

**EN BLOC AMENDMENTS TO H.R. 5005, AS  
REPORTED  
OFFERED BY MR. ARMEY OF TEXAS**

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

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

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

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

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

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

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

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



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

Page 142, line 2, insert “including” before “interventions”.

Page 142, line 4, insert a comma after “asters”.

In section 811(f)(1)—

- (1) insert “or” before “Harbor”; and
- (2) strike “or Oil Spill Liability Trust Fund”.

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

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

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

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

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



In section 301—

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

(2) strike paragraph (9); and

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

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

**1 SEC. 309. TECHNOLOGY CLEARINGHOUSE TO ENCOURAGE  
2 AND SUPPORT INNOVATIVE SOLUTIONS TO  
3 ENHANCE HOMELAND SECURITY.**

4 (a) ESTABLISHMENT OF PROGRAM.—The Secretary,  
5 acting through the Under Secretary for Science and Tech-  
6 nology, shall establish and promote a program to encour-  
7 age technological innovation in facilitating the mission of  
8 the Department (as described in section 101).

9 (b) ELEMENTS OF PROGRAM.—The program de-  
10 scribed in subsection (a) shall include the following compo-  
11 nents:

12 (1) The establishment of a centralized Federal  
13 clearinghouse for information relating to tech-  
14 nologies that would further the mission of the De-  
15 partment for dissemination, as appropriate, to Fed-  
16 eral, State, and local government and private sector  
17 entities for additional review, purchase, or use.



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

4           (3) The establishment of a technical assistance  
5 team to assist in screening, as appropriate, pro-  
6 posals submitted to the Secretary (except as pro-  
7 vided in subsection (c)(2)) to assess the feasibility,  
8 scientific and technical merits, and estimated cost of  
9 such proposals, as appropriate.

10          (4) The provision of guidance, recommenda-  
11 tions, and technical assistance, as appropriate, to as-  
12 sist Federal, State, and local government and pri-  
13 vate sector efforts to evaluate and implement the use  
14 of technologies described in paragraph (1) or (2).

15          (5) The provision of information for persons  
16 seeking guidance on how to pursue proposals to de-  
17 velop or deploy technologies that would enhance  
18 homeland security, including information relating to  
19 Federal funding, regulation, or acquisition.

20          (c) MISCELLANEOUS PROVISIONS.—

21           (1) IN GENERAL.—Nothing in this section shall  
22 be construed as authorizing the Secretary or the  
23 technical assistance team established under sub-  
24 section (b)(3) to set standards for technology to be  
25 used by the Department, any other executive agency,



1 any State or local government entity, or any private  
2 sector entity.

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

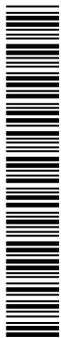
8 (3) COORDINATION.—In carrying out this sec-  
9 tion, the Secretary shall coordinate with the Tech-  
10 nical Support Working Group (organized under the  
11 April 1982 National Security Decision Directive  
12 Numbered 30).

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

13 **SEC. . ENHANCEMENT OF NON-FEDERAL**  
14 **CYBERSECURITY.**

15 In carrying out the responsibilities under section 201,  
16 the Under Secretary for Information Analysis and Infra-  
17 structure Protection shall—

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



1 (A) analysis and warnings related to  
2 threats to, and vulnerabilities of, critical infor-  
3 mation systems; and

4 (B) in coordination with the Under Sec-  
5 retary for Emergency Preparedness and Re-  
6 sponse, crisis management support in response  
7 to threats to, or attacks on, critical information  
8 systems; and

9 (2) as appropriate, provide technical assistance,  
10 upon request, to the private sector and other govern-  
11 ment entities, in coordination with the Under Sec-  
12 retary for Emergency Preparedness and Response,  
13 with respect to emergency recovery plans to respond  
14 to major failures of critical information systems.

At the end of title II add the following:

15 **SEC. . NET GUARD.**

16 The Under Secretary for Information Analysis and  
17 Infrastructure Protection may establish a national tech-  
18 nology guard, to be known as “NET Guard”, comprised  
19 of local teams of volunteers with expertise in relevant  
20 areas of science and technology, to assist local commu-  
21 nities to respond and recover from attacks on information  
22 systems and communications networks.



Strike section 814.

In section 761—

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

(2) in the proposed section 9701(e), strike “title” and insert “part”.

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

1 **SEC. 774. SENSE OF CONGRESS REAFFIRMING THE CONTIN-**  
2 **UED IMPORTANCE AND APPLICABILITY OF**  
3 **THE POSSE COMITATUS ACT.**

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

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

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



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

4           (4) Nevertheless, by its express terms, the  
5 Posse Comitatus Act is not a complete barrier to the  
6 use of the Armed Forces for a range of domestic  
7 purposes, including law enforcement functions, when  
8 the use of the Armed Forces is authorized by Act of  
9 Congress or the President determines that the use of  
10 the Armed Forces is required to fulfill the Presi-  
11 dent's obligations under the Constitution to respond  
12 promptly in time of war, insurrection, or other seri-  
13 ous emergency.

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

24           (b) SENSE OF CONGRESS.—The Congress reaffirms  
25 the continued importance of section 1385 of title 18,



1 United States Code, and it is the sense of the Congress  
 2 that nothing in this Act should be construed to alter the  
 3 applicability of such section to any use of the Armed  
 4 Forces as a posse comitatus to execute the laws.

