

109TH CONGRESS
2^D SESSION

H. R. 5588

To require the Secretary of Veterans Affairs to protect sensitive personal information of veterans, to ensure that veterans are appropriately notified of any breach of data security with respect to such information, to provide free credit monitoring and credit reports for veterans and others affected by any such breach of data security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 12, 2006

Mr. SALAZAR (for himself and Mr. EVANS) introduced the following bill; which was referred to the Committee on Veterans' Affairs

A BILL

To require the Secretary of Veterans Affairs to protect sensitive personal information of veterans, to ensure that veterans are appropriately notified of any breach of data security with respect to such information, to provide free credit monitoring and credit reports for veterans and others affected by any such breach of data security, 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Comprehensive Vet-
3 erans’ Data Protection and Identity Theft Prevention Act
4 of 2006”.

5 **SEC. 2. DEFINITIONS.**

6 For purposes of this Act, the following definitions
7 shall apply:

8 (1) **DATA BREACH.**—The term “data breach”
9 means the unauthorized acquisition or use of data in
10 electronic or printed form containing sensitive per-
11 sonal information, including information com-
12 promised with respect to the theft of data first pub-
13 licly reported on May 22, 2006.

14 (2) **DATA IN ELECTRONIC FORM.**—The term
15 “data in electronic form” means any data stored
16 electronically or digitally on any computer system or
17 database and includes recordable tapes and other
18 mass storage devices.

19 (3) **DEPARTMENT.**—The term “Department”
20 means the Department of Veterans Affairs.

21 (4) **ENCRYPTION.**—The term “encryption”
22 means the protection of data in electronic form in
23 storage or transit using an encryption technology
24 that has been adopted by an established standards
25 setting body which renders such data indecipherable
26 in the absence of associated cryptographic keys nec-

1 essary to enable decryption of such data, together
2 with appropriate management and safeguards of
3 such keys to protect the integrity of the encryption.

4 (5) NATIONWIDE CONSUMER REPORTING AGEN-
5 CY.—The term “nationwide consumer reporting
6 agency” means a consumer reporting agency de-
7 scribed in section 603(p) of the Fair Credit Report-
8 ing Act.

9 (6) SECRETARY.—The term “Secretary” means
10 the Secretary of Veterans Affairs.

11 (7) SENSITIVE PERSONAL INFORMATION.—The
12 term “sensitive personal information” means the
13 name, address, or telephone number of a veteran or
14 other individual, in combination with any of the fol-
15 lowing:

16 (A) Social Security number.

17 (B) Any information not available as part
18 of the public record regarding the veteran or
19 other individual’s military service or health.

20 (C) Any financial account or other finan-
21 cial information relating to the veteran or other
22 person.

1 **SEC. 3. PROTECTION OF SENSITIVE PERSONAL INFORMA-**
2 **TION OF VETERANS.**

3 (a) **AFFIRMATIVE OBLIGATION.**—The Secretary shall
4 have an affirmative obligation to protect from any data
5 breach the sensitive personal information of veterans and
6 any other individuals that the Department (or any third-
7 party entity acting on behalf of the Department) pos-
8 sesses, creates, or maintains as well as any information
9 or tools, including passwords or cryptographic keys used
10 to protect the integrity of encrypted data, used to access
11 sensitive personal information maintained independently
12 by others.

13 (b) **SECURITY POLICIES AND PROCEDURES.**—The
14 Secretary shall implement and maintain reasonable poli-
15 cies and procedures to protect the security and confiden-
16 tiality of sensitive personal information relating to any vet-
17 eran or other individual that is maintained, serviced, or
18 communicated by or on behalf of the Department against
19 any unauthorized access.

20 (c) **POLICIES AND PROCEDURES REGARDING ACCESS**
21 **AND USE.**—The Secretary, by regulation, shall prescribe
22 policies and procedures regarding employee and third
23 party access to, and use of, sensitive personal information
24 as well as the protection of such sensitive personal infor-
25 mation, which the Department receives, maintains, or
26 transmits. Such policies and procedures shall be issued be-

1 fore the end of the 90-day period beginning on the date
2 of the enactment of this Act.

