109TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
109–522

# CYBER-SECURITY ENHANCEMENT AND CONSUMER DATA PROTECTION ACT OF 2006

JUNE 22, 2006.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SENSENBRENNER, from the Committee on the Judiciary, submitted the following

# R E P O R T

[To accompany H.R. 5318]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 5318) to amend title 18, United States Code, to better assure cyber-security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

**SECTION 1. SHORT TITLE.**

This Act may be cited as the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006".

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

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

(1) by striking "or" at the end of subparagraph (B); and

(2) by adding at the end the following:

"(D) a means of identification (as defined in section 1028(d)) from a protected computer; or

"(E) the capability to gain access to or remotely control a protected computer.".

**SEC. 3. USE OF FULL INTERSTATE AND FOREIGN COMMERCE POWER FOR CRIMINAL PENALTIES.**

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

(b) ELIMINATION OF REQUIREMENT OF AN INTERSTATE OR FOREIGN COMMUNICATION FOR CERTAIN OFFENSES INVOLVING PROTECTED COMPUTERS.—Section 1030(a)(2)(C) of title 18, United States Code, is amended by striking "if the conduct involved an interstate or foreign communication".

**SEC. 4. RICO PREDICATES.**

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

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

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

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

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

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

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

**"§ 1039. Concealment of security breaches involving personal information**

"(a) OFFENSE.—Whoever owns or possesses data in electronic form containing a means of identification (as defined in section 1028), having knowledge of a major security breach of the system containing such data maintained by such person, and knowingly fails to provide notice of such breach to the United States Secret Service or Federal Bureau of Investigation, with the intent to prevent, obstruct, or impede a lawful investigation of such breach, shall be fined under this title, imprisoned not more than 5 years, or both.

"(b) DEFINITIONS.—As used in this section—

"(1) MAJOR SECURITY BREACH.—The term 'major security breach' means any security breach—

"(A) whereby means of identification pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired, and such acquisition causes a significant risk of identity theft;

"(B) involving databases owned by the Federal Government; or

"(C) involving primarily data in electronic form containing means of identification of Federal Government employees or contractors involved in national security matters or law enforcement.

"(2) SIGNIFICANT RISK OF IDENTITY THEFT.—

"(A) IN GENERAL.—The term 'significant risk of identity theft' means such risk that a reasonable person would conclude, after a reasonable opportunity to investigate, that it is more probable than not that identity theft has occurred or will occur as a result of the breach.

"(B) PRESUMPTION.—If the data in electronic form containing a means of identification involved in a suspected breach has been encrypted, redacted, requires technology to use or access the data that is not commercially available, or has otherwise been rendered unusable, then there shall be a presumption that the breach has not caused a significant risk of identity theft. Such presumption may be rebutted by facts demonstrating that the encryption code has been or is reasonably likely to be compromised, that the entity that acquired the data is believed to possess the technology to access it, or the owner or possessor of the data is or reasonably should be aware of an unusual pattern of misuse of the data that indicates fraud or identity theft.".

(b) RULEMAKING.—Within 180 days after the date of enactment of this Act, the Attorney General and Secretary of Homeland Security shall jointly promulgate rules and regulations, after adequate notice and an opportunity for comment, as are reasonably necessary, governing the form, content, and timing of the notices required pursuant to section 1039 of title 18, United States Code. Such rules and regulations shall not require the deployment or use of specific products or technologies, including any specific computer hardware or software, to protect against a security breach. Such rules and regulations shall require that—

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

(2) if the United States Secret Service or Federal Bureau of Investigation determines that any notice required to be made to consumers under State or Federal law would impede or compromise a criminal investigation or national security, the United States Secret Service or Federal Bureau of Investigation shall direct in writing within 7 days that such notice shall be delayed for 30 days, or until the United States Secret Service or Federal Bureau of Investigation de-

termines that such notice will not impede or compromise a criminal investigation or national security;

(3) the United States Secret Service shall notify the Federal Bureau of Investigation, if the United States Secret Service determines that such breach may involve espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y))), except for offenses affecting the duties of the United States Secret Service under section 3056(a) of title 18, United States Code; and

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

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

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

(e) RELATION TO STATE LAWS.—

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

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

(f) DUTY OF FEDERAL AGENCIES AND DEPARTMENTS.—An agency or department of the Federal Government which would be required to give notice of a major security breach under section 1039 of title 18, United States Code, if that agency or department were a person, shall notify the United States Secret Service or Federal Bureau of Investigation of the breach in the same time and manner as a person subject to that section. The rulemaking authority under subsection (b) shall include the authority to make rules for notice under this subsection of a major security breach.

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

"1039. Concealment of security breaches involving personal information.".

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

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

"(c)(1) The punishment for an offense under subsection (a) or (b) is a fine under this title or imprisonment for not more than 30 years, or both.

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

"(A) the person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

"(B) any property, real or personal, constituting or derived from, any proceeds the person obtained, directly or indirectly, as a result of such violation.".

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

(a) DIRECTIVE.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall forthwith review its guidelines and policy statements applicable to persons convicted of offenses under sections 1028, 1028A, 1030, 1030A, 2511 and 2701 of title 18, United States Code and any other relevant provisions of law, in order to reflect the intent of Congress that such penalties be increased in comparison to those currently provided by such guidelines and policy statements.

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

(1) the level of sophistication and planning involved in such offense;

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

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

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

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

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

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

(8) whether the offense was intended to, or had the effect of significantly interfering with or disrupting a critical infrastructure;

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

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

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

(1) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(2) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(3) make any conforming changes to the sentencing guidelines; and

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

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

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

(1) by striking "or" at the end of clause (iv);

(2) by inserting "or" at the end of clause (v); and

(3) by adding at the end the following:

"(vi) damage affecting ten or more protected computers during any 1-year period.".

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

(c) Section 2332b(g)(5)(B)(i) of title 18, United States Code, is amended by striking "(v) (relating to protection of computers)" and inserting "(vi) (relating to the protection of computers)".

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

(a) ADDITIONAL FUNDING FOR RESOURCES.—

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

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

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

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

(2) AVAILABILITY.—Any amounts appropriated under paragraph (1) shall remain available until expended.

(b) USE OF ADDITIONAL FUNDING.—Funds made available under subsection (a) shall be used by the Director of the United States Secret Service, the Director of the Federal Bureau of Investigation, and the Attorney General, for the United States Secret Service, the Federal Bureau of Investigation, and the criminal division of the Department of Justice, respectively, to—

(1) hire and train law enforcement officers to—

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

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

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

## PURPOSE AND SUMMARY

The purpose of H.R. 5318, the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006," is to supplement and in-

crease the tools available to the Department of Justice to investigate and prosecute criminals who use computers to further their criminal activities, particularly those who seek to obtain personal information that can be used to commit financial fraud and identity theft. In addition, the legislation ensures that the Federal Bureau of Investigation and United States Secret Service will be notified and provided a meaningful opportunity to investigate major data security breaches, and that the Department of Justice will prosecute criminal activity associated with those breaches.