Amend the heading for section 766 to read as follows:

**5 SEC. 766. REGULATORY AUTHORITY AND PREEMPTION.**

In section 766—

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

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

6 (b) PREEMPTION OF STATE OR LOCAL LAW.—Ex-  
 7 cept as otherwise provided in this Act, this Act preempts  
 8 no State or local law, except that any authority to preempt  
 9 State or local law vested in any Federal agency or official  
 10 transferred to the Department pursuant to this Act shall  
 11 be transferred to the Department effective on the date of  
 12 the transfer to the Department of that Federal agency or  
 13 official.

Page 31, after line 5, insert the following:



1 **SEC. 207. INFORMATION SECURITY.**

2 In carrying out the responsibilities under section 201,  
3 the Under Secretary for Information Analysis and Infra-  
4 structure Protection shall—

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

9 (A) analysis and warnings related to  
10 threats to, and vulnerabilities of, critical infor-  
11 mation systems; and

12 (B) in coordination with the Under Sec-  
13 retary for Emergency Preparedness and Re-  
14 sponse, crisis management support in response  
15 to threats to, or attacks on, critical information  
16 systems; and

17 (2) as appropriate, provide technical assistance,  
18 upon request, to the private sector and with other  
19 government entities, in coordination with the Under  
20 Secretary for Emergency Preparedness and Re-  
21 sponse, with respect to emergency recovery plans to  
22 respond to major failures of critical information sys-  
23 tems.

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



1           **TITLE XI—INFORMATION**  
2                           **SECURITY**

3   **SEC. 1101. INFORMATION SECURITY.**

4           (a) **SHORT TITLE.**—The amendments made by this  
5 title may be cited as the “Federal Information Security  
6 Management Act of 2002”.

7           (b) **INFORMATION SECURITY.**—

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

11                   **“SUBCHAPTER II—INFORMATION**  
12                                   **SECURITY**

13   **“§ 3531. Purposes**

14           “The purposes of this subchapter are to—

15                   “(1) provide a comprehensive framework for en-  
16                   suring the effectiveness of information security con-  
17                   trols over information resources that support Fed-  
18                   eral operations and assets;

19                   “(2) recognize the highly networked nature of  
20                   the current Federal computing environment and pro-  
21                   vide effective governmentwide management and over-  
22                   sight of the related information security risks, in-  
23                   cluding coordination of information security efforts  
24                   throughout the civilian, national security, and law  
25                   enforcement communities;



1           “(3) provide for development and maintenance  
2 of minimum controls required to protect Federal in-  
3 formation and information systems;

4           “(4) provide a mechanism for improved over-  
5 sight of Federal agency information security pro-  
6 grams;

7           “(5) acknowledge that commercially developed  
8 information security products offer advanced, dy-  
9 namic, robust, and effective information security so-  
10 lutions, reflecting market solutions for the protection  
11 of critical information infrastructures important to  
12 the national defense and economic security of the  
13 nation that are designed, built, and operated by the  
14 private sector; and

15           “(6) recognize that the selection of specific  
16 technical hardware and software information secu-  
17 rity solutions should be left to individual agencies  
18 from among commercially developed products.”.

19 **“§ 3532. Definitions**

20           “(a) IN GENERAL.—Except as provided under sub-  
21 section (b), the definitions under section 3502 shall apply  
22 to this subchapter.

23           “(b) ADDITIONAL DEFINITIONS.—As used in this  
24 subchapter—



1           “(1) the term ‘information security’ means pro-  
2           tecting information and information systems from  
3           unauthorized access, use, disclosure, disruption,  
4           modification, or destruction in order to provide—

5                   “(A) integrity, which means guarding  
6                   against improper information modification or  
7                   destruction, and includes ensuring information  
8                   nonrepudiation and authenticity;

9                   “(B) confidentiality, which means pre-  
10                  serving authorized restrictions on access and  
11                  disclosure, including means for protecting per-  
12                  sonal privacy and proprietary information;

13                  “(C) availability, which means ensuring  
14                  timely and reliable access to and use of infor-  
15                  mation; and

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

19           “(2) the term ‘national security system’ means  
20           any information system (including any telecommuni-  
21           cations system) used or operated by an agency or by  
22           a contractor of an agency, or other organization on  
23           behalf of an agency, the function, operation, or use  
24           of which—

25                   “(A) involves intelligence activities;



1           “(B) involves cryptologic activities related  
2 to national security;

3           “(C) involves command and control of mili-  
4 tary forces;

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

7           “(E) is critical to the direct fulfillment of  
8 military or intelligence missions provided that  
9 this definition does not apply to a system that  
10 is used for routine administrative and business  
11 applications (including payroll, finance, logis-  
12 tics, and personnel management applications);

13           “(3) the term ‘information technology’ has the  
14 meaning given that term in section 5002 of the  
15 Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

16           “(4) the term ‘information system’ means any  
17 equipment or interconnected system or subsystems  
18 of equipment that is used in the automatic acquisi-  
19 tion, storage, manipulation, management, movement,  
20 control, display, switching, interchange, trans-  
21 mission, or reception of data or information, and  
22 includes—

23           “(A) computers and computer networks;

24           “(B) ancillary equipment;



1                   “(C) software, firmware, and related proce-  
2                   dures;

3                   “(D) services, including support services;  
4                   and

5                   “(E) related resources.”.

