

.....
(Original Signature of Member)

110TH CONGRESS
1ST SESSION

H. R.

To amend title 18, United States Code, to better assure cyber-security,
and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. SMITH of Texas introduced the following bill; which was referred to the
Committee on _____

A BILL

To amend title 18, United States Code, to better assure
cyber-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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cyber-Security En-
5 hancement and Consumer Data Protection Act of 2007”.

6 **SEC. 2. PERSONAL ELECTRONIC RECORDS.**

7 Section 1030(a)(2) of title 18, United States Code,
8 is amended—

1 (1) by striking “or” at the end of subparagraph
2 (B); and

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

4 “(D) a means of identification (as defined
5 in section 1028(d)) from a protected computer;
6 or

7 “(E) the capability to gain access to or re-
8 motely control a protected computer.”.

9 **SEC. 3. USE OF FULL INTERSTATE AND FOREIGN COM-**
10 **MERCE POWER FOR CRIMINAL PENALTIES.**

11 (a) BROADENING OF SCOPE.—Section 1030(e)(2)(B)
12 of title 18, United States Code, is amended by inserting
13 “or affecting” after “which is used in”.

14 (b) ELIMINATION OF REQUIREMENT OF AN INTER-
15 STATE OR FOREIGN COMMUNICATION FOR CERTAIN OF-
16 FENSES INVOLVING PROTECTED COMPUTERS.—Section
17 1030(a)(2)(C) of title 18, United States Code, is amended
18 by striking “if the conduct involved an interstate or for-
19 eign communication”.

20 **SEC. 4. RICO PREDICATES.**

21 Section 1961(1)(B) of title 18, United States Code,
22 is amended by inserting “section 1030 (relating to fraud
23 and related activity in connection with computers),” before
24 “section 1084”.

1 **SEC. 5. CYBER-EXTORTION.**

2 Section 1030(a)(7) of title 18, United States Code,
3 is amended by inserting “, or to access without authoriza-
4 tion or exceed authorized access to a protected computer”
5 after “cause damage to a protected computer”.

6 **SEC. 6. CONSPIRACY TO COMMIT CYBER-CRIMES.**

7 Section 1030(b) of title 18, United States Code, is
8 amended by inserting “or conspires” after “attempts”.

9 **SEC. 7. NOTICE TO LAW ENFORCEMENT.**

10 (a) **CRIMINAL PENALTY FOR FAILURE TO NOTIFY**
11 **LAW ENFORCEMENT.**—Chapter 47 of title 18, United
12 States Code, is amended by adding at the end the fol-
13 lowing:

14 **“§ 1039. Concealment of security breaches involving**
15 **personal information**

16 “(a) **OFFENSE.**—Whoever owns or possesses data in
17 electronic form containing a means of identification (as
18 defined in section 1028), having knowledge of a major se-
19 curity breach of the system containing such data main-
20 tained by such person, and knowingly fails to provide no-
21 tice of such breach to the United States Secret Service
22 or Federal Bureau of Investigation, with the intent to pre-
23 vent, obstruct, or impede a lawful investigation of such
24 breach, shall be fined under this title, imprisoned not more
25 than 5 years, or both.

26 “(b) **DEFINITIONS.**—As used in this section—

1 “(1) MAJOR SECURITY BREACH.—The term
2 ‘major security breach’ means any security breach—

3 “(A) whereby means of identification per-
4 taining to 10,000 or more individuals is, or is
5 reasonably believed to have been acquired, and
6 such acquisition causes a significant risk of
7 identity theft;

8 “(B) involving databases owned by the
9 Federal Government; or

10 “(C) involving primarily data in electronic
11 form containing means of identification of Fed-
12 eral Government employees or contractors in-
13 volved in national security matters or law en-
14 forcement.

15 “(2) SIGNIFICANT RISK OF IDENTITY THEFT.—

16 “(A) IN GENERAL.—The term ‘significant
17 risk of identity theft’ means such risk that a
18 reasonable person would conclude, after a rea-
19 sonable opportunity to investigate, that it is
20 more probable than not that identity theft has
21 occurred or will occur as a result of the breach.

22 “(B) PRESUMPTION.—If the data in elec-
23 tronic form containing a means of identification
24 involved in a suspected breach has been
25 encrypted, redacted, requires technology to use

1 or access the data that is not commercially
2 available, or has otherwise been rendered unus-
3 able, then there shall be a presumption that the
4 breach has not caused a significant risk of iden-
5 tity theft. Such presumption may be rebutted
6 by facts demonstrating that the encryption code
7 has been or is reasonably likely to be com-
8 promised, that the entity that acquired the data
9 is believed to possess the technology to access
10 it, or the owner or possessor of the data is or
11 reasonably should be aware of an unusual pat-
12 tern of misuse of the data that indicates fraud
13 or identity theft.”.