## BACKGROUND AND NEED FOR THE LEGISLATION

In recent years, identity theft has become an increasingly prevalent national problem. The illegal use of personally-identifiable information to engage in fraudulent or other illegal behavior has grown dramatically and annual losses resulting from identity theft amount to $50 billion.[1] In February, 2005, it was revealed that organized criminals had fraudulently obtained personal data on nearly 145,000 consumers from ChoicePoint, Inc., an Alpharetta, Georgia-based data broker.[2] The criminals used the data to commit various acts of identity theft. Since that watershed breach, businesses that maintain such data, including other data brokers,[3] financial institutions,[4] media companies,[5] retailers,[6] universities,[7] and Federal government agencies[8] have experienced similar breaches involving sensitive information that can be used to commit identity theft and financial crimes. Although many of these breaches involved unsophisticated criminal efforts to obtain personal data, or simple negligence by the owners or possessors of the data who failed to protect it from loss or theft, the Committee also is aware that organized criminals have increasingly turned to computer crime to engage in identity theft and financial fraud.[9] Many of these criminal organizations, operating largely out of Eastern Europe and Asia,[10] utilize sophisticated tools such as botnets and malicious code to commit their crimes.[11] These tools permit criminals to download large caches of personal and financial information and steal user names, passwords, and other means of accessing bank and commercial accounts.[12] The criminal organizations traffic this information through underground websites on the Internet, creating a black market in cyberspace for stolen personal and finan-

---

[1] Press Release, White House, Fact Sheet: The President's Identity Theft Task Force (May 10, 2006), available at http://www.whitehouse.gov/news/releases/2006/05/20060510–6.html.

[2] Joseph Menn, Fraud Ring Taps Into Credit Data, L.A. Times, February 15, 2005 at 1.

[3] David Colker, ID Thieves Tap Files at 2nd Big Data Firm, L.A. Times, March 10, 2005 at 1.

[4] Mark Mueller, Inside Ring Is Charged in Financial Data Scheme, Nwrk. Star-Ledger, April 29, 2005 at 21.

[5] Jon Swartz, Time-Warner Data on 600,000 Missing, USA Today, May 3, 2005.

[6] Bill Husted & David Markiewicz, I.D. Theft Slams Chain, 1.4 Million Cards Stolen, Atl.J–Const., April 20, 2005 at 1.

[7] Allison Kolodziej, Data Thieves Prey on Colleges: Schools Becoming More Vigilant to Safeguard Personal Information, Columbus Dis., May 13, 2006 (online version).

[8] Christopher Lee, Personal Data on Veterans Is Stolen, Wash. Post, May 23, 2006 at A1.

[9] Spencer Ante and Brian Grow, Meet the Hackers: Cybercrooks Are Stealing Billions; An Inside Look at Law Enforcement's Biggest Targets, Bus. Week, May 29, 2006 at 58; Jon Swartz, New Breed of Cyberattack Takes Aim at Sensitive Data, USA Today, Dec. 27, 2005, at B1.

[10] Tom Zeller, Jr., Countless Dens of Uncatchable Thieves, N.Y. Times, April 3, 2006, at C3.

[11] Cassell Bryan-Low, Digital Trails: In Eastern Europe, A Gumshoe Chases Internet Villains, Wall St. J., Sept. 1, 2005, at A1.

[12] Id.

cial information.[13] Some of these identity thieves advertise that they have access to literally millions of stolen credit card and bank records for sale.[14]

Recent Federal investigations by the United States Secret Service and Federal Bureau of Investigation have highlighted the scope of this problem. A year-long Secret Service investigation of the "Shadowcrew" organization led to the indictment of 27 U.S. and foreign persons involved in an organized identity theft and financial fraud ring.[15] According to government estimates, the members of the Shadowcrew organization trafficked in at least 1.5 million stolen credit and bank card numbers, and caused an estimated $40 million in losses. A recent investigation by U.S. and U.K. authorities of the website "carderplanet.net" revealed that the site boasted nearly 7,000 members and served as a marketplace for millions of stolen bank and credit card accounts.[16] According to government and private sector estimates, this type of criminal activity affects as many as 10 million Americans and costs businesses and consumers nearly $55 billion per year.[17] The Federal Bureau of Investigation has estimated that annual losses for all types of computer crime—including malware, financial fraud, network intrusions and other activities—exceed $67 billion.[18]

To respond to the ever-increasing sophistication of computer crime and identity theft, Chairman Sensenbrenner and five cosponsors introduced H.R. 5318 on May 9, 2006. The Committee recognizes that comprehensive data security reform legislation necessarily must include additional regulation of personal information, and enhanced tools for law enforcement. The Committee believes that any comprehensive data security legislation must contain the following elements contained in H.R. 5318: (1) increased criminal penalties for data theft and computer crimes; (2) additional tools, including the express ability to use of the Racketeer Influenced and Corrupt Organizations statute and a grant of extraterritorial jurisdiction, to combat transnational cyber-criminal organizations; and (3) a strong incentive for the business community to report data breaches to Federal law enforcement promptly after the discovery of the breach to allow the Secret Service and Federal Bureau of Investigation every opportunity to investigate and prosecute the criminals responsible for these crimes.

## HEARINGS

On May 9, 2006, the House Committee on the Judiciary's Subcommittee on Crime, Terrorism and Homeland Security held a legislative hearing on H.R. 5318. The Subcommittee received testimony from: Ms. Laura H. Parsky, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice; Mr. Joseph LaRocca, Vice President, Loss Prevention, National Retail Federation; Ms. Anne Wallace, Executive Director, Identity Theft

[13] Legislative Hearing on Cyber-Security Enhancement and Consumer Data Protection Act of 2006, 109th Cong., 2d Sess. (2006) (statement of Ms. Laura H. Parsky, Deputy Assistant Attorney General, United States Department of Justice).
[14] Id.
[15] Id.
[16] Cassell Bryan-Low, Fraud Inc.: As Identity Theft Moves Online, Crime Rings Mimic Big Business, Wall St. J., July 13, 2005 at A1.
[17] Id.
[18] Federal Bureau of Investigation Computer Crime Survey (2005).