6   **“§ 3533. Authority and functions of the Director**

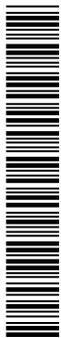
7                   “(a) The Director shall oversee agency information  
8 security policies and practices, by—

9                   “(1) promulgating information security stand-  
10                  ards under section 5131 of the Clinger-Cohen Act of  
11                  1996 (40 U.S.C. 1441);

12                  “(2) overseeing the implementation of policies,  
13                  principles, standards, and guidelines on information  
14                  security;

15                  “(3) requiring agencies, consistent with the  
16                  standards promulgated under such section 5131 and  
17                  the requirements of this subchapter, to identify and  
18                  provide information security protections commensu-  
19                  rate with the risk and magnitude of the harm result-  
20                  ing from the unauthorized access, use, disclosure,  
21                  disruption, modification, or destruction of—

22                                 “(A) information collected or maintained  
23                                 by or on behalf of an agency; or



1           “(B) information systems used or operated  
2           by an agency or by a contractor of an agency  
3           or other organization on behalf of an agency;

4           “(4) coordinating the development of standards  
5           and guidelines under section 20 of the National In-  
6           stitute of Standards and Technology Act (15 U.S.C.  
7           278g-3) with agencies and offices operating or exer-  
8           cising control of national security systems (including  
9           the National Security Agency) to assure, to the max-  
10          imum extent feasible, that such standards and  
11          guidelines are complementary with standards and  
12          guidelines developed for national security systems;

13          “(5) overseeing agency compliance with the re-  
14          quirements of this subchapter, including through  
15          any authorized action under section 5113(b)(5) of  
16          the Clinger-Cohen Act of 1996 (40 U.S.C.  
17          1413(b)(5)) to enforce accountability for compliance  
18          with such requirements;

19          “(6) reviewing at least annually, and approving  
20          or disapproving, agency information security pro-  
21          grams required under section 3534(b);

22          “(7) coordinating information security policies  
23          and procedures with related information resources  
24          management policies and procedures; and



1 “(8) reporting to Congress no later than March  
2 1 of each year on agency compliance with the re-  
3 quirements of this subchapter, including—

4 “(A) a summary of the findings of evalua-  
5 tions required by section 3535;

6 “(B) significant deficiencies in agency in-  
7 formation security practices;

8 “(C) planned remedial action to address  
9 such deficiencies; and

10 “(D) a summary of, and the views of the  
11 Director on, the report prepared by the Na-  
12 tional Institute of Standards and Technology  
13 under section 20(e)(7) of the National Institute  
14 of Standards and Technology Act (15 U.S.C.  
15 278g-3).”.

16 “(b) Except for the authorities described in para-  
17 graphs (4) and (7) of subsection (a), the authorities of  
18 the Director under this section shall not apply to national  
19 security systems.

20 **“§ 3534. Federal agency responsibilities**

21 “(a) The head of each agency shall—

22 “(1) be responsible for—

23 “(A) providing information security protec-  
24 tions commensurate with the risk and mag-  
25 nitude of the harm resulting from unauthorized



1 access, use, disclosure, disruption, modification,  
2 or destruction of—

3 “(i) information collected or main-  
4 tained by or on behalf of the agency; and

5 “(ii) information systems used or op-  
6 erated by an agency or by a contractor of  
7 an agency or other organization on behalf  
8 of an agency;

9 “(B) complying with the requirements of  
10 this subchapter and related policies, procedures,  
11 standards, and guidelines, including—

12 “(i) information security standards  
13 promulgated by the Director under section  
14 5131 of the Clinger-Cohen Act of 1996 (40  
15 U.S.C. 1441); and

16 “(ii) information security standards  
17 and guidelines for national security sys-  
18 tems issued in accordance with law and as  
19 directed by the President; and

20 “(C) ensuring that information security  
21 management processes are integrated with  
22 agency strategic and operational planning proc-  
23 esses;

24 “(2) ensure that senior agency officials provide  
25 information security for the information and infor-



1 information systems that support the operations and as-  
2 sets under their control, including through—

3 “(A) assessing the risk and magnitude of  
4 the harm that could result from the unauthor-  
5 ized access, use, disclosure, disruption, modi-  
6 fication, or destruction of such information or  
7 information systems;

8 “(B) determining the levels of information  
9 security appropriate to protect such information  
10 and information systems in accordance with  
11 standards promulgated under section 5131 of  
12 the Clinger-Cohen Act of 1996 (40 U.S.C.  
13 1441) for information security classifications  
14 and related requirements;

15 “(C) implementing policies and procedures  
16 to cost-effectively reduce risks to an acceptable  
17 level; and

18 “(D) periodically testing and evaluating in-  
19 formation security controls and techniques to  
20 ensure that they are effectively implemented;

21 “(3) delegate to the agency Chief Information  
22 Officer established under section 3506 (or com-  
23 parable official in an agency not covered by such  
24 section) the authority to ensure compliance with the



1 requirements imposed on the agency under this sub-  
2 chapter, including—

3 “(A) designating a senior agency informa-  
4 tion security officer who shall—

5 “(i) carry out the Chief Information  
6 Officer’s responsibilities under this section;

7 “(ii) possess professional qualifica-  
8 tions, including training and experience,  
9 required to administer the functions de-  
10 scribed under this section;

11 “(iii) have information security duties  
12 as that official’s primary duty; and

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

16 “(B) developing and maintaining an agen-  
17 cywide information security program as re-  
18 quired by subsection (b);

