

109TH CONGRESS
2^D SESSION

H. R. 5318

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

IN THE HOUSE OF REPRESENTATIVES

MAY 9, 2006

Mr. SENSENBRENNER (for himself, Mr. COBLE, Mr. SMITH of Texas, Mr. FEENEY, Mr. SCHIFF, and Ms. PRYCE of Ohio) introduced the following bill; which was referred to the Committee on the Judiciary

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 2006”.

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

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

9 (1) by striking “or” at the end of subparagraph

10 (B); and

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

2 “(D) a means of identification (as defined
3 in section 1028(d)) from a protected computer;

4 or

5 “(E) the capability to gain access to or re-
6 motely control without authorization, a pro-
7 tected computer.”.

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

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

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

19 **SEC. 4. RICO PREDICATES.**

20 Section 1961(1)(B) of title 18, United States Code,
21 is amended by inserting “section 1030 (relating to fraud
22 and related activity in connection with computers),” before
23 “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, and if such breach causes a significant risk of
25 identity theft, shall be fined under this title, imprisoned
26 not more than 5 years, or both.

1 “(b) DEFINITION.—As used in this section, the term
2 ‘major security breach’ means any security breach—

3 “(1) whereby personal information pertaining to
4 10,000 or more individuals is, or is reasonably be-
5 lieved to have been acquired;

6 “(2) involving databases owned by the Federal
7 Government; or

8 “(3) involving primarily data in electronic form
9 containing personal information of employees or con-
10 tractors of the Federal Government involved in Na-
11 tional security matters or law enforcement.”.

12 (b) RULEMAKING.—Within 180 days after the date
13 of enactment of this act, the Attorney General and Sec-
14 retary of Homeland Security shall jointly promulgate rules
15 and regulations, after adequate notice and an opportunity
16 for comment, as are reasonably necessary, governing the
17 form, content, and timing of the notices required pursuant
18 to section 1039 of title 18, U.S.C. Such rules and regula-
19 tions shall require that—

20 (1) such notice be provided to the United States
21 Secret Service or Federal Bureau of Investigation
22 before any notice of a breach is made to consumers
23 under State or Federal law, and within 14 days of
24 discovery of the breach;

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

13 (3) the United States Secret Service shall notify
14 the Federal Bureau of Investigation, if the United
15 States Secret Service determines that such breach
16 may involve espionage, foreign counterintelligence,
17 information protected against unauthorized disclo-
18 sure for reasons of national defense or foreign rela-
19 tions, or Restricted Data (as that term is defined in
20 section 11y of the Atomic Energy Act of 1954 (42
21 U.S.C. 2014(y))), except for offenses affecting the
22 duties of the United States Secret Service under sec-
23 tion 3056(a) of title 18, United States Code.

24 (c) IMMUNITY FROM LAWSUIT.—No cause of action
25 shall lie in any court against any law enforcement entity

1 or any person who notifies law enforcement of a security
2 breach pursuant to this section for any penalty, prohibi-
3 tion, or damages relating to the delay of notification for
4 law enforcement purposes under this Act.

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

10 (e) CLERICAL AMENDMENT.—The table of sections
11 at the beginning of chapter 47 of title 18, United States
12 Code, is amended by adding at the end the following new
13 item:

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

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

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

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

20 “(2) The court, in imposing sentence for an offense
21 under subsection (a) or (b), shall, in addition to any other
22 sentence imposed and irrespective of any provision of
23 State law, order that the person forfeit to the United
24 States—

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

4 “(B) any property, real or personal, consti-
5 tuting or derived from, any proceeds the person ob-
6 tained, directly or indirectly, as a result of such vio-
7 lation.”.

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

9 (a) **DIRECTIVE.**—Pursuant to its authority under
10 section 994(p) of title 28, United States Code, and in ac-
11 cordance with this section, the United States Sentencing
12 Commission shall forthwith review its guidelines and pol-
13 icy statements applicable to persons convicted of offenses
14 under sections 1028, 1028A, 1030, 1030A, 2511 and
15 2701 of title 18, United States Code and any other rel-
16 evant provisions of law, in order to reflect the intent of
17 Congress that such penalties be increased in comparison
18 to those currently provided by such guidelines and policy
19 statements.

20 (b) **REQUIREMENTS.**—In determining its guidelines
21 and policy statements on the appropriate sentence for the
22 crimes enumerated in paragraph (a), the Commission shall
23 consider the extent to which the guidelines and policy
24 statements may or may not account for the following fac-
25 tors in order to create an effective deterrent to computer

1 crime and the theft or misuse of personally identifiable
2 data—

3 (1) the level of sophistication and planning in-
4 volved in such offense;

5 (2) whether such offense was committed for
6 purpose of commercial advantage or private financial
7 benefit;

8 (3) the potential and actual loss resulting from
9 the offense;

10 (4) whether the defendant acted with intent to
11 cause either physical or property harm in commit-
12 ting the offense;

13 (5) the extent to which the offense violated the
14 privacy rights of individuals;

15 (6) the effect of the offense upon the operations
16 of a government agency of the United States, or of
17 a State or local government;

18 (7) whether the offense involved a computer
19 used by the government in furtherance of national
20 defense, national security or the administration of
21 justice;

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

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

4 (10) whether the defendant purposefully in-
5 volved a juvenile in the commission of the offense to
6 avoid punishment.

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

9 (1) assure reasonable consistency with other
10 relevant directives and with other sentencing guide-
11 lines;

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

15 (3) make any conforming changes to the sen-
16 tencing guidelines; and

17 (4) assure that the guidelines adequately meet
18 the purposes of sentencing as set forth in section
19 3553(a)(2) of title 18, United States Code.

20 **SEC. 10. ADDITIONAL FUNDING FOR RESOURCES TO INVESTIGATE AND PROSECUTE CRIMINAL ACTIVITY INVOLVING COMPUTERS.**

21 (a) **ADDITIONAL FUNDING FOR RESOURCES.**—

22 (1) **AUTHORIZATION.**—In addition to amounts
23 otherwise authorized for resources to investigate and
24

1 prosecute criminal activity involving computers,
2 there are authorized to be appropriated for each of
3 the fiscal years 2007 through 2011—

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

6 (B) \$10,000,000 to the Attorney General
7 for the Criminal Division of the Department of
8 Justice; and

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

11 (2) AVAILABILITY.—Any amounts appropriated
12 under paragraph (1) shall remain available until ex-
13 pended.

14 (b) USE OF ADDITIONAL FUNDING.—Funds made
15 available under subsection (a) shall be used by the director
16 of the United States Secret Service, the Director of the
17 Federal Bureau of Investigation, and the Attorney Gen-
18 eral, for the United States Secret Service, the Federal Bu-
19 reau of Investigation, and the criminal division of the De-
20 partment of Justice, respectively, to—

21 (1) hire and train law enforcement officers to—

22 (A) investigate crimes committed through
23 the use of computers and other information
24 technology, including through the use of the
25 Internet; and

1 (B) assist in the prosecution of such
2 crimes; and

3 (2) procure advanced tools of forensic science to
4 investigate, prosecute, and study such crimes.

○