Assistance Corporation; and Ms. Susanna Montezemolo, Policy Analyst, Consumers Union.

## COMMITTEE CONSIDERATION

On Thursday, May 25, 2006, the Committee met in open session and ordered favorably reported the bill, H.R. 5318, by voice vote with an amendment, a quorum being present.

## VOTE OF THE COMMITTEE

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee notes that there were no recorded votes on H.R. 5318 during the Committee on the Judiciary's consideration of the bill.

## COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

## NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of House rule XIII is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

## CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to H.R. 5318, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

JUNE 16, 2006.

Hon. F. JAMES SENSENBRENNER, Jr.,
*Chairman, Committee on the Judiciary,*
*House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5318, the Cyber-Security Enhancement and Consumer Data Protection Act of 2006.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz (for federal costs), Melissa Merrell (for the impact on state, local, and tribal governments), and Paige Piper/Bach (for the impact on the private sector).

Sincerely,

DONALD B. MARRON,
*Acting Director.*

Enclosure.

*H.R. 5318—Cyber-Security Enhancement and Consumer Data Protection Act of 2006*

Summary: H.R. 5318 would broaden the coverage of current laws and establish new federal crimes for improper use of personal electronic records and other criminal activity involving computers. The bill also would authorize the appropriation of $30 million for each of fiscal years 2007 through 2011 for the United States Secret Service, the Federal Bureau of Investigation, and the Criminal Division of the Department of Justice to investigate and prosecute violators of the bill's provisions.

Assuming appropriation of the authorized amounts, CBO estimates that implementing the bill would cost $144 million over the 2007–2011 period. H.R. 5318 could affect direct spending and revenues, but we estimate that any such effects would be less than $500,000 annually.

H.R. 5318 contains an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the costs to state, local, and tribal governments would be small and would not exceed the annual threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

H.R. 5318 also would impose private-sector mandates as defined in UMRA. The bill would require certain persons to notify federal law enforcement in the event of a major security breach of certain electronic data. The bill also would prohibit anyone from bringing a cause of action in court against certain persons related to a delay of notification of such a security breach for law enforcement purposes. CBO expects that the cost of complying with the notification mandate would be small. However, because of a lack of information about such cases, CBO cannot estimate the direct cost of complying with the mandate prohibiting lawsuits or whether the aggregate cost of mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 5318 is shown in the following table. For this estimate, CBO assumes that the bill will be enacted by the beginning of fiscal year 2007, that the amounts authorized by the bill will be appropriated by the start of each fiscal year, and that outlays will follow the historical rate of spending for these activities. The costs of this legislation fall within budget function 750 (administration of justice).

| | By fiscal year, in millions of dollars— | | | | |
|---|---|---|---|---|---|
| | 2007 | 2008 | 2009 | 2010 | 2011 |
| CHANGES IN SPENDING SUBJECT TO APPROPRIATION | | | | | |
| Authorization level | 30 | 30 | 30 | 30 | 30 |
| Estimated outlays | 24 | 30 | 30 | 30 | 30 |

In addition to the costs shown in the table, enacting H.R. 5318 could increase collections of civil and criminal fines for violations of the bill's provisions. CBO estimates that any additional collections would not be significant because of the relatively small number of additional cases likely to be affected. Civil fines are recorded as revenues. Criminal fines are recorded as revenues, deposited in

the Crime Victims Fund, and subsequently spent without further appropriation.

Estimated impact on state, local, and tribal governments: H.R. 5318 contains intergovernmental mandates as defined in UMRA because it would require state and local governments to notify federal law enforcement agencies in the event of a security breach involving the personal information of 10,000 or more individuals. Based on information from state and local governments, CBO does not expect such notification requirements to be costly. The bill also would preempt certain state laws that address identity theft. CBO estimates that the cost to state and local governments would be small and well below the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

Estimated impact on the private sector: H.R. 5318 would impose private-sector mandates as defined in UMRA. The bill would require certain persons to notify federal law enforcement in the event of a major security breach of certain electronic data. The bill also would prohibit anyone from bringing a cause of action in court against certain persons related to a delay of notification of such a security breach for law enforcement purposes. CBO expects that the cost of complying with the notification mandate would be small. However, because of a lack of information about such cases, CBO cannot estimate the direct cost of complying with the mandate prohibiting lawsuits or whether the aggregate cost of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

*Security breach notification*

H.R. 5318 would impose a mandate on certain persons regarding notification of a major security breach. The bill would require anyone who owns or possesses data in an electronic form maintained by that person, having knowledge of a major security breach of that data involving personal identification of 10,000 or more individuals, to notify the United States Secret Service or the Federal Bureau of Investigation before notice of such breach is made to consumers and within 14 days of discovery of the breach. Such persons also would have to delay notifying consumers, if so directed by federal law enforcement. Based on information from government sources, CBO expects that the direct cost of complying with the mandate would be small.

*Immunity from lawsuit*

H.R. 5318 also would impose a mandate by prohibiting any cause of action in any court against a person who notifies law enforcement of a security breach pursuant to this bill for any penalty, prohibition, or damages relating to the delay of notification for law enforcement purposes. Because the bill would eliminate existing rights to seek compensation for damages caused by certain acts, it would impose a private-sector mandate. The direct cost of the mandate would be the forgone net value of awards and settlements in such claims. Because of the lack of information about both the value of awards in such cases and the number of claims that would be filed in the absence of this legislation, CBO has no basis for pre-

dicting the level of potential damage awards, if any. Thus, CBO cannot estimate the cost of this mandate.

Previous CBO estimates: CBO has provided cost estimates for seven other pieces of legislation that deal with identity theft or the safeguarding of personal information. Some have different provisions and would require private companies and the government to take certain precautions to safeguard personal information. The cost estimates reflect those differences.

- On May 26, 2006, CBO transmitted a cost estimate for H.R. 3997, the Data Accountability and Trust Act, as ordered reported by the House Committee on Energy and Commerce on May 24, 2006.
- On May 26, 2006, CBO transmitted a cost estimate for H.R. 4127, the Financial Data Protection Act of 2006, as ordered reported by the House Committee on Financial Services on May 24, 2006.
- On April 19, 2006, CBO transmitted a cost estimate for S. 1789, the Personal Data Privacy and Security Act of 2005, as reported by the Senate Committee on the Judiciary on November 17, 2005.
- On April 6, 2006, CBO transmitted a cost estimate for H.R. 4127, the Data Accountability and Trust Act, as ordered reported by the House Committee on Energy and Commerce on March 29, 2006, with a subsequent amendment provided by the committee on April 4, 2006.
- On March 30, 2006, CBO transmitted a cost estimate for H.R. 3997, the Financial Data Protection Act, as ordered reported by the House Committee on Financial Services on March 16, 2006.
- On March 10, 2006, CBO transmitted a cost estimate for S. 1326, the Notification of Risk to Personal Data Act, as ordered reported by the Senate Committee on the Judiciary on October 20, 2005.
- On November 3, 2005, CBO transmitted a cost estimate for S. 1408, the Identity Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005.