19 “(C) developing and maintaining informa-  
20 tion security policies, procedures, and control  
21 techniques to address all applicable require-  
22 ments, including those issued under section  
23 3533 of this title, and section 5131 of the  
24 Clinger-Cohen Act of 1996 (40 U.S.C. 1441);



1           “(D) training and overseeing personnel  
2           with significant responsibilities for information  
3           security with respect to such responsibilities;  
4           and

5           “(E) assisting senior agency officials con-  
6           cerning their responsibilities under subpara-  
7           graph (2);

8           “(4) ensure that the agency has trained per-  
9           sonnel sufficient to assist the agency in complying  
10          with the requirements of this subchapter and related  
11          policies, procedures, standards, and guidelines; and

12          “(5) ensure that the agency Chief Information  
13          Officer, in coordination with other senior agency of-  
14          ficials, reports annually to the agency head on the  
15          effectiveness of the agency information security pro-  
16          gram, including progress of remedial actions.

17          “(b) Each agency shall develop, document, and imple-  
18          ment an agencywide information security program, ap-  
19          proved by the Director under section 3533(a)(5), to pro-  
20          vide information security for the information and informa-  
21          tion systems that support the operations and assets of the  
22          agency, including those provided or managed by another  
23          agency, contractor, or other source, that includes—

24                 “(1) periodic assessments of the risk and mag-  
25                 nitude of the harm that could result from the unau-



1       thorized access, use, disclosure, disruption, modifica-  
2       tion, or destruction of information and information  
3       systems that support the operations and assets of  
4       the agency;

5               “(2) policies and procedures that—

6                       “(A) are based on the risk assessments re-  
7                       quired by subparagraph (1);

8                       “(B) cost-effectively reduce information se-  
9                       curity risks to an acceptable level;

10                      “(C) ensure that information security is  
11                      addressed throughout the life cycle of each  
12                      agency information system; and

13                      “(D) ensure compliance with—

14                               “(i) the requirements of this sub-  
15                               chapter;

16                               “(ii) policies and procedures as may  
17                               be prescribed by the Director, and infor-  
18                               mation security standards promulgated  
19                               under section 5131 of the Clinger-Cohen  
20                               Act of 1996 (40 U.S.C. 1441);

21                               “(iii) minimally acceptable system  
22                               configuration requirements, as determined  
23                               by the agency; and

24                               “(iv) any other applicable require-  
25                               ments, including standards and guidelines



1 for national security systems issued in ac-  
2 cordance with law and as directed by the  
3 President;

4 “(3) subordinate plans for providing adequate  
5 information security for networks, facilities, and sys-  
6 tems or groups of information systems, as appro-  
7 priate;

8 “(4) security awareness training to inform per-  
9 sonnel, including contractors and other users of in-  
10 formation systems that support the operations and  
11 assets of the agency, of—

12 “(A) information security risks associated  
13 with their activities; and

14 “(B) their responsibilities in complying  
15 with agency policies and procedures designed to  
16 reduce these risks;

17 “(5) periodic testing and evaluation of the ef-  
18 fectiveness of information security policies, proce-  
19 dures, and practices, to be performed with a fre-  
20 quency depending on risk, but no less than annually,  
21 of which such testing—

22 “(A) shall include testing of management,  
23 operational, and technical controls of every in-  
24 formation system identified in the inventory re-  
25 quired under section 3505(c); and



1           “(B) may include testing relied on in a  
2           evaluation under section 3535;

3           “(6) a process for planning, implementing, eval-  
4           uating, and documenting remedial action to address  
5           any deficiencies in the information security policies,  
6           procedures, and practices of the agency;

7           “(7) procedures for detecting, reporting, and re-  
8           sponding to security incidents, including—

9           “(A) mitigating risks associated with such  
10          incidents before substantial damage is done;  
11          and

12          “(B) notifying and consulting with, as  
13          appropriate—

14               “(i) law enforcement agencies and rel-  
15               evant Offices of Inspector General;

16               “(ii) an office designated by the Presi-  
17               dent for any incident involving a national  
18               security system; and

19               “(iii) any other agency or office, in ac-  
20               cordance with law or as directed by the  
21               President; and

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

25          “(c) Each agency shall—



1           “(1) report annually to the Director, the Com-  
2           mittees on Government Reform and Science of the  
3           House of Representatives, the Committees on Gov-  
4           ernmental Affairs and Commerce, Science, and  
5           Transportation of the Senate, the appropriate au-  
6           thorization and appropriations committees of Con-  
7           gress, and the Comptroller General on the adequacy  
8           and effectiveness of information security policies,  
9           procedures, and practices, and compliance with the  
10          requirements of this subchapter, including compli-  
11          ance with each requirement of subsection (b);

12           “(2) address the adequacy and effectiveness of  
13          information security policies, procedures, and prac-  
14          tices in plans and reports relating to—

15                   “(A) annual agency budgets;

16                   “(B) information resources management  
17                   under subchapter 1 of this chapter;

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

21                   “(D) program performance under sections  
22                   1105 and 1115 through 1119 of title 31, and  
23                   sections 2801 and 2805 of title 39;

24                   “(E) financial management under chapter  
25                   9 of title 31, and the Chief Financial Officers



1 Act of 1990 (31 U.S.C. 501 note; Public Law  
2 101–576) (and the amendments made by that  
3 Act);

4 “(F) financial management systems under  
5 the Federal Financial Management Improve-  
6 ment Act (31 U.S.C. 3512 note); and

7 “(G) internal accounting and administra-  
8 tive controls under section 3512 of title 31,  
9 United States Code, (known as the ‘Federal  
10 Managers Financial Integrity Act’); and

11 “(3) report any significant deficiency in a pol-  
12 icy, procedure, or practice identified under para-  
13 graph (1) or (2)—

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

17 “(B) if relating to financial management  
18 systems, as an instance of a lack of substantial  
19 compliance under the Federal Financial Man-  
20 agement Improvement Act (31 U.S.C. 3512  
21 note).

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



1           “(A) the time periods, and

2           “(B) the resources, including budget, staffing,  
3           and training,

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

6           “(2) The description under paragraph (1) shall be  
7 based on the risk assessments required under subsection  
8 (b)(2)(1).

9           “(e) Each agency shall provide the public with timely  
10 notice and opportunities for comment on proposed infor-  
11 mation security policies and procedures to the extent that  
12 such policies and procedures affect communication with  
13 the public.

14 **“§ 3535. Annual independent evaluation**

15           “(a)(1) Each year each agency shall have performed  
16 an independent evaluation of the information security pro-  
17 gram and practices of that agency to determine the effec-  
18 tiveness of such program and practices.

19           “(2) Each evaluation by an agency under this section  
20 shall include—

21           “(A) testing of the effectiveness of information  
22 security policies, procedures, and practices of a rep-  
23 resentative subset of the agency’s information sys-  
24 tems;



1           “(B) an assessment (made on the basis of the  
2 results of the testing) of compliance with—

3           “(i) the requirements of this subchapter;  
4           and

5           “(ii) related information security policies,  
6           procedures, standards, and guidelines; and

7           “(C) separate presentations, as appropriate, re-  
8           garding information security relating to national se-  
9           curity systems.

10          “(b) Subject to subsection (c)—

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

17           “(2) for each agency to which paragraph (1)  
18           does not apply, the head of the agency shall engage  
19           an independent external auditor to perform the eval-  
20           uation.

21          “(c) For each agency operating or exercising control  
22 of a national security system, that portion of the evalua-  
23 tion required by this section directly relating to a national  
24 security system shall be performed—



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

3           “(2) in such a manner as to ensure appropriate  
4           protection for information associated with any infor-  
5           mation security vulnerability in such system com-  
6           mensurate with the risk and in accordance with all  
7           applicable laws.

8           “(d) The evaluation required by this section—

9           “(1) shall be performed in accordance with gen-  
10          erally accepted government auditing standards; and

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

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

18          “(f) Agencies and evaluators shall take appropriate  
19          steps to ensure the protection of information which, if dis-  
20          closed, may adversely affect information security. Such  
21          protections shall be commensurate with the risk and com-  
22          ply with all applicable laws and regulations.

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



1           “(2) The Director’s report to Congress under this  
2 subsection shall summarize information regarding infor-  
3 mation security relating to national security systems in  
4 such a manner as to ensure appropriate protection for in-  
5 formation associated with any information security vulner-  
6 ability in such system commensurate with the risk and in  
7 accordance with all applicable laws.

8           “(3) Evaluations and any other descriptions of infor-  
9 mation systems under the authority and control of the Di-  
10 rector of Central Intelligence or of National Foreign Intel-  
11 ligence Programs systems under the authority and control  
12 of the Secretary of Defense shall be made available to Con-  
13 gress only through the appropriate oversight committees  
14 of Congress, in accordance with applicable laws.

15           “(h) The Comptroller General shall periodically  
16 evaluate and report to Congress on—

17                   “(1) the adequacy and effectiveness of agency  
18 information security policies and practices; and

19                   “(2) implementation of the requirements of this  
20 subchapter.

21   **“§ 3536. National security systems**

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



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

6           “(2) implements information security policies  
7           and practices as required by standards and guide-  
8           lines for national security systems, issued in accord-  
9           ance with law and as directed by the President; and

10          “(3) complies with the requirements of this sub-  
11          chapter.

12          **“§ 3537. Authorization of appropriations**

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

16          **“§ 3538. Effect on existing law**

17          “Nothing in this subchapter, section 5131 of the  
18          Clinger-Cohen Act of 1996 (40 U.S.C. 1441), or section  
19          20 of the National Standards and Technology Act (15  
20          U.S.C. 278g-3) may be construed as affecting the author-  
21          ity of the President, the Office of Management and Budg-  
22          et or the Director thereof, the National Institute of Stand-  
23          ards and Technology, or the head of any agency, with re-  
24          spect to the authorized use or disclosure of information,  
25          including with regard to the protection of personal privacy



1 under section 552a of title 5, the disclosure of information  
2 under section 552 of title 5, the management and disposi-  
3 tion of records under chapters 29, 31, or 33 of title 44,  
4 the management of information resources under sub-  
5 chapter I of chapter 35 of this title, or the disclosure of  
6 information to the Congress or the Comptroller General  
7 of the United States.”.

8 (2) CLERICAL AMENDMENT.—The items in the  
9 table of sections at the beginning of such chapter 35  
10 under the heading “SUBCHAPTER II” are amend-  
11 ed to read as follows:

“3531. Purposes.

“3532. Definitions.

“3533. Authority and functions of the Director.

“3534. Federal agency responsibilities.

“3535. Annual independent evaluation.

“3536. National security systems.

“3537. Authorization of appropriations.

“3538. Effect on existing law.”.

