

Union Calendar No. 292

109TH CONGRESS
2^D SESSION

H. R. 5318

[Report No. 109-522]

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

JUNE 22, 2006

Additional sponsor: Mr. CHABOT

JUNE 22, 2006

Reported with an amendment, committed to the Committee of the Whole
House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italie*]

[For text of introduced bill, see copy of bill as introduced on May 9, 2006]

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,*

1 **SECTION 1. SHORT TITLE.**

2 *This Act may be cited as the “Cyber-Security En-*
 3 *hancement and Consumer Data Protection Act of 2006”.*

4 **SEC. 2. PERSONAL ELECTRONIC RECORDS.**

5 *Section 1030(a)(2) of title 18, United States Code, is*
 6 *amended—*

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

9 *(2) by adding at the end the following:*

10 *“(D) a means of identification (as defined*
 11 *in section 1028(d)) from a protected computer;*

12 *or*

13 *“(E) the capability to gain access to or re-*
 14 *motely control a protected computer.”.*

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

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

20 *(b) ELIMINATION OF REQUIREMENT OF AN INTER-*
 21 *STATE OR FOREIGN COMMUNICATION FOR CERTAIN OF-*
 22 *FENSES INVOLVING PROTECTED COMPUTERS.—Section*
 23 *1030(a)(2)(C) of title 18, United States Code, is amended*
 24 *by striking “if the conduct involved an interstate or foreign*
 25 *communication”.*

1 **SEC. 4. RICO PREDICATES.**

2 Section 1961(1)(B) of title 18, United States Code, is
3 amended by inserting “section 1030 (relating to fraud and
4 related activity in connection with computers),” before “sec-
5 tion 1084”.

6 **SEC. 5. CYBER-EXTORTION.**

7 Section 1030(a)(7) of title 18, United States Code, is
8 amended by inserting “, or to access without authorization
9 or exceed authorized access to a protected computer” after
10 “cause damage to a protected computer”.

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

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

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

15 (a) *CRIMINAL PENALTY FOR FAILURE TO NOTIFY LAW*
16 *ENFORCEMENT.*—Chapter 47 of title 18, United States
17 Code, is amended by adding at the end the following:

18 **“§1039. Concealment of security breaches involving**
19 ***personal information***

20 “(a) *OFFENSE.*—Whoever owns or possesses data in
21 electronic form containing a means of identification (as de-
22 fined in section 1028), having knowledge of a major security
23 breach of the system containing such data maintained by
24 such person, and knowingly fails to provide notice of such
25 breach to the United States Secret Service or Federal Bu-
26 reau of Investigation, with the intent to prevent, obstruct,

1 *or impede a lawful investigation of such breach, shall be*
 2 *fined under this title, imprisoned not more than 5 years,*
 3 *or both.*

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

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

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

12 “(B) *involving databases owned by the Fed-*
 13 *eral Government; or*

14 “(C) *involving primarily data in electronic*
 15 *form containing means of identification of Fed-*
 16 *eral Government employees or contractors in-*
 17 *volved in national security matters or law en-*
 18 *forcement.*

19 “(2) *SIGNIFICANT RISK OF IDENTITY THEFT.—*

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

1 “(B) *PRESUMPTION.*—If the data in elec-
2 tronic form containing a means of identification
3 involved in a suspected breach has been
4 encrypted, redacted, requires technology to use or
5 access the data that is not commercially avail-
6 able, or has otherwise been rendered unusable,
7 then there shall be a presumption that the breach
8 has not caused a significant risk of identity
9 theft. Such presumption may be rebutted by facts
10 demonstrating that the encryption code has been
11 or is reasonably likely to be compromised, that
12 the entity that acquired the data is believed to
13 possess the technology to access it, or the owner
14 or possessor of the data is or reasonably should
15 be aware of an unusual pattern of misuse of the
16 data that indicates fraud or identity theft.”.

17 (b) *RULEMAKING.*—Within 180 days after the date of
18 enactment of this Act, the Attorney General and Secretary
19 of Homeland Security shall jointly promulgate rules and
20 regulations, after adequate notice and an opportunity for
21 comment, as are reasonably necessary, governing the form,
22 content, and timing of the notices required pursuant to sec-
23 tion 1039 of title 18, United States Code. Such rules and
24 regulations shall not require the deployment or use of spe-
25 cific products or technologies, including any specific com-

1 *puter hardware or software, to protect against a security*
2 *breach. Such rules and regulations shall require that—*

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

8 *(2) if the United States Secret Service or Federal*
9 *Bureau of Investigation determines that any notice*
10 *required to be made to consumers under State or Fed-*
11 *eral law would impede or compromise a criminal in-*
12 *vestigation or national security, the United States Se-*
13 *cret Service or Federal Bureau of Investigation shall*
14 *direct in writing within 7 days that such notice shall*
15 *be delayed for 30 days, or until the United States Se-*
16 *cret Service or Federal Bureau of Investigation deter-*
17 *mines that such notice will not impede or compromise*
18 *a criminal investigation or national security;*

19 *(3) the United States Secret Service shall notify*
20 *the Federal Bureau of Investigation, if the United*
21 *States Secret Service determines that such breach*
22 *may involve espionage, foreign counterintelligence, in-*
23 *formation protected against unauthorized disclosure*
24 *for reasons of national defense or foreign relations, or*
25 *Restricted Data (as that term is defined in section*

1 *11y of the Atomic Energy Act of 1954 (42 U.S.C.*
2 *2014(y))), except for offenses affecting the duties of the*
3 *United States Secret Service under section 3056(a) of*
4 *title 18, United States Code; and*

