen-
5 cies and subdivisions within the Department
6 that are not related directly to homeland secu-
7 rity.

8 (2) FUNDING ANALYSIS OF MULTIPURPOSE
9 FUNCTIONS.—The analysis required under para-
10 graph (1) for functions that are both related directly
11 and not related directly to homeland security shall
12 include a detailed allocation of funding for each spe-
13 cific mission area within those functions, including
14 an allocation of funding among mission support
15 functions, such as agency overhead, capital assets,
16 and human capital.

17 (3) INCLUDED TERRORISM PREVENTION ACTIVI-
18 TIES.—The analysis required under paragraph
19 (1)(A) shall include the following activities (among
20 others) of the Department:

21 (A) Collection and effective use of intel-
22 ligence and law enforcement operations that
23 screen for and target individuals who plan or
24 intend to carry out acts of terrorism.



1 (B) Investigative, intelligence, and law en-
2 forcement operations that identify and disrupt
3 plans for acts of terrorism or reduce the ability
4 of groups or individuals to commit acts of ter-
5 rorism.

6 (C) Investigative activities and intelligence
7 operations to detect and prevent the introduc-
8 tion of weapons of mass destruction into the
9 United States.

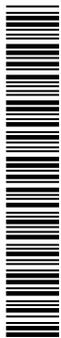
10 (D) Initiatives to detect potential, or the
11 early stages of actual, biological, chemical, radi-
12 ological, or nuclear attacks.

13 (E) Screening individuals against terrorist
14 watch lists.

15 (F) Screening cargo to identify and seg-
16 regate high-risk shipments.

17 (G) Specific utilization of information
18 sharing and intelligence, both horizontally
19 (within the Federal Government) and vertically
20 (among Federal, State, and local governments),
21 to detect or prevent acts of terrorism.

22 (H) Initiatives, including law enforcement
23 and intelligence operations, to preempt, disrupt,
24 and deter acts of terrorism overseas intended to
25 strike the United States.



1 (I) Investments in technology, research
2 and development, training, and communications
3 systems that are designed to improve the per-
4 formance of the Department and its agencies
5 with respect to each of the activities listed in
6 subparagraphs (A) through (H).

7 (4) SEPARATE DISPLAYS FOR MANDATORY AND
8 DISCRETIONARY AMOUNTS.—Each analysis under
9 paragraph (1) shall include separate displays for
10 proposed mandatory appropriations and proposed
11 discretionary appropriations.

12 **SEC. 202. CONSOLIDATED BACKGROUND CHECK PROCESS.**

13 (a) REQUIREMENT.—The Secretary shall establish a
14 single process for conducting the security screening and
15 background checks on individuals participating in any vol-
16 untary or mandatory departmental credentialing or reg-
17 istered traveler program.

18 (b) INCLUDED PROGRAMS.—The process established
19 under subsection (a) shall be sufficient to meet the secu-
20 rity requirements of all applicable Departmental pro-
21 grams, including—

- 22 (1) the Transportation Worker Identification
23 Credential;
24 (2) the Hazmat Endorsement Credential;
25 (3) the Free and Secure Trade program;



1 (4) the NEXUS and SENTRI border crossing
2 programs;

3 (5) the Registered Traveler program of the
4 Transportation Security Administration; and

5 (6) any other similar program or credential con-
6 sidered appropriate for inclusion by the Secretary.

7 (c) FEATURES OF PROCESS.—The process estab-
8 lished under subsection (a) shall include the following:

9 (1) A single submission of security screening in-
10 formation, including personal data and biometric in-
11 formation as appropriate, necessary to meet the se-
12 curity requirements of all applicable departmental
13 programs.

14 (2) An ability to submit such security screening
15 information at any location or through any process
16 approved by the Secretary with respect to any of the
17 applicable departmental programs.

18 (3) Acceptance by the Department of a security
19 clearance issued by a Federal agency, to the extent
20 that the security clearance process of the agency sat-
21 isfies requirements that are at least as stringent as
22 those of the applicable departmental programs under
23 this section.

24 (4) Standards and procedures for protecting in-
25 dividual privacy, confidentiality, record retention,



1 and addressing other concerns relating to informa-
2 tion security.

3 (d) DEADLINES.—The Secretary of Homeland Secu-
4 rity shall—

5 (1) submit a description of the process devel-
6 oped under subsection (a) to the Committee on
7 Homeland Security of the House of Representatives
8 and the Committee on Homeland Security and Gov-
9 ernmental Affairs of the Senate by not later than 6
10 months after the date of the enactment of this Act;
11 and

12 (2) begin implementing such process by not
13 later than 12 months after the date of the enact-
14 ment of this Act.

15 (e) RELATIONSHIP TO OTHER LAWS.—(1) Nothing
16 in this section affects any statutory requirement relating
17 to the operation of the programs described in subsection
18 (b).

19 (2) Nothing in this section affects any statutory re-
20 quirement relating to title III of the Intelligence Reform
21 and Terrorism Prevention Act of 2004 (50 U.S.C. 435b
22 et seq.).



1 **Subtitle B—Homeland Security In-**
2 **formation Sharing and Analysis**
3 **Enhancement**

4 **SEC. 211. SHORT TITLE.**

5 This subtitle may be cited as the “Homeland Security
6 Information Sharing and Analysis Enhancement Act of
7 2005”.

8 **SEC. 212. PROVISION OF TERRORISM-RELATED INFORMA-**
9 **TION TO PRIVATE SECTOR OFFICIALS.**

10 Section 201(d) of the Homeland Security Act of 2002
11 (6 U.S.C. 121(d)) is amended by adding at the end the
12 following:

13 “(20) To require, in consultation with the As-
14 sistant Secretary for Infrastructure Protection, the
15 creation and routine dissemination of analytic re-
16 ports and products designed to provide timely and
17 accurate information that has specific relevance to
18 each of the Nation’s critical infrastructure sectors
19 (as identified in the national infrastructure protec-
20 tion plan issued under paragraph (5)), to private
21 sector officials in each such sector who are respon-
22 sible for protecting institutions within that sector
23 from potential acts of terrorism and for mitigating
24 the potential consequences of any such act.”.



1 **SEC. 213. ANALYTIC EXPERTISE ON THE THREATS FROM BI-**
2 **OLOGICAL AGENTS AND NUCLEAR WEAPONS.**

3 Section 201(d) of the Homeland Security Act of 2002
4 (6 U.S.C. 121(d)) is further amended by adding at the
5 end the following:

6 “(21) To ensure sufficient analytic expertise
7 within the Office of Information Analysis to create
8 and disseminate, on an ongoing basis, products
9 based on the analysis of homeland security informa-
10 tion, as defined in section 892(f)(1), with specific
11 reference to the threat of terrorism involving the use
12 of nuclear weapons and biological agents to inflict
13 mass casualties or other catastrophic consequences
14 on the population or territory of the United States.”.

15 **SEC. 214. ALTERNATIVE ANALYSIS OF HOMELAND SECU-**
16 **RITY INFORMATION.**

17 (a) REQUIREMENT.—Subtitle A of title II of the
18 Homeland Security Act of 2002 (6 U.S.C. 121 et seq.)
19 is amended by adding at the end the following:

20 **“SEC. 203. ALTERNATIVE ANALYSIS OF HOMELAND SECU-**
21 **RITY INFORMATION.**

22 “The Secretary shall establish a process and assign
23 an individual or entity the responsibility to ensure that,
24 as appropriate, elements of the Department conduct alter-
25 native analysis (commonly referred to as ‘red-team anal-
26 ysis’) of homeland security information, as that term is



1 defined in section 892(f)(1), that relates to potential acts
2 of terrorism involving the use of nuclear weapons or bio-
3 logical agents to inflict mass casualties or other cata-
4 strophic consequences on the population or territory of the
5 United States.”.

6 (b) CLERICAL AMENDMENT.—The table of contents
7 in section 1(b) of such Act is amended by inserting after
8 the item relating to section 202 the following:

“Sec. 203. Alternative analysis of homeland security information.”.

9 **SEC. 215. ASSIGNMENT OF INFORMATION ANALYSIS AND**
10 **INFRASTRUCTURE PROTECTION FUNCTIONS.**

11 Section 201(b) of the Homeland Security Act of 2002
12 (6 U.S.C. 121(b)) is amended by adding at the end the
13 following:

14 “(4) ASSIGNMENT OF SPECIFIC FUNCTIONS.—
15 The Under Secretary for Information Analysis and
16 Infrastructure Protection—

17 “(A) shall assign to the Assistant Sec-
18 retary for Information Analysis the responsi-
19 bility for performing the functions described in
20 paragraphs (1), (4), (7) through (14), (16), and
21 (18) of subsection (d);

22 “(B) shall assign to the Assistant Sec-
23 retary for Infrastructure Protection the respon-
24 sibility for performing the functions described



1 in paragraphs (2), (5), and (6) of subsection
2 (d);

3 “(C) shall ensure that the Assistant Sec-
4 retary for Information Analysis and the Assist-
5 ant Secretary for Infrastructure Protection both
6 perform the functions described in paragraphs
7 (3), (15), (17), and (19) of subsection (d);

8 “(D) may assign to each such Assistant
9 Secretary such other duties relating to such re-
10 sponsibilities as the Under Secretary may pro-
11 vide;

12 “(E) shall direct each such Assistant Sec-
13 retary to coordinate with Federal, State, and
14 local law enforcement agencies, and with tribal
15 and private sector entities, as appropriate; and

16 “(F) shall direct the Assistant Secretary
17 for Information Analysis to coordinate with ele-
18 ments of the intelligence community, as appro-
19 priate.”.

20 **SEC. 216. AUTHORITY FOR DISSEMINATING HOMELAND SE-**
21 **CURITY INFORMATION.**

22 (a) IN GENERAL.—Title I of the Homeland Security
23 Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding
24 at the end the following:



1 **“SEC. 104. AUTHORITY FOR DISSEMINATING HOMELAND SE-**
2 **CURITY INFORMATION.**

3 “(a) PRIMARY AUTHORITY.—Except as provided in
4 subsection (b), the Secretary shall be the executive branch
5 official responsible for disseminating homeland security in-
6 formation to State and local government and tribal offi-
7 cials and the private sector.

8 “(b) PRIOR APPROVAL REQUIRED.—No Federal offi-
9 cial may disseminate any homeland security information,
10 as defined in section 892(f)(1), to State, local, tribal, or
11 private sector officials without the Secretary’s prior ap-
12 proval, except—

13 “(1) in exigent circumstances under which it is
14 essential that the information be communicated im-
15 mediately; or

16 “(2) when such information is issued to State,
17 local, or tribal law enforcement officials for the pur-
18 pose of assisting them in any aspect of the adminis-
19 tration of criminal justice.”.

20 (b) CLERICAL AMENDMENT.—The table of contents
21 in section 1(b) of such Act is amended by inserting after
22 the item relating to section 103 the following:

“Sec. 104. Authority for disseminating homeland security information.”.



1 **SEC. 217. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS**
2 **PROGRAM.**

3 (a) ESTABLISHMENT OF PROGRAM.—Subtitle A of
4 title II of the Homeland Security Act of 2002 (6 U.S.C.
5 121 et seq.) is further amended by adding at the end the
6 following:

7 **“SEC. 204. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS**
8 **PROGRAM.**

9 “(a) ESTABLISHMENT.—

10 “(1) IN GENERAL.—The Secretary shall estab-
11 lish a fellowship program in accordance with this
12 section for the purpose of bringing State, local, trib-
13 al, and private sector officials to participate in the
14 work of the Homeland Security Operations Center in
15 order to become familiar with—

16 “(A) the mission and capabilities of that
17 Center; and

18 “(B) the role, programs, products, and
19 personnel of the Office of Information Analysis,
20 the Office of Infrastructure Protection, and
21 other elements of the Department responsible
22 for the integration, analysis, and dissemination
23 of homeland security information, as defined in
24 section 892(f)(1).



1 “(2) PROGRAM NAME.—The program under
2 this section shall be known as the 9/11 Memorial
3 Homeland Security Fellows Program.

4 “(b) ELIGIBILITY.—In order to be eligible for selec-
5 tion as a fellow under the program, an individual must—

6 “(1) have homeland security-related responsibil-
7 ities; and

8 “(2) possess an appropriate national security
9 clearance.

10 “(c) LIMITATIONS.—The Secretary—

11 “(1) may conduct up to 4 iterations of the pro-
12 gram each year, each of which shall be 90 days in
13 duration; and

14 “(2) shall ensure that the number of fellows se-
15 lected for each iteration does not impede the activi-
16 ties of the Center.

17 “(d) CONDITION.—As a condition of selecting an in-
18 dividual as a fellow under the program, the Secretary shall
19 require that the individual’s employer agree to continue
20 to pay the individual’s salary and benefits during the pe-
21 riod of the fellowship.

22 “(e) STIPEND.—During the period of the fellowship
23 of an individual under the program, the Secretary shall,
24 subject to the availability of appropriations—



1 “(i) integrated and analyzed com-
2 prehensively; and

3 “(ii) disseminated in a timely manner,
4 including to appropriately cleared State,
5 local, tribal, and private sector officials;
6 and

7 “(C) such information is used to determine
8 what requests the Department should submit
9 for collection of additional information relating
10 to that threat.”.

11 **SEC. 219. ACCESS OF ASSISTANT SECRETARY FOR INFOR-**
12 **MATION ANALYSIS TO TERRORISM INFORMA-**
13 **TION.**

14 Section 201(d) of the Homeland Security Act of 2002
15 (6 U.S.C. 121(d)) is further amended by adding at the
16 end the following:

17 “(23) To ensure that the Assistant Secretary
18 for Information Analysis—

19 “(A) is routinely and without request given
20 prompt access to all terrorism-related informa-
21 tion collected by or otherwise in the possession
22 of any component of the Department, including
23 all homeland security information (as that term
24 is defined in section 892(f)(1)); and



1 government, tribal, and private sector
2 antiterrorism systems and protocols that have
3 been or are being developed; and

4 “(C) ensuring, to the greatest extent pos-
5 sible, that the homeland security information
6 network and information systems are integrated
7 and interoperable with existing private sector
8 technologies.”.

9 **SEC. 221. IAIP PERSONNEL RECRUITMENT.**

10 (a) IN GENERAL.—Chapter 97 of title 5, United
11 States Code, is amended by adding after section 9701 the
12 following:

13 **“§ 9702. Recruitment bonuses**

14 “(a) IN GENERAL.—Notwithstanding any provision
15 of chapter 57, the Secretary of Homeland Security, acting
16 through the Under Secretary for Information Analysis and
17 Infrastructure Protection, may pay a bonus to an indi-
18 vidual in order to recruit such individual for a position
19 that is primarily responsible for discharging the analytic
20 responsibilities specified in section 201(d) of the Home-
21 land Security Act of 2002 (6 U.S.C. 121(d)) and that—

22 “(1) is within the Directorate for Information
23 Analysis and Infrastructure Protection; and

24 “(2) would be difficult to fill in the absence of
25 such a bonus.



1 In determining which individuals are to receive bonuses
2 under this section, appropriate consideration shall be given
3 to the Directorate's critical need for linguists.

4 “(b) BONUS AMOUNT, FORM, ETC.—

5 “(1) IN GENERAL.—The amount of a bonus
6 under this section shall be determined under regula-
7 tions of the Secretary of Homeland Security, but
8 may not exceed 50 percent of the annual rate of
9 basic pay of the position involved.

10 “(2) FORM OF PAYMENT.—A bonus under this
11 section shall be paid in the form of a lump-sum pay-
12 ment and shall not be considered to be part of basic
13 pay.

14 “(3) COMPUTATION RULE.—For purposes of
15 paragraph (1), the annual rate of basic pay of a po-
16 sition does not include any comparability payment
17 under section 5304 or any similar authority.

18 “(c) SERVICE AGREEMENTS.—Payment of a bonus
19 under this section shall be contingent upon the employee
20 entering into a written service agreement with the Depart-
21 ment of Homeland Security. The agreement shall
22 include—

23 “(1) the period of service the individual shall be
24 required to complete in return for the bonus; and



1 “(2) the conditions under which the agreement
2 may be terminated before the agreed-upon service
3 period has been completed, and the effect of any
4 such termination.

5 “(d) ELIGIBILITY.—A bonus under this section may
6 not be paid to recruit an individual for—

7 “(1) a position to which an individual is ap-
8 pointed by the President, by and with the advice and
9 consent of the Senate;

10 “(2) a position in the Senior Executive Service
11 as a noncareer appointee (as defined under section
12 3132(a)); or

13 “(3) a position which has been excepted from
14 the competitive service by reason of its confidential,
15 policy-determining, policy-making, or policy-advo-
16 cating character.

17 “(e) TERMINATION.—The authority to pay bonuses
18 under this section shall terminate on September 30, 2008.

19 **“§ 9703. Reemployed annuitants**

20 “(a) IN GENERAL.—If an annuitant receiving an an-
21 nuity from the Civil Service Retirement and Disability
22 Fund becomes employed in a position within the Direc-
23 torate for Information Analysis and Infrastructure Protec-
24 tion of the Department of Homeland Security, the annu-
25 itant’s annuity shall continue. An annuitant so reemployed



1 shall not be considered an employee for the purposes of
2 chapter 83 or 84.

3 “(b) TERMINATION.—The exclusion pursuant to this
4 section of the Directorate for Information Analysis and
5 Infrastructure Protection from the reemployed annuitant
6 provisions of chapters 83 and 84 shall terminate 3 years
7 after the date of the enactment of this section, unless ex-
8 tended by the Secretary of Homeland Security. Any such
9 extension shall be for a period of 1 year and shall be re-
10 newable.

11 “(c) ANNUITANT DEFINED.—For purposes of this
12 section, the term ‘annuitant’ has the meaning given such
13 term under section 8331 or 8401, whichever is appro-
14 priate.

15 **“§ 9704. Regulations**

16 “The Secretary of Homeland Security, in consulta-
17 tion with the Director of the Office of Personnel Manage-
18 ment, may prescribe any regulations necessary to carry
19 out section 9702 or 9703.”.