3 (d) SYSTEM RESTORATION REQUIREMENTS.—If the
4 Secretary determines that a data breach has occurred, is
5 likely to have occurred, or is unavoidable, the Secretary
6 shall take prompt and reasonable measures to—

7 (1) repair the breach and restore the security
8 and confidentiality of the sensitive personal informa-
9 tion involved to limit further unauthorized misuse of
10 such information; and

11 (2) restore the integrity of the data security
12 safeguards of the Department and make appropriate
13 improvements to the data security, and the access
14 and use, policies and procedures issued under sub-
15 sections (b) and (c).

16 (e) THIRD PARTY DUTIES.—

17 (1) COORDINATED INVESTIGATION.—Whenever
18 any third party handling sensitive personal informa-
19 tion for or on behalf of the Department determines
20 that a data breach has occurred, is likely to have oc-
21 curred, or is unavoidable, with respect to such infor-
22 mation, the third party shall—

23 (A) promptly notify the Department of
24 such determination;

1 (B) conduct a coordinated investigation
2 with the Department to determine the full scope
3 of any such data breach; and

4 (C) ensure that the appropriate notices are
5 provided as required under section 4 of this
6 Act.

7 (2) CONTRACTUAL OBLIGATION REQUIRED.—
8 The Secretary shall not provide sensitive personal in-
9 formation to a third party unless such third party
10 agrees to fulfill the obligations imposed by sections
11 4, 5, and 6 of this Act.

12 (3) LIABILITY FOR COSTS.—Except as other-
13 wise established by written agreements between the
14 Department and any third party, a third party that
15 suffers a data breach shall be responsible for all
16 costs associated with complying with this Act, as
17 well as other costs related to such a breach, includ-
18 ing any damages relating to such a breach.

19 **SEC. 4. NOTIFICATION OF DATA BREACH.**

20 (a) NOTIFICATION.—Upon discovery of a data
21 breach, the Secretary shall—

22 (1) notify the United States Secret Service, the
23 Inspector General for the Department of Veterans
24 Affairs, the Committees on Veterans' Affairs of the
25 Senate and the House of Representatives, and the

1 Federal Trade Commission that a data breach has
2 occurred and the extent of such a breach;

3 (2) notify each individual whose personal infor-
4 mation was acquired or accessed by an unauthorized
5 person as a result of such a data breach; and

6 (3) place a conspicuous notice on the Depart-
7 ment's Internet website, which shall include a tele-
8 phone number that the individual may use, at no
9 cost to such individual, to contact the Department to
10 inquire about the data breach or the information the
11 Department maintained about that individual.

12 (b) TIMELINESS OF NOTIFICATION.—All notifica-
13 tions required under subsection (a) shall be made as
14 promptly as possible and without unreasonable delay fol-
15 lowing the discovery of a data breach and the implementa-
16 tion of any measures necessary to determine the scope of
17 the breach, prevent any further breach or unauthorized
18 disclosures, and reasonably restore the integrity of the
19 data system.

20 (c) METHOD AND CONTENT OF NOTIFICATION.—

21 (1) METHOD OF NOTIFICATION.—The Secretary
22 shall provide written notification to individuals
23 under subsection (a)(2).

1 (2) CONTENT OF NOTIFICATION.—Such written
2 notification provided to an individual under para-
3 graph (1) shall include—

4 (A) a description of the personal informa-
5 tion that was acquired by an unauthorized per-
6 son;

7 (B) a telephone number that the individual
8 may use, at no cost to such individual, to con-
9 tact the Ombudsman for Data Security in the
10 Department to inquire about the security
11 breach or the information about that individual
12 that the person acquired or accessed, as well as
13 to obtain assistance in addressing identity theft
14 issues;

15 (C) the toll-free contact telephone numbers
16 and addresses for the major credit reporting
17 agencies;

18 (D) a toll-free telephone number and Inter-
19 net website address for the Federal Trade Com-
20 mission whereby the individual may obtain in-
21 formation regarding identity theft; and

22 (E) information regarding the right of an
23 individual, at no cost to that individual, to place
24 a fraud alert, obtain a security freeze, and re-
25 ceive credit monitoring where applicable, includ-

1 ing information clearly describing the advan-
2 tages and disadvantages of these actions.

3 (d) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-
4 SION.—The Federal Trade Commission shall place, in a
5 clear and conspicuous location on its Internet website, a
6 notice of any breach of security that is reported to the
7 Commission under subsection (a)(1).

