

107TH CONGRESS  
2D SESSION

# S. 2629

To provide for an agency assessment, independent review, and Inspector General report on privacy and data protection policies of Federal agencies, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

JUNE 17, 2002

Mr. DASCHLE (for Mr. TORRICELLI) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

---

## A BILL

To provide for an agency assessment, independent review, and Inspector General report on privacy and data protection policies of Federal agencies, 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. PRIVACY AND DATA PROTECTION POLICIES OF**  
4 **FEDERAL AGENCIES.**

5 (a) SHORT TITLE.—This Act may be cited as the  
6 “Federal Privacy and Data Protection Policy Act of  
7 2002”.

1 (b) DEFINITIONS.—In this Act, the term “agency”  
2 has the meaning given that term under section 551(1) of  
3 title 5, United States Code.

4 (c) FINDINGS.—Congress finds that—

5 (1) in the wake of the attacks on the United  
6 States on September 11, 2001, Federal agencies are  
7 collecting an increasing amount of personal informa-  
8 tion from and on individuals as part of the expanded  
9 war on terrorism;

10 (2) the worthwhile goals of those data collection  
11 initiatives are to help ensure homeland security and  
12 protect the people of the United States from future  
13 acts of terrorism;

14 (3) protecting homeland security and fighting  
15 terrorism requires not only seeking to protect lives  
16 and property in the United States, but also ensuring  
17 that individual rights and essential liberties are safe-  
18 guarded;

19 (4) in order to achieve these goals, it is essen-  
20 tial that agencies properly manage, maintain, and  
21 secure personal information on people in the United  
22 States from inappropriate use, disclosure, or dis-  
23 semination to third parties;

24 (5) because of the leading role of the Federal  
25 Government in the expanded war on terrorism, the

1 Federal Government should serve as a role model for  
2 State and local government, and the private sector,  
3 by establishing effective safeguards and procedures  
4 to protect personal data of people in the United  
5 States;

6 (6) in order to ensure that people in the United  
7 States understand and have confidence in the proper  
8 use and safety of personal information, it is essential  
9 for agencies to implement effective privacy policies  
10 and procedures and to state those privacy policies,  
11 both online and offline; and

12 (7) an essential part of ensuring that the people  
13 in the United States have full confidence in the pri-  
14 vacy and security of personal information is to—

15 (A) have agencies confirm adherence by  
16 those agencies to the stated policies; and

17 (B) have independent, third party review,  
18 and confirmation of adherence.

19 (d) PURPOSE.—The purpose of this Act is to provide  
20 a framework for ensuring effective data and privacy man-  
21 agement by Federal agencies to—

22 (1) ensure public confidence and trust in how  
23 agencies collect, maintain, and use personal informa-  
24 tion;

1           (2) ensure continued adherence to data protec-  
2           tion and privacy policies and procedures;

3           (3) ensure that individual rights and essential  
4           liberties are protected; and

5           (4) provide for effective oversight of the collec-  
6           tion and use of individual information.

7           (e) PRIVACY MANAGER.—

8           (1) IN GENERAL.—Each agency shall designate  
9           an employee of that agency as the agency privacy  
10          manager to—

11                (A) be responsible for effective data protec-  
12                tion and management within that agency; and

13                (B) ensure compliance with the privacy  
14                and data security policies.

15          (2) ADDITIONAL RESPONSIBILITIES.—Each pri-  
16          vacy manager shall be responsible for—

17                (A) training and education for employees  
18                to promote awareness of and compliance with  
19                the privacy and data security policies; and

20                (B) developing recommended practices and  
21                procedures to ensure compliance with the pri-  
22                vacy and data security policies.

23          (f) BENCHMARK ASSESSMENT.—

24                (1) IN GENERAL.—Not later than 1 year after  
25                the date of enactment of this Act, each agency shall

1       conduct a detailed benchmark assessment of the pri-  
2       vacy and data protection policies and practices of  
3       that agency with regard to the collection, use, shar-  
4       ing, disclosure, transfer, and security of personally  
5       identifiable information relating to the agency em-  
6       ployees and the public. Such practices shall be accu-  
7       rately and clearly stated in written policies governing  
8       the data collection and use practices of the agency,  
9       both online and offline.