All of the bills would require certain entities to take precautions to safeguard the personal information of consumers, all would preempt state and local laws, and all contain intergovernmental mandates as defined in UMRA. The Senate bills would impose costs that exceed the annual threshold defined in UMRA ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect because those bills would require a large number of intergovernmental entities to make changes that could be costly.

Estimate prepared by: Federal costs: Mark Grabowicz, impact on state, local, and tribal governments: Melissa Merrell, impact on the private sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

## PERFORMANCE GOALS AND OBJECTIVES

The goal of H.R. 5318 is to supplement and increase the tools available to the Department of Justice to investigate and prosecute criminals who use computers to commit crime, particularly those

who seek to obtain personal information that can be used to perpetrate financial fraud and identity theft.

## CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in art. I, § 8 of the Constitution.

## SECTION-BY-SECTION ANALYSIS AND DISCUSSION

An amendment in the nature of a substitute was offered by Chairman Sensenbrenner and was adopted by voice vote. The following section describes the reported bill as amended.

*Section 1. Short title*

This section cites the short title of the bill as the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006."

*Section 2. Personal electronic records*

This section amends 18 U.S.C. § 1030(a)(2) to prohibit unauthorized intrusions to obtain information from a protected computer which may be used as a means of identification. This section also amends section 1030(a)(2) to provide that the use of "botnets" to gain access to, or remotely control a computer without authorization is a Federal crime.

*Section 3. Use of full interstate and foreign commerce power for criminal penalties*

This section broadens coverage of 18 U.S.C. § 1030 by defining "protected computer" to include computers "affecting" interstate or foreign commerce, and by eliminating the requirement in current law that the criminal conduct itself involve an interstate or foreign communication.

*Section 4. Addition of RICO predicates*

This section adds section 1030 computer crimes to the list of predicate offenses in 18 U.S.C. § 1961—the Racketeer Influenced and Corrupt Organizations (RICO) statute. Adding section 1030 crimes as RICO predicate offenses will provide the Department of Justice (DOJ) with an additional tool to investigate and prosecute organized crime syndicates which often use sophisticated computer schemes to commit criminal acts.

*Section 5. Cyber extortion*

This section amends 18 U.S.C. § 1030(a)(7) to prohibit cyber-extortion where the criminal threatens to illegally access a protected computer and demands a promise or agreement from the victim. Existing law only prohibits cyber-extortion where the criminal threatens to damage a protected computer in exchange for money or any thing of value.

*Section 6. Conspiracy offenses*

This section expressly makes it a crime to conspire to violate 18 U.S.C. § 1030 by amending subsection (b) of the existing statute.

*Section 7. Notice to law enforcement*

This section protects law enforcement investigations involving breaches of personal data. Section 7(a) would make it a crime punishable by up to five years in prison to knowingly fail to report breaches of a certain scope to the Federal Bureau of Investigation (FBI) or Secret Service, with the intent to prevent, obstruct or impede a lawful investigation. Under this provision, any person who owns or possesses data in electronic form containing a means of identification (as that term is defined in 18 U.S.C. § 1028) that has been the subject of a breach is required to notify the United States Secret Service or the FBI of the breach, if the person reasonably believes that the breach involves either: (1) the records of at least 10,000 consumers and a "significant risk of identity theft"; (2) any Federal databases; or (3) any contractor involved in national security matters or law enforcement.

The Committee expects that courts will interpret the term "possesses" broadly to strongly encourage rapid notice of data breaches to law enforcement, which is critical to successful investigation and prosecution of any criminal activity associated with the breach. The term "possesses" should include any circumstance wherein entities regularly maintain electronic data containing a means of identification in their systems or databases on behalf of themselves or third parties. However, the Committee understands that a requirement of mandatory notice to law enforcement with concomitant criminal liability for failure to provide such notice will not be appropriate in all circumstances. For instance, the Committee does not intend to apply such a notice requirement to cybersecurity companies who, in the course of monitoring their customers' computer networks or during the transitory analytical manipulation of their customers' data in order to detect, prevent or mitigate cyber attacks or other vulnerabilities, may temporarily maintain some of their customers' data. In the event these cybersecurity companies discover and notify their customer of a possible or actual major security breach of their customer's system, it is the customer who will have the obligation to notify law enforcement of the breach.

The bill defines "significant risk of identity theft" to include breaches where a reasonable person would determine that it is more probable than not that identity theft has occurred or will occur. Data protected by encryption, redaction, technology not commercially available, or by any process which renders the data unusable is presumed to not involve a significant risk of identity theft. Such presumption may be rebutted by evidence that the encryption key is compromised, that the entity who obtained the data is believed to possess the technology to access it, or the owner or possessor of the data is aware (or reasonably should be aware) of an unusual pattern of misuse of the data indicating fraud or identity theft.

The Committee recognizes that the term "encryption" is generally accepted to mean the protection of data in electronic form, in storage or in transit, using a technology that has been adopted by an established standards-setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such technology must include appropriate management and safeguards of these keys to protect the integrity of the encryption. In addition to industry-based

standards-setting bodies, the Committee recognizes that the National Institute of Standards and Technology (NIST) plays a leading role in commercial cryptography standards, working in close cooperation with industry to enable implementation of cryptographic services in information systems. The Committee recognizes that encryption technology standards adopted by these bodies may evolve over time, and has thus resisted calls to establish a definition of "encryption" in the Federal criminal code. The Committee instead expects prosecutors and the courts to look to the standards adopted by industry and NIST to determine whether a particular technology meets the currently-accepted definition of "encryption," and whether any breach of data protected by the use of such technology therefore involves no significant risk of identity theft.

Section 7(b) requires the Departments of Justice and Homeland Security to jointly promulgate rules and regulations governing the form, content and timing of the notices required under this section within 180 days after the date of enactment. The Committee expects that these rules and regulations will only address the mechanics and process of communication between the business community and Federal law enforcement for purposes of providing notice of a major security breach, and subsequent management of any delayed notice to consumers requested by law enforcement. The Committee strongly believes that any such rulemaking remain technology neutral, and not require the deployment or use of specific products or technologies to protect against security breaches.

Section 7(b) sets basic requirements governing the timing of notices to the FBI or Secret Service, including a requirement that notice must occur within 14 days after the discovery of the breach, and before any notice is made to consumers under Federal or State law. The Committee intends that a failure to adhere to the 14-day rule will constitute one element of a violation of the new section 1039. Further, section 7(b) permits law enforcement, upon a determination that notice to consumers would impede or compromise an investigation, to direct the entity that experienced the breach in writing within 7 days that any notice to consumers be delayed for up to 30 days or until such time that law enforcement determines that consumer notice will not impede or compromise a criminal investigation or national security. Section 7(b) also requires the Secret Service to notify the FBI in cases involving espionage, foreign counterintelligence and other matters primarily in the jurisdiction of the FBI. Finally, section 7(b) requires the FBI and Secret Service to notify the Attorney General of each State affected by the breach if either declines to pursue an investigation or deems such notice necessary and appropriate.

Section 7(c) provides civil liability protection for any penalty, prohibition or damages against law enforcement and any other entity that occur as a result of the law enforcement delay. Section 7(d) authorizes the United States Attorney General to pursue civil penalties of up to $50,000 per day, not to exceed $1 million, for knowing failure to report breaches that occur without the requisite criminal intent to impede an investigation. Section 7(e) of the bill provides that the bill's law enforcement notice requirement supercedes State law enforcement notification provisions related to data security breaches, but does not impact State consumer notification laws.

Section 7(h) requires Federal departments and agencies to give notice of major security breaches under new section 1039 in the same time and manner as if the department or agency were a person under that section.

*Section 8. Penalties for section 1030 violations*

This section increases the punishment for violating 18 U.S.C. § 1030(a) or (b) to 30 years. Section 8 also requires a defendant to forfeit to the United States any personal property that was used or intended to be used to commit the section 1030 computer crime, or any real or personal property constituting, or derived from the proceeds of the crime.

*Section 9. Directive to the sentencing commission*

This section directs the Sentencing Commission to amend the sentencing guidelines to reflect Congress' intent to increase penalties for computer crime and theft of personally identifiable information. To assist the Sentencing Commission in this task, the section sets forth factors that the Commission should consider: the level of sophistication and planning; whether the offense was committed for the purpose of commercial advantage or private financial benefit; the potential and actual loss; whether the defendant acted with intent to cause physical or property harm; the extent of any privacy violation; effect on the United States government, if any; the defendant's intent to cause physical or property harm; and disruption of a critical infrastructure.

*Section 10. Damage to protected computers*

This section amends 18 U.S.C. § 1030(a)(5)(B) to make it a Federal crime to access and damage ten or more protected computers during any one-year period. Currently, the Department of Justice must prove at least $5,000 in damage to any protected computer(s) under this section in order to gain a conviction, which can be a difficult hurdle in so-called "botnet" cases.

*Section 11. Addition of funding for resources to investigate and prosecute criminal activity involving computers*

This section provides an additional $30 million annually to the Secret Service, FBI and DOJ to investigate and prosecute cybercrimes.

## AGENCY VIEWS

DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AFFAIRS,
*Washington, DC, May 31, 2006.*

Hon. F. JAMES SENSENBRENNER, Jr.,
*Chairman, Committee on the Judiciary,*
*House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Department of Justice (Department) appreciates the opportunity to comment on H.R. 5318, the "Cyber Security Enhancement and Consumer Data Protection Act of 2006." As Deputy Assistant Attorney General Laura Parsky testified before the Subcommittee on Crime, Terrorism, and Homeland Security earlier this month, we strongly support the legislation's objec-

tives, and appreciate the Committee's willingness to provide us with additional tools to combat the growing threat posed by ever more sophisticated cyber criminals. Our section by section analysis of the bill follows.

*Section 2. Personal electronic records*

This provision would add two new subsections to 18 U.S.C. § 1030(a)(2). Currently, section 1030(a)(2) criminalizes the unauthorized acquisition of information from a computer. Specifically, anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains" any of three listed types of "information" violates section 1030(a)(2).

Section 2 of the bill would add two new items to the list of what cannot be "obtained" from a computer. First, the proposed section 1030(a)(2)(D) would read, "a means of identification (as defined in section 1028(d)) from a protected computer," and second, the proposed section 1030(a)(2)(E) would read, "the capability to gain access to or remotely control without authorization, a protected computer."

The Department believes that proposed section 1030(a)(2)(D) may be redundant. A "means of identification" is already unquestionably a piece of "information." Obtaining that information from a protected computer is already a violation of section 1030(a)(2)(C) if the conduct involved an interstate or foreign communication, and will be a violation of section 1030(a)(2)(C) in every case if section 3 of this bill is enacted. Specifically adding "means of identification" to section 1030(a)(2)'s list of information will invite courts to begin to interpret the term "information" more narrowly.

Proposed section 1030(a)(2)(E) is apparently designed to criminalize the act of creating a "botnet." The Department supports the goal of this provision, in particular the desire to update section 1030 to provide prosecutors with effective tools to combat the growing botnet threat. However, we believe that this provision is not the best way to address this problem. First, the provision has technical problems. A natural reading of the provision suggests that the words "without authorization" apply to "remotely control" and not to "gain access to." Thus, for example, the provision would appear to criminalize the act of intentionally accessing a neighbor's wifi network without authority and then accessing an ordinary website like google or www.washingtonpost.com. This outcome does not appear to be what the section is intended to cover.

Second, we believe that placing this sort of provision in 18 U.S.C. § 1030(a)(2) creates unnecessary confusion in the statutory scheme. In particular, obtaining the capability to control or access another protected computer without authorization would clearly constitute "damage." Under the existing statutory scheme, prohibitions on causing "damage" are located in section 1030(a)(5). We recommend making changes there to avoid making the already complex statute more confusing.

Thus, in order to address the problem of creating botnets, even where they have not yet been used in a denial of service attack or other misconduct, we recommend that section 1030(a)(5) be modified to criminalize causing damage less than $5000, or causing damage to 10 or more protected computers. These changes would allow prosecution of those who install bots on protected computers

even if those bots have not yet been used for any other criminal purpose. For language that would accomplish this goal, see Appendix A.

*Section 5. Cyber extortion*

This provision would add the words "or to access without authorization or exceed authorized access to a protected computer" to section 1030(a)(7). If the goal is to take into account the problem that some cyber-criminals extort companies without explicitly threatening to cause damage to computers, then we recommend a slightly different solution to that problem. It is true that some criminals steal confidential data and then threaten to make that data public if their demands are not met, while others cause the damage first—such as by accessing a corporate computer without authority and encrypting critical data—and then threaten that they will not correct the problem unless the victim pays. In order to address these problems, the Department recommends amending section 1030(a)(7) in the following ways:

> "(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any
>
> (A) threat to cause damage to a protected computer;
>
> (B) threat to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
>
> (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion; . . . ."

*Section 6. Conspiracy to commit cybercrimes*

With respect to the amendment to 18 U.S.C. § 1030, the Department recommends that, in order to be clearer, this provision be revised to instead insert "conspires to commit or" after "Whoever" and before "attempts."

In addition, we recommend making a technical amendment to section 1030(a)(5)(B) to make it consistent as well:

> "by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense *or a conspiracy to commit an offense,* would, if completed, have caused)—"

*Section 7. Notice to law enforcement*

This provision would require notification of law enforcement when a security breach of a system containing personal information occurs. The Department strongly supports the goal of this provision. The Department believes the language requiring prior notification of the U.S. Secret Service or the Federal Bureau of Investigation (FBI) will allow for appropriate law enforcement investigation of unauthorized access to personal information. We have several suggestions, however, to improve the language.

*a. Section 7(a).—Proposed section 1039(b)*

Proposed section 1039(b) defines the term "major security breach." The Department recognizes that there are competing ideas within Congress as to whether the compromise of 10,000 personal records is an appropriate level at which to define a major security breach and therefore require mandatory notification. However, we believe there is a consensus that significant breaches sometimes involve fewer than 10,000 records. For example, an intrusion attack involving the theft of as few as 1,000 credit card numbers is, under the United States Sentencing Guidelines, presumed to involve a minimum of $500,000 in losses. We therefore recommend revising this section to reflect this viewpoint and require such reporting when appropriate.

Proposed section 1039(b)(2) requires any breach of a Federal database to be reported to the FBI or Secret Service. The Department notes that federal agencies are already required by the Federal Information Security Management Act (FISMA) to notify and consult with the Federal information security incident center housed at the Department of Homeland Security. Federal agencies are also required to notify and consult as appropriate with law enforcement agencies and relevant Offices of Inspector General. Inspectors General are often better suited to handle incidents where there is a lack of compliance with policy but no criminal intent. For example, a system administrator may inadvertently publish personal information on a website. The Department believes the existing FISMA legislation, as administered by the Office of Management and Budget in consultation with the agencies and other policy authorities, provides an acceptable framework for reporting federal incidents.

Moreover, the Department believes that not all disclosures of personal information by Federal agencies would necessarily constitute a major security breach. For example, the breach of a database containing Federal agency employee names and phone numbers would not automatically be a "major security breach" for which criminal penalties would be warranted.

In addition, proposed section 1039(b)(3) may create problems with compliance, as it may be difficult for certain data holders to determine whether or not a breach meets the language of this provision. For example, if a large company that does some government contracting experiences a security breach, will it be able to determine which of its employees are involved in national security and whether the breach "primarily" involved them? (The Department also notes that "primarily" here probably is not intended to modify "data in electronic form" but instead "employees or contractors of the Federal Government * * *." We recommend amending the provision to read, "the security breach involves data in electronic form primarily containing personal information of * * *"). Thus, the Department recommends striking the words "involved in national security matters or law enforcement." This change would broaden the provision slightly, but make it much easier for victims of security breaches to comply.

*b. Section 7(b)(1)*

This provision would require notification to law enforcement within 14 days of the discovery of the breach. In identifying the

source of the breach, speed can be critical. Electronic evidence leading to the criminal(s) can easily be either intentionally or inadvertently destroyed, so immediate notification of law enforcement in some cases can provide the best chance that the perpetrators will be identified and brought to justice. We therefore urge consideration of language that would encourage companies to provide an informed notification more quickly. For example, Internet service providers often retain connection data for only a few days, yet this data is critical to identifying the perpetrators of an offense. In other cases, the successful outcome of the investigation can depend upon the information provided by the IT professionals who manage the networks that have been compromised, and an appropriate period of time should be provided so that a comprehensive and accurate assessment of the intrusion and damage incurred can be developed. We also believe that a tiered penalty approach could be an effective way to assure reporting. Under this approach, a civil penalty might be imposed for any knowing failure to report a security breach within a shorter period of time, while criminal sanctions would be reserved for violations involving longer delays in reporting or for violations committed with the intent to obstruct an investigation.

*c. Section 7(b)(2)*

Section 7(b)(2) indicates that where Federal or state law require notification to "consumers" whose information was released as a result of a security breach, either the U.S. Secret Service or the FBI can direct that such notice be delayed for 30 days. Under this provision, the Secret Service or the FBI can idefinitely delay customer notification where such notification will impede or compromise a criminal investigation or national security. We strongly support this provision. We would suggest, however, that this provision be amended so that if it is utilized, the Secret Service or the FBI must notify the entity that experienced the security breach when such notification will no longer impede or compromise a criminal investigation or national security.

*d. Section 7(b)(3)*

The Department supports the designation of both the FBI and the U.S. Secret Service as appropriate recipients of reports from victims of security breaches. However, we recommend that Section 7(b)(3) be stricken from the bill. The Department believes that the manner and means of law enforcement and intelligence information-sharing between federal agencies is well-established, particularly in regard to the arena of computer security and cyber crime, and should be reserved to the Executive Branch.

*e. Section 7(d)*

This provision does not clearly define who has the authority to impose a civil penalty and where jurisdiction would lie for such proceedings. It could be clarified by using language similar to that in 18 U.S.C. § 1034, restructuring the provision to allow it to begin as does section 1034:

> "The Attorney General may bring a civil action in the appropriate United States district court against any per-

son who . . . and, upon proof of such conduct, such person shall be subject to a civil penalty of . . . .''

*Section 8. Penalties for section 1030 violations*

*a. Proposed section 1030(c)(1)—30 year sentence*

This provision would eliminate the complex sentencing scheme for the various subsections of 18 U.S.C. § 1030 and create a single overarching maximum penalty of 30 years in prison. Although the Department has concerns with this across-the-board approach proposed in the bill, we believe that there are ways to improve the efficacy of the penalty provisions of section 1030.

In particular, the Department would recommend increasing penalties in a number of areas. For example, the penalties for the theft of information (section 1030(a)(2)) appear inadequate in light of the rise in identity theft, ''phishing,'' and spyware. We recommend raising these penalties as outlined in Appendix A.

In addition, current sections 1030(a)(1) (theft of classified information) and 1030(a)(4) (fraud in connection with hacking) should have penalties that are commensurate with the penalties for the same conduct when it occurs without an online component. Thus, because the penalty for wire fraud (18 U.S.C. § 1343) was recently increased, the Department recommends raising the penalty for section 1030(a)(4) violations to 20 years in prison.

*b. Proposed section 1030(c)(2)—forfeiture*

In light of the recent amendment of 18 U.S.C. § 2461 by section 410 of the USA PATRIOT Act reauthorization legislation (Pub. L. No. 109–177), the Department recommends the following paragraph (c)(3) be added to section 8 of the bill:

> ''(3) Pursuant to section 2461(c) of title 28, United States Code, the criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse and Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.''

In addition, we recommended the addition of new subsection (d) to section 8 of the bill to provide for civil forfeitures:

> ''(d)(1) IN GENERAL.—Any real or personal property used to commit or facilitate the commission of a violation of this section, the gross proceeds of such violation, and any property traceable to such property or proceeds, shall be subject to forfeiture.
>
> ''(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) of title 18 shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security.

*Section 10. Additional funding for resources to investigate and prosecute criminal activity involving computers*

The United States Attorneys' Offices and the Criminal Division share responsibility for the prosecution of cybercrime cases. In order to ensure that any funds appropriated under this bill for prosecution purposes are allocated as needed among prosecuting components of the Department, we suggest that Section 10(1)(B) be amended as follows:

> "(B) $10,000,000 to the Attorney General for the prosecution of such crimes; . . ."

We also recommend, in order to ensure that the language in the bill makes clear the distinction between the prosecutive and investigative functions of various components of the Department, and the FBI, and the investigative function of the U.S. Secret Service, that the provisions concerning use of funds in section 10(b) be deleted and that Section 10(a)(1) subsections (A) and (C) be collapsed into section 10(a)(1)(A) and amended as follows:

> "(A) $10,000,000 to the Director of the United States Secret Service and $10,000,000 to the Director of the Federal Bureau of Investigation to hire and train law enforcement officers to investigate crimes committed through the use of computers and other information technology, including through the use of the Internet and assist in the prosecution of such crimes and procure advanced tools of forensic science to investigate and study such crimes; . . ."

These changes will make the bill provisions technically correct. However, we note that all of the Department of Justice components currently receive funding for the identified purposes within their current appropriations, and that the authorization is not necessary for them to conduct these activities or to receive additional funding. It is our understanding that United States Secret Service is similarly funded and does not require an authorization to carry out these activities.

The Office of Management and Budget has advised that there is no objection to the presentation of these views from the standpoint of the Administration's program. If we may be of additional assistance, please do not hesitate to contact this office.

Sincerely,

WILLIAM E. MOSCHELLA,
*Assistant Attorney General.*

APPENDIX A

*Proposed Language:*

18 U.S.C. § 1030

(a) Whoever–

(5) (A)~~(i)~~ knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

***(B)***~~(ii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

***(C)***~~(iii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; ~~and~~

~~(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)–~~

~~(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;~~

~~(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;~~

~~(iii) physical injury to any person;~~

~~(iv) a threat to public health or safety; or~~

~~(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;~~

(c) The punishment for an offense under subsection (a) or (b) of this section is–

...

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under

subsection (a)(2), (a)(3), ~~(a)(5)(A)(iii),~~ or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), ~~(a)(5)(A)(iii),~~ or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

~~(4) (A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;~~

~~(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;~~

~~(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and~~

~~(5) (A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and~~

~~(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.~~

***(4) (A) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--***

***(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;***

***(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;***

***(iii) physical injury to any person;***

***(iv) a threat to public health or safety;***

***(v) damage affecting a computer used by or for a government entity in furtherance of the administration of justice, national defense, or national security; or***
***(vi) damage affecting ten or more protected computers during any 1-year period;***

***or an attempt to commit an offense punishable under this subparagraph;***

***(B) except as provided in subparagraphs (c)(4)(D) and (c)(4)(E), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subparagraphs (c)(4)(A)(i) through (vi), or an attempt to commit an offense punishable under this subparagraph;***

***(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5) that occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;***

***(D) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for not more than 20 years, or both;***

***(E) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for any term of years or for life, or both; or***

***(F) a fine under this title, imprisonment for not more than one year, or both, for any other offense under subsection (a)(5), or an attempt to commit an offense punishable under this subparagraph.***

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of ~~subsection (a)(5)(B)~~ ***subparagraph (c)(4)(A)***. Damages for a violation involving only conduct described in ~~subsection (a)(5)(B)(i)~~ ***subparagraph (c)(4)(A)(i)*** are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the

damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 2332b(g)(5)(B)(I)

...1030(a)(5)(A)~~(i)~~ resulting in damage as defined in ~~1030(a)(5)(B)(ii) through (v)~~ ***1030(c)(4)(A)(ii) through (vi)*** (relating to protection of computers)...

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

**TITLE 18, UNITED STATES CODE**

* * * * * * *

# PART I—CRIMES

* * * * * * *

## CHAPTER 47—FRAUD AND FALSE STATEMENTS

Sec.
1001. Statements or entries generally.
* * * * * * *
*1039. Concealment of security breaches involving personal information.*
* * * * * * *

### § 1030. Fraud and related activity in connection with computers

(a) Whoever—
(1) * * *
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A) * * *
(B) information from any department or agency of the United States; **[**or**]**
(C) information from any protected computer **[**if the conduct involved an interstate or foreign communication**]**;
*(D) a means of identification (as defined in section 1028(d)) from a protected computer; or*
*(E) the capability to gain access to or remotely control a protected computer.*

* * * * * * *

(5)(A) * * *
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—
(i) * * *

* * * * * * *

(iv) a threat to public health or safety; **[**or**]**
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; *or*
*(vi) damage affecting ten or more protected computers during any 1-year period.*

* * * * * * *

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any

communication containing any threat to cause damage to a protected computer*, or to access without authorization or exceed authorized access to a protected computer*;

* * * * * * *

(b) Whoever attempts *or conspires* to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

[(c) The punishment for an offense under subsection (a) or (b) of this section is—

[(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

[(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

[(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

[(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2) or an attempt to commit an offense punishable under this subparagraph, if—

[(i) the offense was committed for purposes of commercial advantage or private financial gain;

[(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

[(iii) the value of the information obtained exceeds $5,000; and

[(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph;

[(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

[(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

[(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

[(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

[(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

[(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

[(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.]