12 (c) INFORMATION SECURITY RESPONSIBILITIES OF  
13 CERTAIN AGENCIES.—

14 (1) NATIONAL SECURITY RESPONSIBILITIES.—

15 (A) Nothing in this Act (including any amendment  
16 made by this Act) shall supersede any authority of  
17 the Secretary of Defense, the Director of Central In-  
18 telligence, or other agency head, as authorized by  
19 law and as directed by the President, with regard to  
20 the operation, control, or management of national



1 security systems, as defined by section 3532(3) of  
2 title 44, United States Code.

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

5 (i) in subsection 2224(b), by striking “(b)  
6 OBJECTIVES AND MINIMUM REQUIREMENTS.—  
7 (1)” and inserting “(b) OBJECTIVES OF THE  
8 PROGRAM.—”;

9 (ii) in subsection 2224(b), by striking “(2)  
10 the program shall at a minimum meet the re-  
11 quirements of section 3534 and 3535 of title  
12 44, United States Code.”; and

13 (iii) in subsection 2224(c), by inserting  
14 “, including through compliance with subtitle II  
15 of chapter 35 of title 44” after “infrastruc-  
16 ture”.

17 (2) ATOMIC ENERGY ACT OF 1954.—Nothing in  
18 this Act shall supersede any requirement made by or  
19 under the Atomic Energy Act of 1954 (42 U.S.C.  
20 2011 et seq.). Restricted Data or Formerly Re-  
21 stricted Data shall be handled, protected, classified,  
22 downgraded, and declassified in conformity with the  
23 Atomic Energy Act of 1954 (42 U.S.C. 2011 et  
24 seq.).



1 **SEC. 1102. MANAGEMENT OF INFORMATION TECHNOLOGY.**

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

4 **“SEC. 5131. RESPONSIBILITIES FOR FEDERAL INFORMA-**  
5 **TION SYSTEMS STANDARDS.**

6 “(a)(1)(A) Except as provided under paragraph (2),  
7 the Director of the Office of Management and Budget  
8 shall, on the basis of proposed standards developed by the  
9 National Institute of Standards and Technology pursuant  
10 to paragraphs (2) and (3) of section 20(a) of the National  
11 Institute of Standards and Technology Act (15 U.S.C.  
12 278g–3(a)) and in consultation with the Secretary of  
13 Homeland Security, promulgate information security  
14 standards pertaining to Federal information systems.

15 “(B) Standards promulgated under subparagraph  
16 (A) shall include—

17 “(i) standards that provide minimum informa-  
18 tion security requirements as determined under sec-  
19 tion 20(b) of the National Institute of Standards  
20 and Technology Act (15 U.S.C. 278g–3(b)); and

21 “(ii) such standards that are otherwise nec-  
22 essary to improve the efficiency of operation or secu-  
23 rity of Federal information systems.

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



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

6           “(b) The head of an agency may employ standards  
7 for the cost-effective information security for all oper-  
8 ations and assets within or under the supervision of that  
9 agency that are more stringent than the standards pro-  
10 mulgated by the Director under this section, if such  
11 standards—

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

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

18           “(c)(1) The decision regarding the promulgation of  
19 any standard by the Director under subsection (a) shall  
20 occur not later than 6 months after the submission of the  
21 proposed standard to the Director by the National Insti-  
22 tute of Standards and Technology, as provided under sec-  
23 tion 20 of the National Institute of Standards and Tech-  
24 nology Act (15 U.S.C. 278g-3).



1           “(2) A decision by the Director to significantly mod-  
2 ify, or not promulgate, a proposed standard submitted to  
3 the Director by the National Institute of Standards and  
4 Technology, as provided under section 20 of the National  
5 Institute of Standards and Technology Act (15 U.S.C.  
6 278g-3), shall be made after the public is given an oppor-  
7 tunity to comment on the Director’s proposed decision.”.

8           “(d) In this section, the term ‘information security’  
9 has the meaning given that term in section 3532(b)(1) of  
10 title 44, United States Code.”.

11 **SEC. 1103. NATIONAL INSTITUTE OF STANDARDS AND**  
12 **TECHNOLOGY.**

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

16           “(a) The Institute shall—

17                   “(1) have the mission of developing standards,  
18 guidelines, and associated methods and techniques  
19 for information systems;

20                   “(2) develop standards and guidelines, includ-  
21 ing minimum requirements, for information systems  
22 used or operated by an agency or by a contractor of  
23 an agency or other organization on behalf of an  
24 agency, other than national security systems (as de-



1        fined in section 3532(b)(2) of title 44, United States  
2        Code);

3            “(3) develop standards and guidelines, includ-  
4        ing minimum requirements, for providing adequate  
5        information security for all agency operations and  
6        assets, but such standards and guidelines shall not  
7        apply to national security systems; and

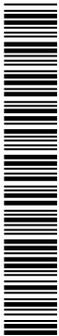
8            “(4) carry out the responsibilities described in  
9        paragraph (3) through the Computer Security Divi-  
10       sion.

11        “(b) The standards and guidelines required by sub-  
12       section (a) shall include, at a minimum—

13            “(1)(A) standards to be used by all agencies to  
14        categorize all information and information systems  
15        collected or maintained by or on behalf of each agen-  
16        cy based on the objectives of providing appropriate  
17        levels of information security according to a range of  
18        risk levels;

19            “(B) guidelines recommending the types of in-  
20        formation and information systems to be included in  
21        each such category; and

22            “(C) minimum information security require-  
23        ments for information and information systems in  
24        each such category;



1           “(2) a definition of and guidelines concerning  
2           detection and handling of information security inci-  
3           dents; and

4           “(3) guidelines developed in coordination with  
5           the National Security Agency for identifying an in-  
6           formation system as a national security system con-  
7           sistent with applicable requirements for national se-  
8           curity systems, issued in accordance with law and as  
9           directed by the President.

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

12                 “(1) consult with other agencies and offices (in-  
13                 cluding, but not limited to, the Director of the Office  
14                 of Management and Budget, the Departments of  
15                 Defense and Energy, the National Security Agency,  
16                 the General Accounting Office, and the Secretary of  
17                 Homeland Security) to assure—

18                         “(A) use of appropriate information secu-  
19                         rity policies, procedures, and techniques, in  
20                         order to improve information security and avoid  
21                         unnecessary and costly duplication of effort;  
22                         and

23                         “(B) that such standards and guidelines  
24                         are complementary with standards and guide-  
25                         lines employed for the protection of national se-



1 security systems and information contained in  
2 such systems;

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

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

9 “(A) standards, as required under sub-  
10 section (b)(1)(A), no later than 12 months after  
11 the date of the enactment of this section; and

12 “(B) minimum information security re-  
13 quirements for each category, as required under  
14 subsection (b)(1)(C), no later than 36 months  
15 after the date of the enactment of this section;

16 “(4) issue guidelines as required under sub-  
17 section (b)(1)(B), no later than 18 months after the  
18 date of the enactment of this Act;

19 “(5) ensure that such standards and guidelines  
20 do not require specific technological solutions or  
21 products, including any specific hardware or soft-  
22 ware security solutions;

23 “(6) ensure that such standards and guidelines  
24 provide for sufficient flexibility to permit alternative



1 solutions to provide equivalent levels of protection  
2 for identified information security risks; and

3 “(7) use flexible, performance-based standards  
4 and guidelines that, to the greatest extent possible,  
5 permit the use of off-the-shelf commercially devel-  
6 oped information security products.”

7 “(d) The Institute shall—

8 “(1) submit standards developed pursuant to  
9 subsection (a), along with recommendations as to  
10 the extent to which these should be made compul-  
11 sory and binding, to the Director of the Office of  
12 Management and Budget for promulgation under  
13 section 5131 of the Clinger-Cohen Act of 1996 (40  
14 U.S.C. 1441);

15 “(2) provide assistance to agencies regarding—

16 “(A) compliance with the standards and  
17 guidelines developed under subsection (a);

18 “(B) detecting and handling information  
19 security incidents; and

20 “(C) information security policies, proce-  
21 dures, and practices;

22 “(3) conduct research, as needed, to determine  
23 the nature and extent of information security  
24 vulnerabilities and techniques for providing cost-ef-  
25 fective information security;



1           “(4) develop and periodically revise performance  
2 indicators and measures for agency information se-  
3 curity policies and practices;

4           “(5) evaluate private sector information secu-  
5 rity policies and practices and commercially available  
6 information technologies to assess potential applica-  
7 tion by agencies to strengthen information security;

8           “(6) evaluate security policies and practices de-  
9 veloped for national security systems to assess po-  
10 tential application by agencies to strengthen infor-  
11 mation security;

12           “(7) periodically assess the effectiveness of  
13 standards and guidelines developed under this sec-  
14 tion and undertake revisions as appropriate;

15           “(8) solicit and consider the recommendations  
16 of the Information Security and Privacy Advisory  
17 Board, established by section 21, regarding stand-  
18 ards and guidelines developed under subsection (a)  
19 and submit such recommendations to the Director of  
20 the Office of Management and Budget with such  
21 standards submitted to the Director; and

22           “(9) prepare an annual public report on activi-  
23 ties undertaken in the previous year, and planned  
24 for the coming year, to carry out responsibilities  
25 under this section.



1 “(e) As used in this section—

2 “(1) the term ‘agency’ has the same meaning as  
3 provided in section 3502(1) of title 44, United  
4 States Code;

5 “(2) the term ‘information security’ has the  
6 same meaning as provided in section 3532(1) of  
7 such title;

8 “(3) the term ‘information system’ has the  
9 same meaning as provided in section 3502(8) of  
10 such title;

11 “(4) the term ‘information technology’ has the  
12 same meaning as provided in section 5002 of the  
13 Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

14 “(5) the term ‘national security system’ has the  
15 same meaning as provided in section 3532(b)(2) of  
16 such title.”.

17 **SEC. 1104. INFORMATION SECURITY AND PRIVACY ADVI-**  
18 **SORY BOARD.**

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

21 (1) in subsection (a), by striking “Computer  
22 System Security and Privacy Advisory Board” and  
23 inserting “Information Security and Privacy Advi-  
24 sory Board”;



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

4           (3) in subsection (a)(2)—

5                 (A) by striking “computer or telecommuni-  
6                 cations technology” and inserting “information  
7                 technology”; and

8                 (B) by striking “computer or telecommuni-  
9                 cations equipment” and inserting “information  
10                technology”;

11           (4) in subsection (a)(3)—

12                 (A) by striking “computer systems” and  
13                 inserting “information system”; and

14                 (B) by striking “computer systems secu-  
15                 rity” and inserting “information security”;

16           (5) in subsection (b)(1) by striking “computer  
17           systems security” and inserting “information secu-  
18           rity”;

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

21                 “(2) to advise the Institute and the Director of  
22                 the Office of Management and Budget on informa-  
23                 tion security and privacy issues pertaining to Fed-  
24                 eral Government information systems, including



1 through review of proposed standards and guidelines  
2 developed under section 20; and”;

3 (7) in subsection (b)(3) by inserting “annually”  
4 after “report”;

5 (8) by inserting after subsection (e) the fol-  
6 lowing new subsection:

7 “(f) The Board shall hold meetings at such locations  
8 and at such time and place as determined by a majority  
9 of the Board.”;

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

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

14 “(h) As used in this section, the terms “information  
15 system” and “information technology” have the meanings  
16 given in section 20.”.