20 (b) CLERICAL AMENDMENT.—The analysis for chap-
21 ter 97 of title 5, United States Code, is amended by add-
22 ing after the item relating to section 9701 the following:

“9702. Recruitment bonuses.

“9703. Reemployed annuitants.

“9704. Regulations.”.



1 **SEC. 222. INFORMATION COLLECTION REQUIREMENTS AND**
2 **PRIORITIES.**

3 (a) IN GENERAL.—Section 102 of the Homeland Se-
4 curity Act of 2002 (6 U.S.C. 112) is amended—

5 (1) by redesignating subsections (e), (f), and
6 (g), as subsections (f), (g), and (h), respectively; and

7 (2) by inserting after subsection (d) the fol-
8 lowing new subsection (e):

9 “(e) PARTICIPATION IN FOREIGN COLLECTION RE-
10 QUIREMENTS AND MANAGEMENT PROCESSES.—The Sec-
11 retary shall be a member of any Federal Government
12 interagency board, established by Executive order or any
13 other binding interagency directive, that is responsible for
14 establishing foreign collection information requirements
15 and priorities for estimative analysis.”.

16 (b) HOMELAND SECURITY INFORMATION REQUIRE-
17 MENTS BOARD.—

18 (1) IN GENERAL.—Title I of such Act (6 U.S.C.
19 111 et seq.) is further amended by adding at the
20 end the following new section:

21 **“SEC. 105. HOMELAND SECURITY INFORMATION REQUIRE-**
22 **MENTS BOARD.**

23 “(a) ESTABLISHMENT OF BOARD.—There is estab-
24 lished an interagency Homeland Security Information Re-
25 quirements Board (hereinafter in this section referred to
26 as the ‘Information Requirements Board’).



1 “(b) MEMBERSHIP.—The following officials are mem-
2 bers of the Information Requirements Board:

3 “(1) The Secretary of Homeland Security, who
4 shall serve as the Chairman of the Information Re-
5 quirements Board.

6 “(2) The Attorney General.

7 “(3) The Secretary of Commerce.

8 “(4) The Secretary of the Treasury.

9 “(5) The Secretary of Defense.

10 “(6) The Secretary of Energy.

11 “(7) The Secretary of State.

12 “(8) The Secretary of the Interior.

13 “(9) The Director of National Intelligence.

14 “(10) The Director of the Federal Bureau of
15 Investigation.

16 “(11) The Director of the National
17 Counterterrorism Center.

18 “(12) The Chief Privacy Officer of the Depart-
19 ment of Homeland Security.

20 “(c) FUNCTIONS.—

21 “(1) OVERSIGHT OF HOMELAND SECURITY RE-
22 QUIREMENTS.—The Information Requirements
23 Board shall oversee the process for establishing
24 homeland security requirements and collection man-
25 agement for all terrorism-related information and all



1 other homeland security information (as defined in
2 section 892(f)(1)) collected within the United States.

3 “(2) DETERMINATION OF COLLECTION PRIOR-
4 ITIES.—The Information Requirements Board
5 shall—

6 “(A) determine the domestic information
7 collection requirements for information relevant
8 to the homeland security mission; and

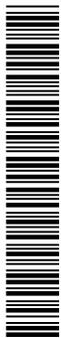
9 “(B) prioritize the collection and use of
10 such information.

11 “(3) COORDINATION OF COLLECTION REQUIRE-
12 MENTS AND MANAGEMENT ACTIVITIES.—

13 “(A) COORDINATION WITH COUNTERPART
14 AGENCIES.—The Chairman shall ensure that
15 the Information Requirements Board carries
16 out its activities in a manner that is fully co-
17 ordinated with the Board’s counterpart entities.

18 “(B) PARTICIPATION OF COUNTERPART
19 ENTITIES.—The Chairman and the Director of
20 National Intelligence shall ensure that each
21 counterpart entity—

22 “(i) has at least one representative on
23 the Information Requirement Board and
24 on every subcomponent of the Board; and



1 “(ii) meets jointly with the Informa-
2 tion Requirements Board (and, as appro-
3 priate, with any subcomponent of the
4 Board) as often as the Chairman and the
5 Director of National Intelligence determine
6 appropriate.

7 “(C) COUNTERPART ENTITY DEFINED.—In
8 this section, the term ‘counterpart entity’
9 means an entity of the Federal Government
10 that is responsible for foreign intelligence collec-
11 tion requirements and management.

12 “(d) MEETINGS.—

13 “(1) IN GENERAL.—The Information Require-
14 ments Board shall meet regularly at such times and
15 places as its Chairman may direct.

16 “(2) INVITED REPRESENTATIVES.—The Chair-
17 man may invite representatives of Federal agencies
18 not specified in subsection (b) to attend meetings of
19 the Information Requirements Board.”.

20 “(2) CLERICAL AMENDMENT.—The table of con-
21 tents in section 1(b) of such Act is further amended
22 by inserting after the item relating to section 104
23 the following new item:

 “Sec. 105. Homeland Security Information Requirements Board.”.



1 **SEC. 223. HOMELAND SECURITY ADVISORY SYSTEM.**

2 (a) IN GENERAL.—Subtitle A of title II of the Home-
3 land Security Act of 2002 is further amended—

4 (1) in section 201(d)(7) (6 U.S.C. 121(d)(7))
5 by inserting “under section 205” after “System”;
6 and

7 (2) by adding at the end the following:

8 **“SEC. 205. HOMELAND SECURITY ADVISORY SYSTEM.**

9 “(a) REQUIREMENT.—The Under Secretary for In-
10 formation Analysis and Infrastructure Protection shall im-
11 plement a Homeland Security Advisory System in accord-
12 ance with this section to provide public advisories and
13 alerts regarding threats to homeland security, including
14 national, regional, local, and economic sector advisories
15 and alerts, as appropriate.

16 “(b) REQUIRED ELEMENTS.—The Under Secretary,
17 under the System—

18 “(1) shall include, in each advisory and alert re-
19 garding a threat, information on appropriate protec-
20 tive measures and countermeasures that may be
21 taken in response to the threat;

22 “(2) shall, whenever possible, limit the scope of
23 each advisory and alert to a specific region, locality,
24 or economic sector believed to be at risk; and

25 “(3) shall not, in issuing any advisory or alert,
26 use color designations as the exclusive means of



1 specifying the homeland security threat conditions
2 that are the subject of the advisory or alert.”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 1(b) of such Act is further amended by adding
5 at the end of the items relating to subtitle A of title II
6 the following:

“Sec. 205. Homeland Security Advisory System.”.

7 **SEC. 224. USE OF OPEN-SOURCE INFORMATION.**

8 Section 201(d) of the Homeland Security Act of 2002
9 (6 U.S.C. 121(d)) is further amended by adding at the
10 end the following:

11 “(25) To ensure that, whenever possible—

12 “(A) the Assistant Secretary for Informa-
13 tion Analysis produces and disseminates reports
14 and analytic products based on open-source in-
15 formation that do not require a national secu-
16 rity classification under applicable law; and

17 “(B) such unclassified open-source reports
18 are produced and disseminated contempora-
19 neously with reports or analytic products con-
20 cerning the same or similar information that
21 the Assistant Secretary for Information Anal-
22 ysis produces and disseminates in a classified
23 format.”.



1 **SEC. 225. FULL AND EFFICIENT USE OF OPEN-SOURCE IN-**
2 **FORMATION.**

3 (a) REQUIREMENT.—Subtitle A of title II of the
4 Homeland Security Act of 2002 (6 U.S.C. 121 et seq.)
5 is further amended by adding at the end the following:

6 **“SEC. 206. FULL AND EFFICIENT USE OF OPEN-SOURCE IN-**
7 **FORMATION.**

8 “The Under Secretary shall ensure that, in meeting
9 their analytic responsibilities under section 201(d) and in
10 formulating requirements for collection of additional infor-
11 mation, the Assistant Secretary for Information Analysis
12 and the Assistant Secretary for Infrastructure Protection
13 make full and efficient use of open-source information
14 wherever possible.”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of such Act is further amended by inserting
17 after the item relating to section 205 the following:

“Sec. 206. Full and efficient use of open-source information.”.

18 **TITLE III—DOMESTIC PRE-**
19 **PAREDNESS AND PROTEC-**
20 **TION**

21 **Subtitle A—Preparedness and**
22 **Protection**

23 **SEC. 301. NATIONAL TERRORISM EXERCISE PROGRAM.**

24 (a) IN GENERAL.—Section 430(c) of the Homeland
25 Security Act of 2002 (6 U.S.C. 238) is amended by strik-



1 ing “and” after the semicolon at the end of paragraph
2 (8), by striking the period at the end of paragraph (9)
3 and inserting “; and”, and by adding at the end the fol-
4 lowing:

5 “(10) designing, developing, performing, and
6 evaluating exercises at the national, State, terri-
7 torial, regional, local, and tribal levels of government
8 that incorporate government officials, emergency re-
9 sponse providers, public safety agencies, the private
10 sector, international governments and organizations,
11 and other appropriate entities to test the Nation’s
12 capability to prevent, prepare for, respond to, and
13 recover from threatened or actual acts of ter-
14 rorism.”.