*(c)(1) The punishment for an offense under subsection (a) or (b) is a fine under this title or imprisonment for not more than 30 years, or both.*

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

*(A) the person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and*

*(B) any property, real or personal, constituting or derived from, any proceeds the person obtained, directly or indirectly, as a result of such violation.*

* * * * * * *

(e) As used in this section—

(1) * * *

(2) the term "protected computer" means a computer—

(A) * * *

(B) which is used in *or affecting* interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

* * * * * * *

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), [or] (v)*, or (vi)* of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.. No action may be

brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

* * * * * * *

***§ 1039. Concealment of security breaches involving personal information***

*(a) OFFENSE.—Whoever owns or possesses data in electronic form containing a means of identification (as defined in section 1028), having knowledge of a major security breach of the system containing such data maintained by such person, and knowingly fails to provide notice of such breach to the United States Secret Service or Federal Bureau of Investigation, with the intent to prevent, obstruct, or impede a lawful investigation of such breach, shall be fined under this title, imprisoned not more than 5 years, or both.*

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

*(1) MAJOR SECURITY BREACH.—The term "major security breach" means any security breach—*

*(A) whereby means of identification pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired, and such acquisition causes a significant risk of identity theft;*

*(B) involving databases owned by the Federal Government; or*

*(C) involving primarily data in electronic form containing means of identification of Federal Government employees or contractors involved in national security matters or law enforcement.*

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

*(A) IN GENERAL.—The term "significant risk of identity theft" means such risk that a reasonable person would conclude, after a reasonable opportunity to investigate, that it is more probable than not that identity theft has occurred or will occur as a result of the breach.*

*(B) PRESUMPTION.—If the data in electronic form containing a means of identification involved in a suspected breach has been encrypted, redacted, requires technology to use or access the data that is not commercially available, or has otherwise been rendered unusable, then there shall be a presumption that the breach has not caused a significant risk of identity theft. Such presumption may be rebutted by facts demonstrating that the encryption code has been or is reasonably likely to be compromised, that the entity that acquired the data is believed to possess the technology to access it, or the owner or possessor of the data is or reasonably should be aware of an unusual pattern of misuse of the data that indicates fraud or identity theft.*

* * * * * * *

**CHAPTER 96—RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS**

* * * * * * *

**§ 1961. Definitions**

As used in this chapter—

(1) "racketeering activity" means (A) any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), which is chargeable under State law and punishable by imprisonment for more than one year; (B) any act which is indictable under any of the following provisions of title 18, United States Code: Section 201 (relating to bribery), section 224 (relating to sports bribery), sections 471, 472, and 473 (relating to counterfeiting), section 659 (relating to theft from interstate shipment) if the act indictable under section 659 is felonious, section 664 (relating to embezzlement from pension and welfare funds), sections 891–894 (relating to extortionate credit transactions), section 1028 (relating to fraud and related activity in connection with identification documents), section 1029 (relating to fraud and related activity in connection with access devices), *section 1030 (relating to fraud and related activity in connection with computers),* section 1084 (relating to the transmission of gambling information), section 1341 (relating to mail fraud), section 1343 (relating to wire fraud), section 1344 (relating to financial institution fraud), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), sections 1461–1465 (relating to obscene matter), section 1503 (relating to obstruction of justice), section 1510 (relating to obstruction of criminal investigations), section 1511 (relating to the obstruction of State or local law enforcement), section 1512 (relating to tampering with a witness, victim, or an informant), section 1513 (relating to retaliating against a witness, victim, or an informant), section 1542 (relating to false statement in application and use of passport), section 1543 (relating to forgery or false use of passport), section 1544 (relating to misuse of passport), section 1546 (relating to fraud and misuse of visas, permits, and other documents), sections 1581–1592 (relating to peonage, slavery, and trafficking in persons)., section 1951 (relating to interference with commerce, robbery, or extortion), section 1952 (relating to racketeering), section 1953 (relating to interstate transportation of wagering paraphernalia), section 1954 (relating to unlawful welfare fund payments), section 1955 (relating to the prohibition of illegal gambling businesses), section 1956 (relating to the laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 1958 (relating to use of interstate commerce facilities in the commission of murder-for-hire), section 1960 (relating to illegal money transmitters), sections 2251, 2251A, 2252, and 2260 (relating to sexual exploitation of children), sections 2312 and 2313 (relating to interstate transportation of stolen motor vehicles), sections 2314 and 2315 (relating to interstate transportation of stolen property) , section 2318 (relating to trafficking in counterfeit labels for phonorecords, computer pro-

grams or computer program documentation or packaging and copies of motion pictures or other audiovisual works), section 2319 (relating to criminal infringement of a copyright), section 2319A (relating to unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances), section 2320 (relating to trafficking in goods or services bearing counterfeit marks), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), sections 2341–2346 (relating to trafficking in contraband cigarettes), sections 2421–24 (relating to white slave traffic), sections 175–178 (relating to biological weapons), sections 229-F (relating to chemical weapons), section 831 (relating to nuclear materials),(C) any act which is indictable under title 29, United States Code, section 186 (dealing with restrictions on payments and loans to labor organizations) or section 501(c) (relating to embezzlement from union funds), (D) any offense involving fraud connected with a case under title 11 (except a case under section 157 of this title), fraud in the sale of securities, or the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), punishable under any law of the United States, (E) any act which is indictable under the Currency and Foreign Transactions Reporting Act, (F) any act which is indictable under the Immigration and Nationality Act, section 274 (relating to bringing in and harboring certain aliens), section 277 (relating to aiding or assisting certain aliens to enter the United States), or section 278 (relating to importation of alien for immoral purpose) if the act indictable under such section of such Act was committed for the purpose of financial gain, or (G) any act that is indictable under any provision listed in section 2332b(g)(5)(B);

* * * * * * *

## CHAPTER 113B—TERRORISM

* * * * * * *

### § 2332b. Acts of terrorism transcending national boundaries

(a) * * *

* * * * * * *

(g) DEFINITIONS.—As used in this section—

(1) * * *

* * * * * * *

(5) the term "Federal crime of terrorism" means an offense that—

(A) * * *

(B) is a violation of—

(i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 175c (relating to variola virus), 229 (relating to chemical weapons), subsection

(a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnaping), 831 (relating to nuclear materials), 832 (relating to participation in nuclear and weapons of mass destruction threats to the United States) 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers), 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through [(v) (relating to protection of computers)] *(vi) (relating to the protection of computers)*, 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1361 (relating to government property or contracts), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to terrorist attacks and other acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air), 2155 (relating to destruction of national defense materials, premises, or utilities), 2156 (relating to national defense material, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2332f (relating to bombing of public places and facilities), 2332g (relating to missile systems designed to destroy aircraft), 2332h (relating to radiological dispersal devices), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), 2339C (relating to financing of terrorism), 2339D (relating to military-type training from a for-

eign terrorist organization), or 2340A (relating to torture) of this title;

* * * * * * *

○