17 **SEC. 1105. TECHNICAL AND CONFORMING AMENDMENTS.**

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

21 (b) **FLOYD D. SPENCE NATIONAL DEFENSE AU-**  
22 **THORIZATION ACT FOR FISCAL YEAR 2001.**—The Floyd  
23 D. Spence National Defense Authorization Act for Fiscal  
24 Year 2001 (Public Law 106–398) is amended by striking  
25 subtitle G of title X.



1 (c) PAPERWORK REDUCTION ACT.—(1) Section  
2 3504(g) of title 44, United States Code, is amended—

3 (A) by adding “and” at the end of paragraph  
4 (1);

5 (B) in paragraph (2)—

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

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

12 (C) by striking paragraph (3).

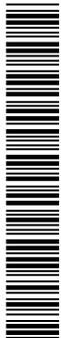
13 (2) Section 3505 of such title is amended by adding  
14 at the end—

15 “(c)(1) The head of each agency shall develop and  
16 maintain an inventory of the information systems (includ-  
17 ing national security systems) operated by or under the  
18 control of such agency;

19 “(2) The identification of information systems in an  
20 inventory under this subsection shall include an identifica-  
21 tion of the interfaces between each such system and all  
22 other systems or networks, including those not operated  
23 by or under the control of the agency;

24 “(3) Such inventory shall be—

25 “(A) updated at least annually;



1           “(B) made available to the Comptroller Gen-  
2           eral; and

3           “(C) used to support information resources  
4           management, including—

5                   “(i) preparation and maintenance of the  
6                   inventory of information resources under sec-  
7                   tion 3506(b)(4);

8                   “(ii) information technology planning,  
9                   budgeting, acquisition, and management under  
10                  section 3506(h), the Clinger-Cohen Act of  
11                  1996, and related laws and guidance;

12                  “(iii) monitoring, testing, and evaluation of  
13                  information security controls under subchapter  
14                  II;

15                  “(iv) preparation of the index of major in-  
16                  formation systems required under section  
17                  552(g) of title 5, United States Code; and

18                  “(v) preparation of information system in-  
19                  ventories required for records management  
20                  under chapters 21, 29, 31, and 33.

21           “(4) The Director shall issue guidance for and over-  
22           see the implementation of the requirements of this sub-  
23           section.”.

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



1 (A) by adding “and” at the end of paragraph  
2 (1);

3 (B) in paragraph (2)—

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

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

9 (C) by striking paragraph (3).

10 **SEC. 1106. CONSTRUCTION.**

11 Nothing in this Act, or the amendments made by this  
12 Act, affects the authority of the National Institute of  
13 Standards and Technology or the Department of Com-  
14 merce relating to the development and promulgation of  
15 standards or guidelines under paragraphs (1) and (2) of  
16 section 20(a) of the National Institute of Standards and  
17 Technology Act (15 U.S.C. 278g-3(a)).

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

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

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

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



1           (7) Anti-terrorism technology that would be ef-  
2           fective in facilitating the defense against acts of ter-  
3           rorism.

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

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

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

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

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

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

Page 182, line 2, strike “and” and insert “or”.

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



1 **SEC. 774. AIR TRANSPORTATION SAFETY AND SYSTEM STA-**  
2 **BILIZATION ACT AMENDMENTS.**

3 The Air Transportation Safety and System Stabiliza-  
4 tion Act (49 U.S.C. 40101 note) is amended—

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

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

9 “(1) AIR CARRIER.—The term ‘air carrier’  
10 means a citizen of the United States undertaking by  
11 any means, directly or indirectly, to provide air  
12 transportation and includes employees and agents  
13 (including persons engaged in the business of pro-  
14 viding air transportation security and their affili-  
15 ates) of such citizen. For purposes of the preceding  
16 sentence, the term ‘agent’, as applied to persons en-  
17 gaged in the business of providing air transportation  
18 security, shall only include persons that have con-  
19 tracted directly with the Federal Aviation Adminis-  
20 tration on or after February 17, 2002, to provide  
21 such security, or are not debarred.”.

Page 12, line 5, strike “and”.

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

Page 12, after line 9, insert the following:



1 (G) monitor connections between illegal  
 2 drug trafficking and terrorism, coordinate ef-  
 3 forts to sever such connections, and otherwise  
 4 contribute to efforts to interdict illegal drug  
 5 trafficking.

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

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

(2) serve as the United States Interdiction Co-  
 ordinator for the Director of National Drug Control  
 Policy.”.

In section 307(b)(1)—

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

(2) redesignate subparagraph (B) as subpara-  
 graph (C); and

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

6 (B) ensure that the research funded is of high  
 7 quality, as determined through merit review proc-  
 8 esses developed under section 301(10); and



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

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

1 **SEC. 506. SENSE OF CONGRESS REGARDING FUNDING OF**  
2 **TRAUMA SYSTEMS.**

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