15 (b) NATIONAL TERRORISM EXERCISE PROGRAM.—

16 (1) ESTABLISHMENT OF PROGRAM.—Title VIII
17 of the Homeland Security Act of 2002 (Public Law
18 107–296) is amended by adding at the end the fol-
19 lowing new subtitle:

20 **“Subtitle J—Terrorism**
21 **Preparedness Exercises**

22 **“SEC. 899a. NATIONAL TERRORISM EXERCISE PROGRAM.**

23 “(a) IN GENERAL.—The Secretary, through the Of-
24 fice for Domestic Preparedness, shall establish a National
25 Terrorism Exercise Program for the purpose of testing



1 and evaluating the Nation’s capabilities to prevent, pre-
2 pare for, respond to, and recover from threatened or ac-
3 tual acts of terrorism that—

4 “(1) enhances coordination for terrorism pre-
5 paredness between all levels of government, emer-
6 gency response providers, international governments
7 and organizations, and the private sector;

8 “(2) is—

9 “(A) multidisciplinary in nature, including,
10 as appropriate, information analysis and
11 cybersecurity components;

12 “(B) as realistic as practicable and based
13 on current risk assessments, including credible
14 threats, vulnerabilities, and consequences;

15 “(C) carried out with the minimum degree
16 of notice to involved parties regarding the tim-
17 ing and details of such exercises, consistent
18 with safety considerations;

19 “(D) evaluated against performance meas-
20 ures and followed by corrective action to solve
21 identified deficiencies; and

22 “(E) assessed to learn best practices,
23 which shall be shared with appropriate Federal,
24 State, territorial, regional, local, and tribal per-



1 sonnel, authorities, and training institutions for
2 emergency response providers; and

3 “(3) assists State, territorial, local, and tribal
4 governments with the design, implementation, and
5 evaluation of exercises that—

6 “(A) conform to the requirements of para-
7 graph (2); and

8 “(B) are consistent with any applicable
9 State homeland security strategy or plan.

10 “(b) NATIONAL LEVEL EXERCISES.—The Secretary,
11 through the National Terrorism Exercise Program, shall
12 perform on a periodic basis national terrorism prepared-
13 ness exercises for the purposes of—

14 “(1) involving top officials from Federal, State,
15 territorial, local, tribal, and international govern-
16 ments, as the Secretary considers appropriate;

17 “(2) testing and evaluating the Nation’s capa-
18 bility to detect, disrupt, and prevent threatened or
19 actual catastrophic acts of terrorism, especially those
20 involving weapons of mass destruction; and

21 “(3) testing and evaluating the Nation’s readi-
22 ness to respond to and recover from catastrophic
23 acts of terrorism, especially those involving weapons
24 of mass destruction.



1 “(c) CONSULTATION WITH FIRST RESPONDERS.—In
2 implementing the responsibilities described in subsections
3 (a) and (b), the Secretary shall consult with a geographic
4 (including urban and rural) and substantive cross section
5 of governmental and nongovernmental first responder dis-
6 ciplines, including as appropriate—

7 “(1) Federal, State, and local first responder
8 training institutions;

9 “(2) representatives of emergency response pro-
10 viders; and

11 “(3) State and local officials with an expertise
12 in terrorism preparedness.”.

13 (2) CLERICAL AMENDMENT.—The table of con-
14 tents in section 1(b) of such Act is amended by add-
15 ing at the end of the items relating to title VIII the
16 following:

“Subtitle J—Terrorism Preparedness Exercises

“Sec. 899a. National terrorism exercise program.”.

17 (c) TOPOFF PREVENTION EXERCISE.—No later
18 than one year after the date of enactment of this Act, the
19 Secretary of Homeland Security shall design and carry out
20 a national terrorism prevention exercise for the purposes
21 of—

22 (1) involving top officials from Federal, State,
23 territorial, local, tribal, and international govern-
24 ments; and



1 (2) testing and evaluating the Nation's capa-
2 bility to detect, disrupt, and prevent threatened or
3 actual catastrophic acts of terrorism, especially those
4 involving weapons of mass destruction.

5 **SEC. 302. TECHNOLOGY DEVELOPMENT AND TRANSFER.**

6 (a) ESTABLISHMENT OF TECHNOLOGY CLEARING-
7 HOUSE.—Not later than 90 days after the date of enact-
8 ment of this Act, the Secretary shall complete the estab-
9 lishment of the Technology Clearinghouse under section
10 313 of the Homeland Security Act of 2002.

11 (b) TRANSFER PROGRAM.—Section 313 of the Home-
12 land Security Act of 2002 (6 U.S.C. 193) is amended—

13 (1) by adding at the end of subsection (b) the
14 following new paragraph:

15 “(6) The establishment of a homeland security
16 technology transfer program to facilitate the identi-
17 fication, modification, and commercialization of tech-
18 nology and equipment for use by Federal, State, and
19 local governmental agencies, emergency response
20 providers, and the private sector to prevent, prepare
21 for, or respond to acts of terrorism.”;

22 (2) by redesignating subsection (c) as sub-
23 section (d); and

24 (3) by inserting after subsection (b) the fol-
25 lowing new subsection:

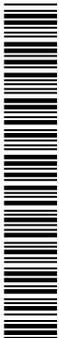


1 “(c) TECHNOLOGY TRANSFER PROGRAM.—In devel-
2 oping the program described in subsection (b)(6), the Sec-
3 retary, acting through the Under Secretary for Science
4 and Technology, shall—

5 “(1) in consultation with the other Under Sec-
6 retaries of the Department and the Director of the
7 Office for Domestic Preparedness, on an ongoing
8 basis—

9 “(A) conduct surveys and reviews of avail-
10 able appropriate technologies that have been, or
11 are in the process of being developed, tested,
12 evaluated, or demonstrated by the Department,
13 other Federal agencies, or the private sector or
14 foreign governments and international organiza-
15 tions and that may be useful in assisting Fed-
16 eral, State, and local governmental agencies,
17 emergency response providers, or the private
18 sector to prevent, prepare for, or respond to
19 acts of terrorism;

20 “(B) conduct or support research, develop-
21 ment, tests, and evaluations, as appropriate of
22 technologies identified under subparagraph (A),
23 including any necessary modifications to such
24 technologies for antiterrorism use;



1 “(C) communicate to Federal, State, and
2 local governmental agencies, emergency re-
3 sponse providers, or the private sector the avail-
4 ability of such technologies for antiterrorism
5 use, as well as the technology’s specifications,
6 satisfaction of appropriate standards, and the
7 appropriate grants available from the Depart-
8 ment to purchase such technologies;

9 “(D) coordinate the selection and adminis-
10 tration of all technology transfer activities of
11 the Science and Technology Directorate, includ-
12 ing projects and grants awarded to the private
13 sector and academia; and

14 “(E) identify priorities based on current
15 risk assessments within the Department of
16 Homeland Security for identifying, researching,
17 developing, testing, evaluating, modifying, and
18 fielding existing technologies for antiterrorism
19 purposes;

20 “(2) in support of the activities described in
21 paragraph (1)—

22 “(A) consult with Federal, State, and local
23 emergency response providers;



1 “(B) consult with government agencies and
2 nationally recognized standards development or-
3 ganizations as appropriate;

4 “(C) enter into agreements and coordinate
5 with other Federal agencies, foreign govern-
6 ments, and national and international organiza-
7 tions as the Secretary determines appropriate,
8 in order to maximize the effectiveness of such
9 technologies or to facilitate commercialization of
10 such technologies; and

11 “(D) consult with existing technology
12 transfer programs and Federal and State train-
13 ing centers that research, develop, test, evalu-
14 ate, and transfer military and other tech-
15 nologies for use by emergency response pro-
16 viders; and

17 “(3) establish a working group in coordination
18 with the Secretary of Defense to advise and assist
19 the technology clearinghouse in the identification of
20 military technologies that are in the process of being
21 developed, or are developed, by the Department of
22 Defense or the private sector, which may include—

23 “(A) representatives from the Department
24 of Defense or retired military officers;



1 “(B) nongovernmental organizations or
2 private companies that are engaged in the re-
3 search, development, testing, or evaluation of
4 related technologies or that have demonstrated
5 prior experience and success in searching for
6 and identifying technologies for Federal agen-
7 cies;

8 “(C) Federal, State, and local emergency
9 response providers; and

10 “(D) to the extent the Secretary considers
11 appropriate, other organizations, other inter-
12 ested Federal, State, and local agencies, and
13 other interested persons.”.

14 (c) REPORT.—Not later than 1 year after the date
15 of enactment of this Act, the Under Secretary for Science
16 and Technology shall transmit to the Congress a descrip-
17 tion of the progress the Department has made in imple-
18 menting the provisions of section 313 of the Homeland
19 Security Act of 2002, as amended by this Act, including
20 a description of the process used to review unsolicited pro-
21 posals received as described in subsection (b)(3) of such
22 section.

23 (d) SAVINGS CLAUSE.—Nothing in this section (in-
24 cluding the amendments made by this section) shall be
25 construed to alter or diminish the effect of the limitation



1 on the authority of the Secretary of Homeland Security
2 under section 302(4) of the Homeland Security Act of
3 2002 (6 U.S.C. 182(4)) with respect to human health-re-
4 lated research and development activities.

5 **SEC. 303. REVIEW OF ANTITERRORISM ACQUISITIONS.**

6 (a) STUDY.—The Secretary of Homeland Security
7 shall conduct a study of all Department of Homeland Se-
8 curity procurements, including ongoing procurements and
9 anticipated procurements, to—

10 (1) identify those that involve any product,
11 equipment, service (including support services), de-
12 vice, or technology (including information tech-
13 nology) that is being designed, developed, modified,
14 or procured for the specific purpose of preventing,
15 detecting, identifying, or deterring acts of terrorism
16 or limiting the harm such acts might otherwise
17 cause; and

18 (2) assess whether such product, equipment,
19 service (including support services), device, or tech-
20 nology is an appropriate candidate for the litigation
21 and risk management protections of subtitle G of
22 title VIII of the Homeland Security Act of 2002.

23 (b) SUMMARY AND CLASSIFICATION REPORT.—Not
24 later than 180 days after the date of enactment of this



1 Act, the Secretary shall transmit to the Congress a
2 report—

3 (1) describing each product, equipment, service
4 (including support services), device, and technology
5 identified under subsection (a) that the Secretary
6 believes would be an appropriate candidate for the
7 litigation and risk management protections of sub-
8 title G of title VIII of the Homeland Security Act
9 of 2002;

10 (2) listing each such product, equipment, serv-
11 ice (including support services), device, and tech-
12 nology in order of priority for deployment in accord-
13 ance with current terrorism risk assessment infor-
14 mation; and

15 (3) setting forth specific actions taken, or to be
16 taken, to encourage or require persons or entities
17 that sell or otherwise provide such products, equip-
18 ment, services (including support services), devices,
19 and technologies to apply for the litigation and risk
20 management protections of subtitle G of title VIII of
21 the Homeland Security Act of 2002, and to ensure
22 prioritization of the Department's review of such
23 products, equipment, services, devices, and tech-
24 nologies under such Act in accordance with the



1 prioritization set forth in paragraph (2) of this sub-
2 section.

3 **SEC. 304. CENTER OF EXCELLENCE FOR BORDER SECUR-**
4 **RITY.**

5 The Secretary of Homeland Security shall establish
6 a university-based Center for Excellence for Border Secu-
7 rity following the merit-review processes and procedures
8 that have been established for selecting University Pro-
9 grams Centers of Excellence. The Center shall prioritize
10 its activities on the basis of risk to address the most sig-
11 nificant threats, vulnerabilities, and consequences posed
12 by the Nation's borders and border control systems, in-
13 cluding the conduct of research, the examination of exist-
14 ing and emerging border security technology and systems,
15 and the provision of education, technical, and analytical
16 assistance for the Department of Homeland Security to
17 effectively secure the Nation's borders.

18 **SEC. 305. REQUIREMENTS RELATING TO THE CONTAINER**
19 **SECURITY INITIATIVE (CSI).**

20 (a) RISK ASSESSMENT AND DESIGNATION OF NEW
21 FOREIGN SEAPORTS.—

22 (1) RISK ASSESSMENT.—The Secretary of
23 Homeland Security shall conduct a risk assessment
24 of each foreign seaport that the Secretary is consid-
25 ering designating as a port under the Container Se-



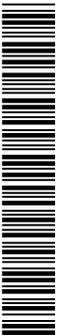
1 security Initiative (CSI) on or after the date of the en-
2 actment of this Act. Each such assessment shall
3 evaluate the level of risk for the potential com-
4 promise of cargo containers by terrorists or terrorist
5 weapons.

6 (2) DESIGNATION.—The Secretary is author-
7 ized to designate a foreign seaport as a port under
8 CSI on or after the date of the enactment of this
9 Act only if the Secretary determines, based on a risk
10 assessment under paragraph (1) and a cost-benefit
11 analysis, that the benefits of designating such port
12 outweigh the cost of expanding the program to such
13 port.

14 (b) DEPLOYMENT OF INSPECTION EQUIPMENT TO
15 NEW CSI PORTS.—

16 (1) DEPLOYMENT.—The Secretary is author-
17 ized to assist in the loaning of nonintrusive inspec-
18 tion equipment for cargo containers, on a non-
19 reimbursable basis, at each CSI port designated
20 under subsection (a)(2) and provide training for per-
21 sonnel at the CSI port to operate the nonintrusive
22 inspection equipment.

23 (2) ADDITIONAL REQUIREMENTS.—The Sec-
24 retary shall establish technical capability require-
25 ments and standard operating procedures for non-



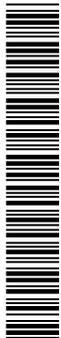
1 intrusive inspection equipment described in para-
2 graph (1) and shall require each CSI port to agree
3 to operate such equipment in accordance with such
4 requirements and procedures as a condition for re-
5 ceiving the equipment and training under such para-
6 graph.

7 (c) DEPLOYMENT OF PERSONNEL TO NEW CSI
8 PORTS; REEVALUATION OF PERSONNEL AT ALL CSI
9 PORTS.—

10 (1) DEPLOYMENT.—The Secretary shall deploy
11 Department of Homeland Security personnel to each
12 CSI port designated under subsection (a)(1) with re-
13 spect to which the Secretary determines that the de-
14 ployment is necessary to successfully implement the
15 requirements of CSI at the port.

16 (2) REEVALUATION.—The Secretary shall peri-
17 odically review relevant risk assessment information
18 with respect to all CSI ports at which Department
19 of Homeland Security personnel are deployed to as-
20 sess whether or not continued deployment of such
21 personnel, in whole or in part, is necessary to suc-
22 cessfully implement the requirements of CSI at the
23 port.

24 (d) INSPECTION AND SCREENING AT UNITED
25 STATES PORTS OF ENTRY.—Cargo containers arriving at



1 a United States port of entry from a CSI port shall under-
2 go the same level of inspection and screening for potential
3 compromise by terrorists or terrorist weapons as cargo
4 containers arriving at a United States port of entry from
5 a foreign seaport that is not participating in CSI unless
6 the containers were initially inspected at the CSI port at
7 the request of CSI personnel and such personnel verify
8 and electronically record that the inspection indicates that
9 the containers have not been compromised by terrorists
10 or terrorist weapons.

11 (e) DEFINITION.—In this section, the term “Con-
12 tainer Security Initiative” or “CSI” means the program
13 carried out by the Department of Homeland Security
14 under which the Department enters into agreements with
15 foreign seaports to—

16 (1) establish security criteria to identify high-
17 risk maritime cargo containers bound for the United
18 States based on advance information; and

19 (2) screen or inspect such maritime cargo con-
20 tainers for potential compromise by terrorists or ter-
21 rorist weapons prior to shipment to the United
22 States.

23 **SEC. 306. SECURITY OF MARITIME CARGO CONTAINERS.**

24 (a) REGULATIONS.—



1 (1) IN GENERAL.—Not later than 180 days
2 after the date of the enactment of this Act, the Sec-
3 retary of Homeland Security shall issue regulations
4 for the security of maritime cargo containers moving
5 within the intermodal transportation system in ac-
6 cordance with the requirements of paragraph (2).

7 (2) REQUIREMENTS.—The regulations issued
8 pursuant to paragraph (1) shall be in accordance
9 with recommendations of the Maritime Transpor-
10 tation Security Act Subcommittee of the Advisory
11 Committee on Commercial Operations of the Depart-
12 ment of Homeland Security, including recommenda-
13 tions relating to obligation to seal, recording of seal
14 changes, modal changes, seal placement, ocean car-
15 rier seal verification, and addressing seal anomalies.

16 (b) INTERNATIONAL AGREEMENTS.—The Secretary
17 shall seek to enter into agreements with foreign countries
18 and international organizations to establish standards for
19 the security of maritime cargo containers moving within
20 the intermodal transportation system that, to the max-
21 imum extent practicable, meet the requirements of sub-
22 section (a)(2).

23 (c) CONTAINER TARGETING STRATEGY.—

24 (1) STRATEGY.—The Secretary shall develop a
25 strategy to improve the ability of the Department of



1 Homeland Security to use information contained in
2 shipping bills of lading to identify and provide addi-
3 tional review of anomalies in such bills of lading.
4 The strategy shall include a method of contacting
5 shippers in a timely fashion to verify or explain any
6 anomalies in shipping bills of lading.

7 (2) REPORT.—Not later than 90 days after the
8 date of the enactment of this Act, the Secretary
9 shall submit to the appropriate congressional com-
10 mittees a report on the implementation of this sub-
11 section, including information on any data searching
12 technologies that will be used to implement the
13 strategy.

14 (d) CONTAINER SECURITY DEMONSTRATION PRO-
15 GRAM.—

16 (1) PROGRAM.—The Secretary is authorized to
17 establish and carry out a demonstration program
18 that integrates nonintrusive inspection equipment,
19 including radiation detection equipment and gamma
20 ray inspection equipment, at an appropriate United
21 States seaport, as determined by the Secretary.

22 (2) REQUIREMENT.—The demonstration pro-
23 gram shall also evaluate automatic identification
24 methods for containers and vehicles and a data shar-
25 ing network capable of transmitting inspection data



1 between ports and appropriate entities within the
2 Department of Homeland Security.