8 **SEC. 5. FRAUD ALERTS.**

9 (a) INCLUSION IN CONSUMER FILES.—The Secretary
10 shall arrange, upon the request of a veteran or other indi-
11 vidual affected by a data breach and at no cost to the
12 veteran or other individual, to include a fraud alert in the
13 file of that veteran or other individual with each nation-
14 wide consumer reporting agencies in the manner provided
15 under section 605A(a) for a period of not less than 1 year,
16 beginning on the date of such request, unless the veteran
17 or other individual requests that such fraud alert be re-
18 moved before the end of such period, and the agency has
19 received appropriate proof of the identity of the requestor
20 for such purpose.

21 (b) DISTRIBUTION.—Each nationwide consumer re-
22 porting agency referred to in subsection (a) shall also pro-
23 vide the alert required under such subsection in the file
24 of a veteran or other individual along with any credit score
25 generated in using that file, for a period of not less than

1 1 year, beginning on the date of such request, unless the
2 veteran or other individual requests that such fraud alert
3 be removed before the end of such period, and the agency
4 has received appropriate proof of the identity of the re-
5 questor for such purpose.

6 **SEC. 6. CREDIT SECURITY FREEZE.**

7 (a) IN GENERAL.—The Secretary shall arrange, upon
8 the request of a veteran or other individual affected by
9 a data breach and at no cost to the veteran or other indi-
10 vidual, to apply a security freeze to the file of that veteran
11 or other individual with each nationwide consumer report-
12 ing agency for a period of not less than 1 year, beginning
13 on the date of such request, unless the veteran or other
14 individual requests that such security freeze be removed
15 before the end of such period, and the agency has received
16 appropriate proof of the identity of the requestor for such
17 purpose.

18 (b) CONFIRMATION AND PIN NUMBERS.—The agen-
19 cy shall send a written confirmation of the security freeze
20 to the veteran or other individual within 5 business days
21 of placing the freeze. The agency shall refer the informa-
22 tion regarding the security freeze to other consumer re-
23 porting agencies. The agency shall provide the veteran or
24 other individual with a unique personal identification num-
25 ber or password to be used by the veteran or other indi-

1 vidual when providing authorization for the release of his
2 or her credit for a specific party or period of time.

3 (c) TEMPORARY LIFT OF FREEZE.—The agency that
4 receives a request from a veteran or other individual to
5 temporarily lift a freeze on a consumer report shall comply
6 with the request no later than 3 business days after receiv-
7 ing the request. Such request shall be specific as to the
8 period to which the temporary lift of a freeze shall apply.

9 (d) NEGOTIATING AUTHORITY.—The Secretary shall
10 have broad authority to negotiate and secure the best pos-
11 sible price for services provided under this section. All rea-
12 sonable costs shall be borne by the Secretary.

13 **SEC. 7. AUTHORITY TO PROVIDE MITIGATION SERVICES TO**
14 **VICTIMS OF DATA SECURITY BREACHES.**

15 (a) IN GENERAL.—The Secretary shall provide, free
16 of charge, to each individual whose personal information
17 is (or was before the date of enactment of this Act) com-
18 promised by a data breach at the Department of Veterans
19 Affairs—

20 (1) credit monitoring services, during a 1-year
21 period beginning on the date of enactment of this
22 Act; and

23 (2) a copy of the consumer report (as defined
24 in section 603 of the Fair Credit Reporting Act) of
25 the affected individual once annually during the 2-

1 year period beginning on the date on which the cred-
2 it monitoring services required by paragraph (1) ter-
3 minate, which shall be in addition to any other con-
4 sumer report provided to the individual under other-
5 wise applicable law, free of charge or otherwise.

6 (b) NEGOTIATING AUTHORITY.—The Secretary of
7 Veterans Affairs shall have broad authority to negotiate
8 and secure the best possible price for services provided
9 under this section.

10 **SEC. 8. OMBUDSMAN.**

11 (a) ESTABLISHMENT.—The Secretary shall establish
12 the position of an Ombudsman for Data Security within
13 the Department.

14 (b) DUTIES.—The Ombudsman for Data Security
15 shall—

16 (1) provide information and assistance to vet-
17 erans or other individuals affected by data breaches,
18 including providing information and assistance on
19 identity theft and issues relating to identity theft;

20 (2) assist veterans or other individuals affected
21 by a data breach with placing fraud alerts and secu-
22 rity freezes;

23 (3) provide veterans with ongoing education on
24 general financial matters and identity theft in par-
25 ticular; and

1 (4) carry out such other duties and responsibil-
2 ities as the Secretary may designate to the Ombuds-
3 man for Data Security.

○