Calendar No. 181

112TH CONGRESS
1st Session

SENATE

REPORT
112–91

PERSONAL DATA PRIVACY AND SECURITY ACT OF 2011

NOVEMBER 7, 2011.—Ordered to be printed

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

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 1151]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to which was referred the bill (S. 1151), to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information, having considered the same, reports favorably thereon, with an amendment, and recommends that the bill, as amended, do pass.

CONTENTS

I. BACKGROUND AND PURPOSE OF THE PERSONAL DATA PRIVACY AND SECURITY ACT OF 2011

A. SUMMARY

Advanced technologies, combined with the realities of the post-9/11 digital era, have created strong incentives and opportunities for collecting and selling personal information about ordinary Americans. Today, private sector and governmental entities alike routinely traffic in billions of electronic personal records about Americans. Americans rely on this data to facilitate financial transactions, provide services, prevent fraud, screen employees, investigate crimes, and find loved ones. The Government also relies upon this information to enhance national security and to combat crime.

The growing market for personal information has also become a treasure trove that is both valuable and vulnerable to identity thieves. As a result, the consequences of a data security breach can be quite serious. For Americans caught up in the endless cycle of watching their credit unravel, undoing the damage caused by security breaches and identity theft can become a time-consuming and lifelong endeavor. In addition, while identity theft is a major privacy concern for most Americans, the use and collection of personal data by Government agencies can have an even greater impact on Americans' privacy. The loss or theft of Government data can potentially expose ordinary citizens, Government employees, and members of the armed services alike to national security and personal security threats.

Despite these well-known dangers, the Nation's privacy laws lag far behind the capabilities of technology and the cunning of identity thieves. The Personal Data Privacy and Security Act of 2011 is a comprehensive privacy bill that seeks to close this privacy gap by establishing meaningful national standards for providing notice of data security breaches, and by addressing the underlying problem of lax data security to make it less likely for data security breaches to occur in the first place.

B. THE GROWING PROBLEM OF DATA SECURITY BREACHES AND IDENTITY THEFT

Since the Personal Data Privacy and Security Act was first reported by the Judiciary Committee in November 2005, more than 535 million records containing sensitive personal information have been involved in data security breaches, according to the Privacy Rights Clearinghouse.[1] For example, during the spring of 2011, Sony disclosed several major data breaches involving its PlayStation Network, Qriocity music and video service and Sony Online Entertainment service, exposing the sensitive personal information of more than 101 million users.[2] In another high-profile data security breach, a computer hacker penetrated the databases of the online marketing firm Epsilon, compromising name and email address information about the customers of scores of major

[1] See "Privacy Rights Clearinghouse Chronology of Data Breaches," available at http://www.privacyrights.org/.

[2] "Sony Data Breach Tally Rises to 101 Million," eWeek.com, May 3, 2011.

U.S. businesses, including Target, Citigroup, and Walgreen, and affecting the privacy of millions of U.S. consumers.[3]

In January 2009, Heartland Payment Systems, one of the Nation's leading processors of credit and debit card transactions, announced that its processing system records containing more than 130 million credit card accounts had been breached by hackers. In January 2007, mega-retailer TJX disclosed that it suffered a data breach affecting at least 45.7 million credit and debit cards.[4] These data breaches follow many other major commercial data breaches, including breaches at ChoicePoint and LexisNexis.

Federal Government agencies, and even the Congress, have not been immune to data security breaches. In June 2011, computer hackers affiliated with the hacker group known as Lulz Security breached the United States Senate website.[5] In February 2009, the Federal Aviation Administration revealed that computer hackers breached one of its servers and stole sensitive personal information concerning 45,000 current and former FAA employees.[6] In June 2008, Walter Reed Medical Center reported that the personal information of 1,000 Military Health System beneficiaries may have been improperly disclosed through the unauthorized sharing of data.[7] In May 2006, the Department of Veterans Affairs lost an unsecured laptop computer hard drive containing the health records and other sensitive personal information of approximately 26.5 million veterans and their spouses.[8] And, in May, 2007, the Transportation Security Administration (TSA) reported that the personal and financial records of 100,000 TSA employees were lost after a computer hard drive was reported missing from the Agency's headquarters, exposing the Department of Homeland Security to potential national security risks.[9]

The steady wave of data security breaches in recent years is a window into a broader, more challenging trend. Insecure databases are now low-hanging fruit for hackers looking to steal identities and commit fraud. Lax data security is also a threat to American businesses. The President's report on Cyberspace Policy Review noted that industry estimates of losses from data theft of intellectual property in 2008 alone range as high as $1 trillion.[10] Because data security breaches adversely affect many segments of the American community, a meaningful solution to this growing problem must carefully balance the interests and needs of consumers, business, and the Government.