10       (2) CONTENT.—At a minimum, each bench-  
11       mark assessment shall determine and state—

12               (A) the personally identifiable information  
13       the agency collects on—

14                       (i) employees of the agency; and

15                       (ii) members of the public;

16               (B) any purpose for which the personally  
17       identifiable information is collected;

18               (C) any notice given to individuals regard-  
19       ing the collection and use of personal informa-  
20       tion, relating to that individual;

21               (D) any access given to individuals to re-  
22       view, amend, correct, supplement, or delete per-  
23       sonal information relating to that individual;

24               (E) whether or not consent is obtained  
25       from an individual before personally identifiable

1 information is collected, used, transferred, or  
2 disclosed and any method used to obtain con-  
3 sent;

4 (F) the policies and practices of the agency  
5 for the security of personally identifiable infor-  
6 mation;

7 (G) the policies and practices of the agency  
8 for the proper use of personally identifiable in-  
9 formation;

10 (H) the training and education procedures  
11 of the agency to adequately train personnel on  
12 agency policies and procedures for privacy and  
13 data protection;

14 (I) the policies and procedures of the agen-  
15 cy for monitoring and reporting violations of  
16 privacy and data protection policies; and

17 (J) the policies and procedures of the  
18 agency for assessing the impact of technologies  
19 on the stated privacy and security policies.

20 (g) RECORDING.—A written report of each bench-  
21 mark assessment shall be prepared and recorded with the  
22 Inspector General of the agency to serve as a benchmark  
23 for the data protection and privacy practices and policies  
24 of the agency. Each benchmark assessment shall be signed  
25 by the agency privacy manager, verifying that the agency

1 is in good faith compliance with the policies and practices  
2 stated in the benchmark assessment.

3 (h) INDEPENDENT, THIRD-PARTY REVIEW.—

4 (1) IN GENERAL.—At least every 3 years, each  
5 agency shall have performed an independent, third-  
6 party review of the privacy and data protection prac-  
7 tices of the agency to—

8 (A) determine the effectiveness of the pri-  
9 vacy and data protection policies, practices, and  
10 procedures; and

11 (B) ensure compliance with the stated pri-  
12 vacy policy of the agency.

13 (2) PURPOSES.—The purposes of reviews under  
14 this subsection are to—

15 (A) measure privacy and data protection  
16 practices against the original benchmark assess-  
17 ment of the agency;

18 (B) ensure compliance and consistency  
19 with both online and offline stated privacy poli-  
20 cies; and

21 (C) provide agencies with ongoing aware-  
22 ness and recommendations regarding privacy  
23 and data protection practices.

24 (3) REQUIREMENTS OF REVIEW.—The Inspec-  
25 tor General of each agency shall contract with an

1 independent, third party that is a recognized leader  
2 in privacy consulting, privacy technology, and data  
3 collection and use management to—

4 (A) evaluate the privacy and data protec-  
5 tion practices of the agency; and

6 (B) recommend strategies and specific  
7 steps to improve privacy and data protection  
8 management.

9 (4) CONTENT.—Each review under this sub-  
10 section shall include—

11 (A) a review of the original benchmark as-  
12 sessment concerning the privacy and data pro-  
13 tection practices of the agency with regard to  
14 the collection, use, sharing, disclosure, transfer,  
15 and security of personally identifiable informa-  
16 tion relating to agency employees and the pub-  
17 lic;

18 (B) a detailed review of the current offline  
19 privacy and data protection practices of the  
20 agency with regard to the collection, use, shar-  
21 ing, disclosure, transfer, and security of person-  
22 ally identifiable information of the employees of  
23 the agency and the public to check for compli-  
24 ance with the original benchmark assessment,  
25 especially concerning whether those practices



1 are accurately reflected in the written policies  
2 of the agency; and

3 (C) a detailed electronic scan of any  
4 website of the agency with a technology product  
5 that alerts an agency to the privacy  
6 vulnerabilities on that web page, including—

7 (i) possible noncompliance with the  
8 benchmark assessment;

9 (ii) whether the privacy and data pro-  
10 tection practices of the agency comply to  
11 the written privacy policy of the agency;  
12 and

13 (iii) whether there are any risks for  
14 inadvertent release of personally identifi-  
15 able information from the website of the  
16 agency.

17 (5) RESTRICTIONS TO AVOID CONFLICT OF IN-  
18 TEREST.—An independent contractor that has sub-  
19 stantial business with an agency may not perform a  
20 review under this subsection for that agency.

21 (6) REPORT.—Upon completion of a review, the  
22 Inspector General of an agency shall submit to the  
23 head of that agency a detailed report on the review,  
24 including recommendations for improvements or en-

1       hancements to privacy and data protection practices  
2       of the agency.

3       (i) INTERNET AVAILABILITY.—Each agency shall  
4       make each agency benchmark assessment, each inde-  
5       pendent third party review, and each report of the Inspec-  
6       tor General relating to that review available to the public  
7       on the website of the agency.

○