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

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

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

22 *(e) RELATION TO STATE LAWS.—*

23 *(1) IN GENERAL.—The requirement to notify law*
24 *enforcement under this section shall supersede any*

1 *other notice to law enforcement required under State*
 2 *law.*

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

12 (f) *DUTY OF FEDERAL AGENCIES AND DEPART-*
 13 *MENTS.—An agency or department of the Federal Govern-*
 14 *ment which would be required to give notice of a major se-*
 15 *curity breach under section 1039 of title 18, United States*
 16 *Code, if that agency or department were a person, shall no-*
 17 *tify the United States Secret Service or Federal Bureau of*
 18 *Investigation of the breach in the same time and manner*
 19 *as a person subject to that section. The rulemaking author-*
 20 *ity under subsection (b) shall include the authority to make*
 21 *rules for notice under this subsection of a major security*
 22 *breach.*

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

4 “(c)(1) *The punishment for an offense under subsection*
 5 *(a) or (b) is a fine under this title or imprisonment for*
 6 *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 State*
 10 *law, order that the person forfeit to the United States—*

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

14 “(B) *any property, real or personal, constituting*
 15 *or derived from, any proceeds the person obtained, di-*
 16 *rectly or indirectly, as a result of such violation.”.*

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

18 (a) *DIRECTIVE.—Pursuant to its authority under sec-*
 19 *tion 994(p) of title 28, United States Code, and in accord-*
 20 *ance with this section, the United States Sentencing Com-*
 21 *mission shall forthwith review its guidelines and policy*
 22 *statements applicable to persons convicted of offenses under*
 23 *sections 1028, 1028A, 1030, 1030A, 2511 and 2701 of title*
 24 *18, United States Code and any other relevant provisions*
 25 *of law, in order to reflect the intent of Congress that such*

1 *penalties be increased in comparison to those currently pro-*
2 *vided by such guidelines and policy statements.*

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

10 (1) *the level of sophistication and planning in-*
11 *volved in such offense;*

12 (2) *whether such offense was committed for pur-*
13 *pose of commercial advantage or private financial*
14 *benefit;*

15 (3) *the potential and actual loss resulting from*
16 *the offense;*

17 (4) *whether the defendant acted with intent to*
18 *cause either physical or property harm in committing*
19 *the offense;*

20 (5) *the extent to which the offense violated the*
21 *privacy rights of individuals;*

22 (6) *the effect of the offense upon the operations*
23 *of a government agency of the United States, or of a*
24 *State or local government;*

1 (7) *whether the offense involved a computer used*
2 *by the government in furtherance of national defense,*
3 *national security or the administration of justice;*

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

7 (9) *whether the offense was intended to, or had*
8 *the effect of creating a threat to public health or safe-*
9 *ty, injury to any person, or death; and*

10 (10) *whether the defendant purposefully involved*
11 *a juvenile in the commission of the offense to avoid*
12 *punishment.*

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

15 (1) *assure reasonable consistency with other rel-*
16 *evant directives and with other sentencing guidelines;*

17 (2) *account for any additional aggravating or*
18 *mitigating circumstances that might justify excep-*
19 *tions to the generally applicable sentencing ranges;*

20 (3) *make any conforming changes to the sen-*
21 *tencing guidelines; and*

22 (4) *assure that the guidelines adequately meet*
23 *the purposes of sentencing as set forth in section*
24 *3553(a)(2) of title 18, United States Code.*

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

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

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

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

6 and

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

8 “(vi) damage affecting ten or more
9 protected computers during any 1-year pe-
10 riod.”.

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

14 (c) Section 2332b(g)(5)(B)(i) of title 18, United States
15 Code, is amended by striking “(v) (relating to protection
16 of computers)” and inserting “(vi) (relating to the protec-
17 tion of computers)”.

18 **SEC. 11. ADDITIONAL FUNDING FOR RESOURCES TO INVES-**
19 **TIGATE AND PROSECUTE CRIMINAL ACTIVITY**
20 **INVOLVING COMPUTERS.**

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

22 (1) **AUTHORIZATION.**—In addition to amounts
23 otherwise authorized for resources to investigate and
24 prosecute criminal activity involving computers, there
25 are authorized to be appropriated for each of the fis-
26 cal years 2007 through 2011—

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

3 (B) \$10,000,000 to the Attorney General for
4 the Criminal Division of the Department of Jus-
5 tice; and

6 (C) \$10,000,000 to the Director of the Fed-
7 eral Bureau of Investigation.

8 (2) AVAILABILITY.—Any amounts appropriated
9 under paragraph (1) shall remain available until ex-
10 pended.

11 (b) USE OF ADDITIONAL FUNDING.—Funds made
12 available under subsection (a) shall be used by the Director
13 of the United States Secret Service, the Director of the Fed-
14 eral Bureau of Investigation, and the Attorney General, for
15 the United States Secret Service, the Federal Bureau of In-
16 vestigation, and the criminal division of the Department
17 of Justice, respectively, to—

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

19 (A) investigate crimes committed through
20 the use of computers and other information tech-
21 nology, including through the use of the Internet;
22 and

23 (B) assist in the prosecution of such crimes;
24 and

- 1 (2) *procure advanced tools of forensic science to*
- 2 *investigate, prosecute, and study such crimes.*

Union Calendar No. 292

109TH CONGRESS
2^D Session

H. R. 5318

[Report No. 109-522]

A BILL

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

JUNE 22, 2006

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed