

109TH CONGRESS
2^D SESSION

H. R. 5001

To amend the Homeland Security Act of 2002 to enhance homeland security information sharing, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 16, 2006

Mr. SIMMONS (for himself and Ms. ZOE LOFGREN of California) introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To amend the Homeland Security Act of 2002 to enhance homeland security information sharing, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Homeland Security
5 Information Sharing Enhancement Act of 2006”.

6 **SEC. 2. FINDINGS ON DISSEMINATION OF HOMELAND SE-**
7 **CURITY-RELATED INFORMATION.**

8 Congress finds the following:

9 (1) Section 201(d)(1) of the Homeland Security
10 Act of 2002 gives the Department of Homeland Se-

1 curity authority to access, receive, and analyze law
2 enforcement information, intelligence information,
3 and other information from Federal, State, and local
4 government agencies—including law enforcement
5 agencies—and to integrate such information in order
6 to detect, identify, and assess terrorist threats to the
7 homeland.

8 (2) Section 201(d)(4) of the Homeland Security
9 Act of 2002 likewise gives the Department the power
10 to ensure “timely and efficient access” to these cat-
11 egories of information in order to effectively dis-
12 charge its information sharing responsibilities.

13 (3) Section 102A(f)(1)(B)(iii) of the National
14 Security Act of 1947 (50 U.S.C. 403–
15 1(f)(1)(B)(iii)), as amended by section 1011 of the
16 Intelligence Reform and Terrorism Prevention Act
17 of 2004, prohibits the Director of National Intel-
18 ligence from disseminating information directly to
19 State and local government officials.

20 (4) Under section 119(f)(1)(E) of the National
21 Security Act of 1947 (50 U.S.C. 404o(f)(1)(E)), as
22 amended, the Director of the National
23 Counterterrorism Center supports the responsibil-
24 ities of the Department of Homeland Security to dis-
25 seminate terrorism information.

1 (5) Section 201(d)(9) of the Homeland Security
2 Act of 2002 gives the Department of Homeland Se-
3 curity the responsibility to disseminate information
4 analyzed by the Department to other Federal, State,
5 and local agencies with responsibilities relating to
6 homeland security “in order to assist in the deter-
7 rence, prevention, preemption of, or response to, ter-
8 rorist attacks. . .”.

9 (6) Section 201(d)(11) of the Homeland Secu-
10 rity Act of 2002 (6 U.S.C. 121(d)(11)) explicitly
11 gives the Department the responsibility to ensure
12 “appropriate exchanges of information, including law
13 enforcement-related information, relating to threats
14 of terrorism against the United States”.

15 (7) Section 201(d)(14) of the Homeland Secu-
16 rity Act of 2002 gives the Department the responsi-
17 bility “to establish and utilize . . . a secure commu-
18 nications and information technology infrastructure
19 . . . in order to access, receive, and analyze data”
20 and to disseminate that data to State, local, and
21 tribal law enforcement agencies as appropriate.

22 **SEC. 3. HOMELAND SECURITY ADVISORY SYSTEM.**

23 (a) IN GENERAL.—Subtitle A of title II of the Home-
24 land Security Act of 2002 is amended by adding at the
25 end the following:

1 **“SEC. 203. HOMELAND SECURITY ADVISORY SYSTEM.**

2 “(a) REQUIREMENT.—The Under Secretary for In-
3 formation and Analysis shall implement a Homeland Secu-
4 rity Advisory System in accordance with this section to
5 provide public advisories and alerts regarding threats to
6 homeland security, including national, regional, local, and
7 economic sector advisories and alerts, as appropriate.

8 “(b) REQUIRED ELEMENTS.—The Under Secretary,
9 under the System—

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

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

17 “(3) shall not, in issuing any advisory or alert,
18 use color designations as the exclusive means of
19 specifying the homeland security threat conditions
20 that are the subject of the advisory or alert.”.

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

“Sec. 203. Homeland Security Advisory System.”.

1 **SEC. 4. HOMELAND SECURITY INFORMATION SHARING.**

2 (a) IN GENERAL.—Subtitle A of title II of the Home-
3 land Security Act of 2002 (6 U.S.C. 121 et seq.), as
4 amended by section 3, is further amended by adding at
5 the end the following:

6 **“SEC. 204. HOMELAND SECURITY INFORMATION SHARING.**

7 “(a) INFORMATION SHARING ENVIRONMENT.—Con-
8 sistent with section 1016 of the National Intelligence Re-
9 form and Terrorism Prevention Act of 2004 (6 U.S.C.
10 485), the Secretary shall integrate and standardize the in-
11 formation of the intelligence components of the Depart-
12 ment into a Department information sharing environment,
13 to be administered by the Under Secretary for Intelligence
14 and Analysis.

15 “(b) INFORMATION SHARING AND KNOWLEDGE
16 MANAGEMENT OFFICERS.—For each intelligence compo-
17 nent of the Department, the Secretary shall designate an
18 information sharing and knowledge management officer
19 who shall report to the Under Secretary for Intelligence
20 and Analysis with respect to coordinating the different
21 systems used in the Department to gather and disseminate
22 homeland security information.

23 “(c) STATE, LOCAL, AND PRIVATE-SECTOR SOURCES
24 OF INFORMATION.—

25 “(1) ESTABLISHMENT OF BUSINESS PROC-
26 ESSES.—The Under Secretary for Intelligence and

1 Analysis shall establish Department-wide procedures
2 for the review and analysis of information gathered
3 from State, local, tribal, and private-sector sources
4 and, as appropriate, integrate such information into
5 the information gathered by the Department and
6 other department and agencies of the Federal Gov-
7 ernment.

8 “(2) FEEDBACK.—The Secretary shall develop
9 mechanisms to provide analytical and operational
10 feedback to any State, local, tribal, and private-sec-
11 tor entities that gather information and provide such
12 information to the Secretary.

13 “(d) TRAINING AND EVALUATION OF EMPLOYEES.—

14 “(1) TRAINING.—The Under Secretary shall
15 provide to employees of the Department opportuni-
16 ties for training and education to develop an under-
17 standing of the definition of homeland security infor-
18 mation, how information available to them as part of
19 their duties might qualify as homeland security in-
20 formation, and how information available to them is
21 relevant to the Office of Intelligence and Analysis.

22 “(2) EVALUATIONS.—The Under Secretary
23 shall, on an ongoing basis, evaluate how employees
24 of the Office of Intelligence and Analysis and the in-
25 telligence components of the Department are uti-

1 lizing homeland security information and partici-
2 pating in the Department information sharing envi-
3 ronment.”.

4 (b) CLERICAL AMENDMENT.—The table of contents
5 in section 1(b) of such Act is further amended by adding
6 at the end of the items relating to such subtitle the fol-
7 lowing:

“Sec. 204. Homeland security information sharing.”.

8 (c) ESTABLISHMENT OF COMPREHENSIVE INFORMA-
9 TION TECHNOLOGY NETWORK ARCHITECTURE.—

10 (1) IN GENERAL.—Subtitle A of title II of the
11 Homeland Security Act of 2002 (6 U.S.C. 121 et
12 seq.) is amended by adding at the end the following
13 new section:

14 **“SEC. 205. COMPREHENSIVE INFORMATION TECHNOLOGY**
15 **NETWORK ARCHITECTURE.**

16 “(a) ESTABLISHMENT.—The Secretary, acting
17 through the Chief Intelligence Officer, shall establish a
18 comprehensive information technology network architec-
19 ture for the Office of Intelligence and Analysis.

20 “(b) NETWORK MODEL.—The comprehensive infor-
21 mation technology network architecture established under
22 subsection (a) shall, to the extent possible, incorporate the
23 approaches, features, and functions of the network pro-
24 posed by the Markle Foundation in reports issued in Octo-
25 ber 2002 and December 2003, known as the System-wide

1 Homeland Security Analysis and Resource Exchange
2 (SHARE) Network.

3 “(c) COMPREHENSIVE INFORMATION TECHNOLOGY
4 NETWORK ARCHITECTURE DEFINED.—the term ‘com-
5 prehensive information technology network architecture’
6 means an integrated framework for evolving or maintain-
7 ing existing information technology and acquiring new in-
8 formation technology to achieve the strategic goals and in-
9 formation resources management goals of the Office of In-
10 formation and Analysis.”.

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

“Sec. 205. Comprehensive information technology network architecture.”.

15 (3) REPORTS.—

16 (A) REPORT ON IMPLEMENTATION OF
17 PLAN.—Not later than 360 days after the date
18 of the enactment of this Act, the Secretary of
19 Homeland Security shall submit to the Com-
20 mittee on Homeland Security and Govern-
21 mental Affairs of the Senate and the Committee
22 on Homeland Security of the House of Rep-
23 resentatives a report containing a plan to imple-
24 ment the comprehensive information technology
25 network architecture for the Office of Intel-

1 ligence and Analysis of the Department of
2 Homeland Security required under section 209
3 of the Homeland Security Act of 2002, as
4 added by paragraph (1). Such report shall in-
5 clude the following:

6 (i) Priorities for the development of
7 the comprehensive information technology
8 network architecture and a rationale for
9 such priorities.

10 (ii) An explanation of how the various
11 components of the comprehensive informa-
12 tion technology network architecture will
13 work together and interconnect.

14 (iii) A description of the technology
15 challenges that the Office of Intelligence
16 and Analysis will face in implementing the
17 comprehensive information technology net-
18 work architecture.

19 (iv) A description of technology op-
20 tions that are available or are in develop-
21 ment that may be incorporated into the
22 comprehensive technology network archi-
23 tecture, the feasibility of incorporating
24 such options, and the advantages and dis-
25 advantages of doing so.

1 (v) An explanation of any security
2 protections to be developed as part of the
3 comprehensive information technology net-
4 work architecture.

5 (vi) A description of any safeguards
6 for civil liberties and privacy to be built
7 into the comprehensive information tech-
8 nology network architecture.

9 (vii) An operational best practices
10 plan.

11 (B) PROGRESS REPORT.—Not later than
12 180 days after the date on which the report is
13 submitted under subparagraph (A), the Sec-
14 retary of Homeland Security shall submit to the
15 Committee on Homeland Security and Govern-
16 mental Affairs of the Senate and the Committee
17 on Homeland Security of the House of Rep-
18 resentatives a report on the progress of the Sec-
19 retary in developing the comprehensive informa-
20 tion technology network architecture required
21 under section 209 of the Homeland Security
22 Act of 2002, as added by paragraph (1).

23 (d) INTELLIGENCE COMPONENT DEFINED.—Section
24 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)

1 is amended by adding at the end the following new para-
2 graph:

3 “(17) The term ‘intelligence component of the
4 Department’ means any directorate, agency, or ele-
5 ment of the Department that gathers, receives, ana-
6 lyzes, produces, or disseminates homeland security
7 information except—

8 “(A) a directorate, agency, or element of
9 the Department that is required to be main-
10 tained as a distinct entity under this Act; or

11 “(B) any personnel security, physical secu-
12 rity, document security, or communications se-
13 curity program within any directorate, agency,
14 or element of the Department.”.

15 **SEC. 5. AUTHORITY FOR DISSEMINATING HOMELAND SECU-**
16 **RITY-RELATED INFORMATION.**

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

20 **“SEC. 104. AUTHORITY FOR DISSEMINATING HOMELAND SE-**
21 **CURITY-RELATED INFORMATION.**

22 “(a) PRIMARY AUTHORITY.—Except as provided in
23 subsection (b), the Secretary or the Secretary’s designee
24 shall be the executive branch official responsible for dis-
25 seminating homeland security-related terrorist threat in-

1 formation to State and local government and tribal offi-
2 cials and the private sector.

3 “(b) PRIOR APPROVAL REQUIRED.—No Federal offi-
4 cial may issue any homeland security-related analysis, ad-
5 visory, or alert without the Secretary’s prior approval, ex-
6 cept—

7 “(1) in exigent circumstances under which it is
8 essential that the information be communicated im-
9 mediately; or

10 “(2) when such analysis advisory or alert is
11 issued to Federal, State, local, or tribal law enforce-
12 ment officials for the purpose of assisting them in
13 any aspect of the administration of criminal jus-
14 tice.”.

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 such title the following:

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

○