14 (b) RULEMAKING.—Within 180 days after the date
15 of enactment of this Act, the Attorney General and Sec-
16 retary of Homeland Security shall jointly promulgate rules
17 and regulations, after adequate notice and an opportunity
18 for comment, as are reasonably necessary, governing the
19 form, content, and timing of the notices required pursuant
20 to section 1039 of title 18, United States Code. Such rules
21 and regulations shall not require the deployment or use
22 of specific products or technologies, including any specific
23 computer hardware or software, to protect against a secu-
24 rity breach. Such rules and regulations shall require
25 that—

1 (1) such notice be provided to the United States
2 Secret Service or Federal Bureau of Investigation
3 before any notice of a breach is made to consumers
4 under State or Federal law, and within 14 days of
5 discovery of the breach;

6 (2) if the United States Secret Service or Fed-
7 eral Bureau of Investigation determines that any no-
8 tice required to be made to consumers under State
9 or Federal law would impede or compromise a crimi-
10 nal investigation or national security, the United
11 States Secret Service or Federal Bureau of Inves-
12 tigation shall direct in writing within 7 days that
13 such notice shall be delayed for 30 days, or until the
14 United States Secret Service or Federal Bureau of
15 Investigation determines that such notice will not
16 impede or compromise a criminal investigation or
17 national security;

18 (3) the United States Secret Service shall notify
19 the Federal Bureau of Investigation, if the United
20 States Secret Service determines that such breach
21 may involve espionage, foreign counterintelligence,
22 information protected against unauthorized disclo-
23 sure for reasons of national defense or foreign rela-
24 tions, or Restricted Data (as that term is defined in
25 section 11y of the Atomic Energy Act of 1954 (42

1 U.S.C. 2014(y))), except for offenses affecting the
2 duties of the United States Secret Service under sec-
3 tion 3056(a) of title 18, United States Code; and

4 (4) the United States Secret Service or Federal
5 Bureau of Investigation notify the Attorney General
6 in each State affected by the breach, if the United
7 States Secret Service or Federal Bureau of Inves-
8 tigation declines to pursue a criminal investigation,
9 or as deemed necessary and appropriate.

10 (c) IMMUNITY FROM LAWSUIT.—No cause of action
11 shall lie in any court against any law enforcement entity
12 or any person who notifies law enforcement of a security
13 breach pursuant to this section for any penalty, prohibi-
14 tion, or damages relating to the delay of notification for
15 law enforcement purposes under this Act.

16 (d) CIVIL PENALTY FOR FAILURE TO NOTIFY.—
17 Whoever knowingly fails to give a notice required under
18 section 1039 of title 18, United States Code, shall be sub-
19 ject to a civil penalty of not more than \$50,000 for each
20 day of such failure, but not more than \$1,000,000.

21 (e) RELATION TO STATE LAWS.—

22 (1) IN GENERAL.—The requirement to notify
23 law enforcement under this section shall supersede
24 any other notice to law enforcement required under
25 State law.

1 (2) EXCEPTION FOR STATE CONSUMER NOTICE
2 LAWS.—The notice required to law enforcement
3 under this section shall be in addition to any notice
4 to consumers required under State or Federal law
5 following the discovery of a security breach. Nothing
6 in this section annuls, alters, affects or exempts any
7 person from complying with the laws of any State
8 with respect to notice to consumers of a security
9 breach, except as provided by subsections (b) and
10 (c).

11 (f) DUTY OF FEDERAL AGENCIES AND DEPART-
12 MENTS.—An agency or department of the Federal Govern-
13 ment which would be required to give notice of a major
14 security breach under section 1039 of title 18, United
15 States Code, if that agency or department were a person,
16 shall notify the United States Secret Service or Federal
17 Bureau of Investigation of the breach in the same time
18 and manner as a person subject to that section. The rule-
19 making authority under subsection (b) shall include the
20 authority to make rules for notice under this subsection
21 of a major security breach.

22 (g) CLERICAL AMENDMENT.—The table of sections
23 at the beginning of chapter 47 of title 18, United States
24 Code, is amended by adding at the end the following new
25 item:

“1039. Concealment of security breaches involving personal information.”.

1 **SEC. 8. PENALTIES FOR SECTION 1030 VIOLATIONS.**

2 Subsection (c) of section 1030 of title 18, United
3 States Code, is amended to read as follows:

4 “(c)(1) The punishment for an offense under sub-
5 section (a) or (b) is a fine under this title or imprisonment
6 for not more than 30 years, or both.

7 “(2) The court, in imposing sentence for an offense
8 under subsection (a) or (b), shall, in addition to any other
9 sentence imposed and irrespective of any provision of
10 State law, order that the person forfeit to the United
11 States—

12 “(A) the person’s interest in any personal prop-
13 erty that was used or intended to be used to commit
14 or to facilitate the commission of such violation; and

15 “(B) any property, real or personal, consti-
16 tuting or derived from, any proceeds the person ob-
17 tained, directly or indirectly, as a result of such vio-
18 lation.”.

19 **SEC. 9. DIRECTIVE TO SENTENCING COMMISSION.**

20 (a) DIRECTIVE.—Pursuant to its authority under
21 section 994(p) of title 28, United States Code, and in ac-
22 cordance with this section, the United States Sentencing
23 Commission shall forthwith review its guidelines and pol-
24 icy statements applicable to persons convicted of offenses
25 under sections 1028, 1028A, 1030, 1030A, 2511 and
26 2701 of title 18, United States Code and any other rel-

1 evant provisions of law, in order to reflect the intent of
2 Congress that such penalties be increased in comparison
3 to those currently provided by such guidelines and policy
4 statements.

5 (b) REQUIREMENTS.—In determining its guidelines
6 and policy statements on the appropriate sentence for the
7 crimes enumerated in paragraph (a), the Commission shall
8 consider the extent to which the guidelines and policy
9 statements may or may not account for the following fac-
10 tors in order to create an effective deterrent to computer
11 crime and the theft or misuse of personally identifiable
12 data—

13 (1) the level of sophistication and planning in-
14 volved in such offense;

15 (2) whether such offense was committed for
16 purpose of commercial advantage or private financial
17 benefit;

18 (3) the potential and actual loss resulting from
19 the offense;

20 (4) whether the defendant acted with intent to
21 cause either physical or property harm in commit-
22 ting the offense;

23 (5) the extent to which the offense violated the
24 privacy rights of individuals;

1 (6) the effect of the offense upon the operations
2 of a government agency of the United States, or of
3 a State or local government;

4 (7) whether the offense involved a computer
5 used by the government in furtherance of national
6 defense, national security or the administration of
7 justice;

8 (8) whether the offense was intended to, or had
9 the effect of significantly interfering with or dis-
10 rupting a critical infrastructure;

11 (9) whether the offense was intended to, or had
12 the effect of creating a threat to public health or
13 safety, injury to any person, or death; and

14 (10) whether the defendant purposefully in-
15 volved a juvenile in the commission of the offense to
16 avoid punishment.

17 (c) **ADDITIONAL REQUIREMENTS.**—In carrying out
18 this section, the Commission shall—

19 (1) assure reasonable consistency with other
20 relevant directives and with other sentencing guide-
21 lines;

22 (2) account for any additional aggravating or
23 mitigating circumstances that might justify excep-
24 tions to the generally applicable sentencing ranges;

1 (3) make any conforming changes to the sen-
2 tencing guidelines; and

3 (4) assure that the guidelines adequately meet
4 the purposes of sentencing as set forth in section
5 3553(a)(2) of title 18, United States Code.

6 **SEC. 10. DAMAGE TO PROTECTED COMPUTERS.**

7 (a) Section 1030(a)(5)(B) of title 18, United States
8 Code, is amended—

9 (1) by striking “or” at the end of clause (iv);

10 (2) by inserting “or” at the end of clause (v);

11 and

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

13 “(vi) damage affecting ten or more
14 protected computers during any 1-year pe-
15 riod.”.

16 (b) Section 1030(g) of title 18, United States Code,
17 is amended by striking “or” after “(iv),” and inserting
18 “, or (vi)” after “(v)”.

19 (c) Section 2332b(g)(5)(B)(i) of title 18, United
20 States Code, is amended by striking “(v) (relating to pro-
21 tection of computers)” and inserting “(vi) (relating to the
22 protection of computers)”.

1 **SEC. 11. ADDITIONAL FUNDING FOR RESOURCES TO INVESTIGATE AND PROSECUTE CRIMINAL ACTIVITY INVOLVING COMPUTERS.**

2
3
4 (a) **ADDITIONAL FUNDING FOR RESOURCES.**—

5 (1) **AUTHORIZATION.**—In addition to amounts
6 otherwise authorized for resources to investigate and
7 prosecute criminal activity involving computers,
8 there are authorized to be appropriated for each of
9 the fiscal years 2007 through 2011—

10 (A) \$10,000,000 to the Director of the
11 United States Secret Service;

12 (B) \$10,000,000 to the Attorney General
13 for the Criminal Division of the Department of
14 Justice; and

15 (C) \$10,000,000 to the Director of the
16 Federal Bureau of Investigation.

17 (2) **AVAILABILITY.**—Any amounts appropriated
18 under paragraph (1) shall remain available until ex-
19 pended.

20 (b) **USE OF ADDITIONAL FUNDING.**—Funds made
21 available under subsection (a) shall be used by the Direc-
22 tor of the United States Secret Service, the Director of
23 the Federal Bureau of Investigation, and the Attorney
24 General, for the United States Secret Service, the Federal
25 Bureau of Investigation, and the criminal division of the
26 Department of Justice, respectively, to—

- 1 (1) hire and train law enforcement officers to—
- 2 (A) investigate crimes committed through
- 3 the use of computers and other information
- 4 technology, including through the use of the
- 5 Internet; and
- 6 (B) assist in the prosecution of such
- 7 crimes; and
- 8 (2) procure advanced tools of forensic science to
- 9 investigate, prosecute, and study such crimes.