3 (3) REPORT.—Upon completion of the dem-
4 onstration program, the Secretary shall submit to
5 the appropriate congressional committees a report
6 on the implementation of this subsection.

7 (e) CONSOLIDATION OF CONTAINER SECURITY PRO-
8 GRAMS.—The Secretary shall consolidate all programs of
9 the Department of Homeland Security relating to the se-
10 curity of maritime cargo containers, including the dem-
11 onstration program established pursuant to subsection
12 (d), to achieve enhanced coordination and efficiency.

13 **SEC. 307. SECURITY PLAN FOR GENERAL AVIATION AT**
14 **RONALD REAGAN WASHINGTON NATIONAL**
15 **AIRPORT.**

16 Not later than 180 days after the date of enactment
17 of this Act, the Secretary of Homeland Security shall im-
18 plement section 823(a) of the Vision 100—Century of
19 Aviation Reauthorization Act (49 U.S.C. 41718 note; 117
20 Stat. 2595).

21 **SEC. 308. INTEROPERABLE COMMUNICATIONS ASSIST-**
22 **ANCE.**

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

24 (1) The 9/11 Commission determined that the
25 inability of first responders to communicate effec-



1 tively on September 11, 2001 was a critical obstacle
2 to an effective multi-jurisdictional response.

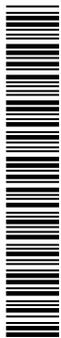
3 (2) Many jurisdictions across the country still
4 experience difficulties communicating that may con-
5 tribute to confusion, delays, or added risks when re-
6 sponding to an emergency.

7 (3) During fiscal year 2004, the Office for Do-
8 mestic Preparedness awarded over \$834,000,000 for
9 2,912 projects through Department of Homeland
10 Security grant programs for the purposes of improv-
11 ing communications interoperability.

12 (4) Interoperable communications systems are
13 most effective when designed to comprehensively ad-
14 dress, on a regional basis, the communications of all
15 types of public safety agencies, first responder dis-
16 ciplines, and State and local government facilities.

17 (5) Achieving communications interoperability
18 is complex due to the extensive training, system
19 modifications, and agreements among the different
20 jurisdictions that are necessary to implement effec-
21 tive communications systems.

22 (6) The Congress authorized the Department of
23 Homeland Security to create an Office for Interoper-
24 ability and Compatibility in the Intelligence Reform
25 and Terrorism Prevention Act of 2004 to, among



1 other things, establish a comprehensive national ap-
2 proach, coordinate federal activities, accelerate the
3 adoption of standards, and encourage research and
4 development to achieve interoperable communica-
5 tions for first responders.

6 (7) The Office for Interoperability and Compat-
7 ibility includes the SAFECOM Program that serves
8 as the umbrella program within the Federal govern-
9 ment to improve public safety communications inter-
10 operability, and has developed the RAPIDCOM pro-
11 gram, the Statewide Communications Interoper-
12 ability Planning Methodology, and a Statement of
13 Requirements to provide technical, planning, and
14 purchasing assistance for Federal departments and
15 agencies, State and local governments, and first re-
16 sponders.

17 (b) SENSE OF CONGRESS.—It is the sense of the
18 Congress that the Department of Homeland Security
19 should implement as expeditiously as possible the initia-
20 tives assigned to the Office for Interoperability and Com-
21 patibility under section 7303 of the Intelligence Reform
22 and Terrorism Prevention Act of 2004 (6 U.S.C. 194),
23 including specifically the following:



1 and Governmental Affairs of the Senate by no later than
2 120 days after the date of the enactment of this Act re-
3 garding how the Department of Homeland Security will
4 implement the applicable recommendations from the Gov-
5 ernment Accountability Office report entitled “Homeland
6 Security: Much is Being Done to Protect Agriculture from
7 a Terrorist Attack, but Important Challenges Remain”
8 (GAO-05-214).

9 **Subtitle B—Department of Home-**
10 **land Security Cybersecurity En-**
11 **hancement**

12 **SEC. 311. SHORT TITLE.**

13 This subtitle may be cited as the “Department of
14 Homeland Security Cybersecurity Enhancement Act of
15 2005”.

16 **SEC. 312. ASSISTANT SECRETARY FOR CYBERSECURITY.**

17 (a) IN GENERAL.—Subtitle A of title II of the Home-
18 land Security Act of 2002 (6 U.S.C. 121 et seq.) is further
19 amended by adding at the end the following:

20 **“SEC. 207. ASSISTANT SECRETARY FOR CYBERSECURITY.**

21 “(a) IN GENERAL.—There shall be in the Directorate
22 for Information Analysis and Infrastructure Protection a
23 National Cybersecurity Office headed by an Assistant Sec-
24 retary for Cybersecurity (in this section referred to as the



1 ‘Assistant Secretary’), who shall assist the Secretary in
2 promoting cybersecurity for the Nation.

3 “(b) GENERAL AUTHORITY.—The Assistant Sec-
4 retary, subject to the direction and control of the Sec-
5 retary, shall have primary authority within the Depart-
6 ment for all cybersecurity-related critical infrastructure
7 protection programs of the Department, including with re-
8 spect to policy formulation and program management.

9 “(c) RESPONSIBILITIES.—The responsibilities of the
10 Assistant Secretary shall include the following:

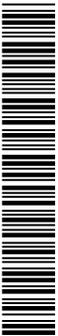
11 “(1) To establish and manage—

12 “(A) a national cybersecurity response sys-
13 tem that includes the ability to—

14 “(i) analyze the effect of cybersecurity
15 threat information on national critical in-
16 frastructure; and

17 “(ii) aid in the detection and warning
18 of attacks on, and in the restoration of,
19 cybersecurity infrastructure in the after-
20 math of such attacks;

21 “(B) a national cybersecurity threat and
22 vulnerability reduction program that identifies
23 cybersecurity vulnerabilities that would have a
24 national effect on critical infrastructure, per-
25 forms vulnerability assessments on information



1 technologies, and coordinates the mitigation of
2 such vulnerabilities;

3 “(C) a national cybersecurity awareness
4 and training program that promotes
5 cybersecurity awareness among the public and
6 the private sectors and promotes cybersecurity
7 training and education programs;

8 “(D) a government cybersecurity program
9 to coordinate and consult with Federal, State,
10 and local governments to enhance their
11 cybersecurity programs; and

12 “(E) a national security and international
13 cybersecurity cooperation program to help fos-
14 ter Federal efforts to enhance international
15 cybersecurity awareness and cooperation.

16 “(2) To coordinate with the private sector on
17 the program under paragraph (1) as appropriate,
18 and to promote cybersecurity information sharing,
19 vulnerability assessment, and threat warning regard-
20 ing critical infrastructure.

21 “(3) To coordinate with other directorates and
22 offices within the Department on the cybersecurity
23 aspects of their missions.

24 “(4) To coordinate with the Under Secretary
25 for Emergency Preparedness and Response to en-



1 sure that the National Response Plan developed pur-
2 suant to section 502(6) of the Homeland Security
3 Act of 2002 (6 U.S.C. 312(6)) includes appropriate
4 measures for the recovery of the cybersecurity ele-
5 ments of critical infrastructure.

6 “(5) To develop processes for information shar-
7 ing with the private sector, consistent with section
8 214, that—

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

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

16 “(6) To coordinate with the Chief Information
17 Officer of the Department in establishing a secure
18 information sharing architecture and information
19 sharing processes, including with respect to the De-
20 partment’s operation centers.

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

24 “(8) To consult with the Office for Domestic
25 Preparedness to ensure that realistic cybersecurity



1 scenarios are incorporated into tabletop and recovery
2 exercises.

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

6 “(10) To consult and coordinate within the De-
7 partment and, where appropriate, with other rel-
8 evant Federal agencies, on security of digital control
9 systems, such as Supervisory Control and Data Ac-
10 quisition (SCADA) systems.

11 “(d) AUTHORITY OVER THE NATIONAL COMMUNICA-
12 TIONS SYSTEM.—The Assistant Secretary shall have pri-
13 mary authority within the Department over the National
14 Communications System.”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of such Act is amended by adding at the
17 end of the items relating to subtitle A of title II the fol-
18 lowing:

“Sec. 207. Assistant Secretary for Cybersecurity.”.

19 **SEC. 313. CYBERSECURITY DEFINED.**

20 Section 2 of the Homeland Security Act of 2002 (6
21 U.S.C. 101) is amended by adding at the end the fol-
22 lowing:

23 “(17)(A) The term ‘cybersecurity’ means the
24 prevention of damage to, the protection of, and the
25 restoration of computers, electronic communications



1 systems, electronic communication services, wire
2 communication, and electronic communication, in-
3 cluding information contained therein, to ensure its
4 availability, integrity, authentication, confidentiality,
5 and nonrepudiation.

6 “(B) In this paragraph—

7 “(i) each of the terms ‘damage’ and ‘com-
8 puter’ has the meaning that term has in section
9 1030 of title 18, United States Code; and

10 “(ii) each of the terms ‘electronic commu-
11 nications system’, ‘electronic communication
12 service’, ‘wire communication’, and ‘electronic
13 communication’ has the meaning that term has
14 in section 2510 of title 18, United States
15 Code.”.

16 **SEC. 314. CYBERSECURITY TRAINING PROGRAMS AND**
17 **EQUIPMENT.**

18 (a) IN GENERAL.—The Secretary of Homeland Secu-
19 rity, acting through the Assistant Secretary for
20 Cybersecurity, may establish, in conjunction with the Na-
21 tional Science Foundation, a program to award grants to
22 institutions of higher education (and consortia thereof)
23 for—

24 (1) the establishment or expansion of
25 cybersecurity professional development programs;



1 (2) the establishment or expansion of associate
2 degree programs in cybersecurity; and

3 (3) the purchase of equipment to provide train-
4 ing in cybersecurity for either professional develop-
5 ment programs or degree programs.

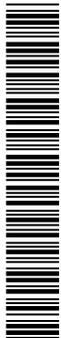
6 (b) ROLES.—

7 (1) DEPARTMENT OF HOMELAND SECURITY.—

8 The Secretary, acting through the Assistant Sec-
9 retary for Cybersecurity and in consultation with the
10 Director of the National Science Foundation, shall
11 establish the goals for the program established
12 under this section and the criteria for awarding
13 grants under the program.

14 (2) NATIONAL SCIENCE FOUNDATION.—The Di-
15 rector of the National Science Foundation shall op-
16 erate the program established under this section
17 consistent with the goals and criteria established
18 under paragraph (1), including soliciting applicants,
19 reviewing applications, and making and admin-
20 istering grant awards. The Director may consult
21 with the Assistant Secretary for Cybersecurity in se-
22 lecting awardees.

23 (3) FUNDING.—The Secretary shall transfer to
24 the National Science Foundation the funds nec-
25 essary to carry out this section.



1 (c) GRANT AWARDS.—

2 (1) PEER REVIEW.—All grant awards under
3 this section shall be made on a competitive, merit-
4 reviewed basis.

5 (2) FOCUS.—In making grant awards under
6 this section, the Director shall, to the extent prac-
7 ticable, ensure geographic diversity and the partici-
8 pation of women and underrepresented minorities.

9 (3) PREFERENCE.—In making grant awards
10 under this section, the Director shall give preference
11 to applications submitted by consortia of institutions
12 to encourage as many students and professionals as
13 possible to benefit from this program.

14 (d) AUTHORIZATION OF APPROPRIATIONS.—Of the
15 amount authorized under section 101, there is authorized
16 to be appropriated to the Secretary for carrying out this
17 section \$3,700,000 for fiscal year 2006.

18 (e) DEFINITIONS.—In this section, the term “institu-
19 tion of higher education” has the meaning given that term
20 in section 101(a) of the Higher Education Act of 1965
21 (20 U.S.C. 1001(a)).

22 **SEC. 315. INFORMATION SECURITY REQUIREMENTS AND**
23 **OMB RESPONSIBILITIES NOT AFFECTED.**

24 (a) IN GENERAL.—This subtitle does not affect—



1 (1) any information security requirement under
2 any other Federal law; or

3 (2) the responsibilities of the Director of the
4 Office of Management and Budget under any other
5 Federal law.

6 (b) LAWS INCLUDED.—The laws referred to in sub-
7 section (a) include the following:

8 (1) Chapter 35 of title 44, United States Code,
9 popularly known as the Paperwork Reduction Act.

10 (2) The Clinger-Cohen Act of 1996 (divisions D
11 and E of Public Law 104–106), including the provi-
12 sions of law enacted by amendments made by that
13 Act.

14 (3) The Federal Information Security Manage-
15 ment Act of 2002 (title III of Public Law 107–347),
16 including the provisions of law enacted by amend-
17 ments made by that Act.

18 **Subtitle C—Security of Public**
19 **Transportation Systems**

20 **SEC. 321. SECURITY BEST PRACTICES.**

21 Not later than 120 days after the date of enactment
22 of this Act, the Secretary of Homeland Security shall de-
23 velop, disseminate to appropriate owners, operators, and
24 providers of public transportation systems, public trans-
25 portation employees and employee representatives, and



1 Federal, State, and local officials, and transmit to Con-
2 gress, a report containing best practices for the security
3 of public transportation systems. In developing best prac-
4 tices, the Secretary shall be responsible for consulting with
5 and collecting input from owners, operators, and providers
6 of public transportation systems, public transportation
7 employee representatives, first responders, industry asso-
8 ciations, private sector experts, academic experts, and ap-
9 propriate Federal, State, and local officials.

10 **SEC. 322. PUBLIC AWARENESS.**

11 Not later than 90 days after the date of enactment
12 of this Act, the Secretary of Homeland Security shall de-
13 velop a national plan for public outreach and awareness.
14 Such plan shall be designed to increase awareness of
15 measures that the general public, public transportation
16 passengers, and public transportation employees can take
17 to increase public transportation system security. Such
18 plan shall also provide outreach to owners, operators, pro-
19 viders, and employees of public transportation systems to
20 improve their awareness of available technologies, ongoing
21 research and development efforts, and available Federal
22 funding sources to improve public transportation security.
23 Not later than 9 months after the date of enactment of
24 this Act, the Secretary shall implement the plan developed
25 under this section.



1 **Subtitle D—Critical Infrastructure**
2 **Prioritization**

3 **SEC. 331. CRITICAL INFRASTRUCTURE.**

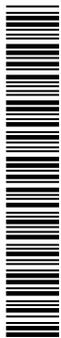
4 (a) COMPLETION OF PRIORITIZATION.—Not later
5 than 90 days after the date of the enactment of this Act,
6 the Secretary of Homeland Security shall complete the
7 prioritization of the Nation’s critical infrastructure ac-
8 cording to all of the following criteria:

9 (1) The threat of terrorist attack, based on
10 threat information received and analyzed by the Of-
11 fice of Information Analysis of the Department re-
12 garding the intentions and capabilities of terrorist
13 groups and other potential threats to the Nation’s
14 critical infrastructure.

15 (2) The likelihood that an attack would cause
16 the destruction or significant disruption of such in-
17 frastructure.

18 (3) The likelihood that an attack would result
19 in substantial numbers of deaths and serious bodily
20 injuries, a substantial adverse impact on the na-
21 tional economy, or a substantial adverse impact on
22 national security.

23 (b) COOPERATION.—Such prioritization shall be de-
24 veloped in cooperation with other relevant Federal agen-



1 cies, State, local, and tribal governments, and the private
2 sector, as appropriate.

3 **SEC. 332. SECURITY REVIEW.**

4 (a) REQUIREMENT.—Not later than 9 months after
5 the date of the enactment of this Act, the Secretary, in
6 coordination with other relevant Federal agencies, State,
7 local, and tribal governments, and the private sector, as
8 appropriate, shall—

9 (1) review existing Federal, State, local, tribal,
10 and private sector plans for securing the critical in-
11 frastructure included in the prioritization developed
12 under section 331;

13 (2) recommend changes to existing plans for se-
14 curing such infrastructure, as the Secretary deter-
15 mines necessary; and

16 (3) coordinate and contribute to protective ef-
17 forts of other Federal, State, local, and tribal agen-
18 cies and the private sector, as appropriate, as di-
19 rected in Homeland Security Presidential Directive
20 7.

21 (b) CONTENTS OF PLANS.—The recommendations
22 made under subsection (a)(2) shall include—

23 (1) necessary protective measures to secure
24 such infrastructure, including milestones and time-
25 frames for implementation; and



1 (2) to the extent practicable, performance
2 metrics to evaluate the benefits to both national se-
3 curity and the Nation's economy from the implemen-
4 tation of such protective measures.

5 **SEC. 333. IMPLEMENTATION REPORT.**

6 (a) IN GENERAL.—Not later than 15 months after
7 the date of the enactment of this Act, the Secretary shall
8 submit a report to the Committee on Homeland Security
9 of the House of Representatives and the Committee on
10 Homeland Security and Governmental Affairs of the Sen-
11 ate on the implementation of section 332. Such report
12 shall detail—

13 (1) the Secretary's review and coordination of
14 security plans under section 332; and

15 (2) the Secretary's oversight of the execution
16 and effectiveness of such plans.

17 (b) UPDATE.—Not later than 1 year after the sub-
18 mission of the report under subsection (a), the Secretary
19 shall provide an update of such report to the congressional
20 committees described in subsection (a).

21 **SEC. 334. PROTECTION OF INFORMATION.**

22 Information that is generated, compiled, or dissemi-
23 nated by the Department of Homeland Security in car-
24 rying out this section—



1 (1) is exempt from disclosure under section 552
2 of title 5, United States Code; and

3 (2) shall not, if provided by the Department to
4 a State or local government or government agency—

5 (A) be made available pursuant to any
6 State or local law requiring disclosure of infor-
7 mation or records;

8 (B) otherwise be disclosed or distributed to
9 any person by such State or local government
10 or government agency without the written con-
11 sent of the Secretary; or

12 (C) be used other than for the purpose of
13 protecting critical infrastructure or protected
14 systems, or in furtherance of an investigation or
15 the prosecution of a criminal act.

16 **TITLE IV—MISCELLANEOUS**

17 **SEC. 401. BORDER SECURITY AND ENFORCEMENT COORDI-** 18 **NATION AND OPERATIONS.**

19 (a) FINDINGS.—The Congress makes the following
20 findings:

21 (1) In creating the Department of Homeland
22 Security, the Congress sought to enhance the Na-
23 tion's capabilities to prevent, protect against, and re-
24 spond to terrorist acts by consolidating existing Fed-
25 eral agencies with homeland security functions into



1 a single new Department, and by realigning the mis-
2 sions of those legacy agencies to more directly sup-
3 port our national homeland security efforts.

4 (2) As part of this massive government reorga-
5 nization, section 442 of the Homeland Security Act
6 of 2002 (Public Law 107–273) established a Bureau
7 of Border Security and transferred into it all of the
8 functions, programs, personnel, assets, and liabilities
9 pertaining to the following programs: the Border Pa-
10 trol; alien detention and removal; immigration-re-
11 lated intelligence, investigations, and enforcement
12 activities; and immigration inspections at ports of
13 entry.

14 (3) Title IV of the Homeland Security Act of
15 2002 (Public Law 107–273) also transferred to the
16 new Department the United States Customs Service,
17 as a distinct entity within the new Department, to
18 further the Department’s border integrity mission.

19 (4) Utilizing its reorganization authority pro-
20 vided in the Homeland Security Act of 2002, the
21 President submitted a reorganization plan for the
22 Department on January 30, 2003.

23 (5) This plan merged the customs and immigra-
24 tion border inspection and patrol functions, along
25 with agricultural inspections functions, into a new



1 entity called United States Customs and Border
2 Protection.

3 (6) The plan also combined the customs and
4 immigration enforcement agents, as well as the Of-
5 fice of Detention and Removal Operations, the Of-
6 fice of Federal Protective Service, the Office of Fed-
7 eral Air Marshal Service, and the Office of Intel-
8 ligence, into another new entity called United States
9 Immigration and Customs Enforcement.

10 (7) The President's January 30, 2003, reorga-
11 nization plan did not explain the reasons for sepa-
12 rating immigration inspection and border patrol
13 functions from other immigration-related enforce-
14 ment activities, which was contrary to the single Bu-
15 reau of Border Security as prescribed by the Con-
16 gress in the section 441 of the Homeland Security
17 Act of 2002.

18 (8) Two years after this structure has been in
19 effect, questions remain about whether the Depart-
20 ment has organized itself properly, and is managing
21 its customs and immigration enforcement and border
22 security resources in the most efficient, sensible, and
23 effective manner.

24 (9) The current structure has resulted in less
25 cooperation and information sharing between these



1 two critical functions than is desirable, and has
2 caused operational and administrative difficulties
3 that are hampering efforts to secure our borders and
4 ensure the integrity of our border control system.

5 (10) United States Immigration and Customs
6 Enforcement has faced major budgetary challenges
7 that are, in part, attributable to the inexact division
8 of resources upon the separation of immigration
9 functions. These budget shortfalls have forced
10 United States Immigration and Customs Enforce-
11 ment to impose hiring freezes and to release aliens
12 that otherwise should be detained.

13 (11) The current structure also has resulted in
14 unnecessary overlap and duplication between United
15 States Immigration and Customs Enforcement and
16 United States Customs and Border Protection, both
17 in the field and at the headquarters level. There are
18 intelligence, legislative affairs, public affairs, and
19 international affairs offices in both agencies.

20 (12) Border security and customs and immigra-
21 tion enforcement should be one seamless mission.

22 (b) REPORT.—

23 (1) IN GENERAL.—Not later than 30 days after
24 the date of the enactment of this Act, the Secretary
25 of Homeland Security shall review and evaluate the



1 current organizational structure of the Department
2 of Homeland Security established by the President's
3 January 30, 2003, reorganization plan and submit a
4 report of findings and recommendations to the Con-
5 gress.

6 (2) CONTENTS OF REPORT.—The report shall
7 include—

8 (A) a description of the rationale for, and
9 any benefits of, the current organizational divi-
10 sion of United States Immigration and Customs
11 Enforcement and United States Customs and
12 Border Protection, with respect to the Depart-
13 ment's immigration and customs missions;

14 (B) a description of the organization, mis-
15 sions, operations, and policies of United States
16 Customs and Border Protection and United
17 States Immigration and Customs Enforcement,
18 and areas of unnecessary overlap or operational
19 gaps among and between these missions;

20 (C) an analysis of alternative organiza-
21 tional structures that could provide a more ef-
22 fective way to deliver maximum efficiencies and
23 mission success;

24 (D) a description of the current role of the
25 Directorate of Border and Transportation Secu-



1 rity with respect to providing adequate direction
2 and oversight of the two agencies, and whether
3 this management structure is still necessary;

4 (E) an analysis of whether the Federal Air
5 Marshals and the Federal Protective Service are
6 properly located within the Department within
7 United States Immigration and Customs En-
8 forcement;

9 (F) the proper placement and functions of
10 a specialized investigative and patrol unit oper-
11 ating at the southwest border on the Tohono
12 O’odham Nation, known as the Shadow Wolves;

13 (G) the potential costs of reorganization,
14 including financial, programmatic, and other
15 costs, to the Department; and

16 (H) recommendations for correcting the
17 operational and administrative problems that
18 have been caused by the division of United
19 States Customs and Border Protection and
20 United States Immigration and Customs En-
21 forcement, including any appropriate reorga-
22 nization plans.

23 **SEC. 402. GAO REPORT TO CONGRESS.**

24 Not later than 6 months after the date of the enact-
25 ment of this Act, the Comptroller General of the United



1 States shall submit to the Congress a report that sets
2 forth—

3 (1) an assessment of the effectiveness of the or-
4 ganizational and management structure of the De-
5 partment of Homeland Security in meeting the De-
6 partment's missions; and

7 (2) recommendations to facilitate and improve
8 the organization and management of the Depart-
9 ment to best meet those missions.

10 **SEC. 403. PLAN FOR ESTABLISHING CONSOLIDATED AND**
11 **COLOCATED REGIONAL OFFICES.**

12 Not later than 60 days after the date of the enact-
13 ment of this Act, the Secretary of Homeland Security shall
14 develop and submit to the Congress a plan for establishing
15 consolidated and colocated regional offices for the Depart-
16 ment of Homeland Security in accordance with section
17 706 of the Homeland Security Act of 2002 (6 U.S.C.
18 346).

19 **SEC. 404. PLAN TO REDUCE WAIT TIMES.**

20 Not later than 180 days after the date of enactment
21 of this Act, the Secretary of Homeland Security shall de-
22 velop a plan—

23 (1) to improve the operational efficiency of se-
24 curity screening checkpoints at commercial service



1 airports so that average peak waiting periods at
2 such checkpoints do not exceed 20 minutes; and

3 (2) to ensure that there are no significant dis-
4 parities in immigration and customs processing
5 times among airports that serve as international
6 gateways.

7 **SEC. 405. DENIAL OF TRANSPORTATION SECURITY CARD.**

8 Section 70105(c) of title 46, United States Code, is
9 amended—

10 (1) in paragraph (3) by inserting before the pe-
11 riod “before an administrative law judge”; and

12 (2) by adding at the end the following:

13 “(5) In making a determination under paragraph
14 (1)(D), the Secretary shall not consider a felony conviction
15 if—

16 “(A) that felony occurred more than 7 years
17 prior to the date of the Secretary’s determination;
18 and

19 “(B) the felony was not related to terrorism (as
20 that term is defined in section 2 of the Homeland
21 Security Act of 2002 (6 U.S.C. 101)).”.



1 **SEC. 406. TRANSFER OF EXISTING CUSTOMS PATROL OFFI-**
2 **CERS UNIT AND ESTABLISHMENT OF NEW**
3 **CPO UNITS IN THE BUREAU OF IMMIGRATION**
4 **AND CUSTOMS ENFORCEMENT.**

5 (a) TRANSFER OF EXISTING UNIT.—Not later than
6 180 days after the date of the enactment of this Act, the
7 Secretary of Homeland Security shall transfer to the Bu-
8 reau of Immigration and Customs Enforcement all func-
9 tions (including the personnel, assets, and obligations held
10 by or available in connection with such functions) of the
11 Customs Patrol Officers unit of the Bureau of Customs
12 and Border Protection operating on the Tohono O’odham
13 Indian reservation (commonly known as the ‘Shadow
14 Wolves’ unit).

15 (b) ESTABLISHMENT OF NEW UNITS.—The Sec-
16 retary is authorized to establish within the Bureau of Im-
17 migration and Customs Enforcement additional units of
18 Customs Patrol Officers in accordance with this section.

19 (c) DUTIES.—The Secretary is authorized to estab-
20 lish within the Bureau of Immigration and Customs En-
21 forcement additional units of Customs Patrol Officers in
22 accordance with this section.

23 (d) BASIC PAY FOR JOURNEYMAN OFFICERS.—The
24 rate of basic pay for a journeyman Customs Patrol Officer
25 in a unit described in this section shall be not less than
26 the rate of basic pay for GS–13 of the General Schedule.



1 (e) SUPERVISORS.—Each unit described under this
2 section shall be supervised by a Chief Customs Patrol Offi-
3 cer, who shall have the same rank as a resident agent-
4 in-charge of the Office of Investigations.