---

[3] "Fact box: U.S. data breach hits Target, Marriott customers," Reuters/MSNBC, April 4, 2011.

[4] "Breach of data at TJX is called the biggest ever, Stolen numbers put at 45.7 million," Boston Globe, March 29, 2007.

[5] "Hackers Break into Senate Computers," Reuters, June 14, 2011.

[6] "FAA Breach Heightens Cybersecurity Concerns," Federal Computer Week, February 23, 2009.

[7] "Walter Reed: Data Breach at Military Hospitals," The Associated Press, June 3, 2008.

[8] See Testimony of the Honorable James Nicholson, Secretary of Veterans Affairs, before the House Committee on Government Reform, June 8, 2006.

[9] See "TSA seeks hard drive, personal data for 100,000," USA Today, May 5, 2007; see also, the Federal Times, "Union Sues TSA over loss of data on employees," May 9, 2007.

[10] "President's Report on Cyberspace Policy Review," May 29, 2009, at page 2. A recent report to Congress by the Office of the National Counterintelligence Executive also found that cyber-espionage conducted by, among others, China and Russia has resulted in the theft of tens of billions of dollars of trade secrets, technology and intellectual property from U.S. Government and private computer systems each year. See "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011," October, 2011.

C. THE PERSONAL DATA PRIVACY AND SECURITY ACT OF 2011

The Personal Data Privacy and Security Act of 2011 takes several meaningful and important steps to balance the interests and needs of consumers, business, and the Government in order to better protect Americans sensitive personal data. This legislation is supported by a wide range of consumer, business, and government organizations.

1. Data security program

The bill recognizes that, in the Information Age, any company that wants to be trusted by the public must earn that trust by vigilantly protecting the information that it uses and collects. The bill takes important steps to accomplish this goal by requiring that companies that have databases with sensitive personal information on more than 10,000 Americans establish and implement a data privacy and security program. There are exemptions to this requirement for companies already subject to and in compliance with data security requirements under the Gramm-Leach-Bliley (GLB) Act and the Health Information Portability and Accountability (HIPAA) Act. Section 202(a)(4)(C) directs companies to consider data minimization as part of their data security program planning process. Eliminating personal data that is no longer needed is a crucial and basic element of good data security practice. By contrast, retaining sensitive data that is no longer needed for a business purpose unnecessarily creates rich targets for data breaches and identity theft.[11]

In addition, in light of the largely passive role of certain service providers that provide electronic data transmission, routing, intermediate and transient storage, or connections services with respect to sensitive personally identifiable information, the bill assigns limited obligations to such businesses. In the bill, the term "service provider" is defined as a business entity that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network for sensitive personally identifiable information on an undifferentiated basis from other information that such entity transmits, routes, or stores, or for which such entity provides connections. Section 201(b)(3) of the bill exempts such service providers from the data security program requirements in the bill, to the extent that the service provider is exclusively engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication. By "exclusively," the Committee intends that a service provider is exempt only to the extent it is engaged in the activities of a service provider as defined by the bill. The Committee also recognizes that a service provider may also be engaged in activities that are covered by the bill and does not intend that that an entity would lose the service provider exemption for its purely service provider functions.[12]

[11] For example, one of the recent breaches suffered by Sony included the financial information of tens of thousands of individuals held on an "outdated" database that the company retained but no longer used. This practice put the outdated data at an even greater risk of breach, because little attention was given to the safekeeping of the data.

[12] The Committee notes that with respect to section 202(d) of the bill, the "providers of services" under this provision are not the same entities as the "service providers" defined by the bill. The entities subject to this provision are persons or entities other than service providers, with whom a business entity contracts for services other than the services or functions of a serv-

2. Notice

Second, because American consumers should know when they are at risk of identity theft or other harms because of a data security breach, the bill also requires that business entities and Federal agencies promptly notify affected individuals and law enforcement when a data security breach occurs. Armed with such knowledge, consumers can take steps to protect themselves, their families, and their personal and financial well-being. Additionally, law enforcement can also take the steps needed to mitigate or thwart a cyberattack. Notice to individuals must be provided within 60 days following discovery of the security breach, unless delayed by the Federal Trade Commission, or Federal law enforcement. The trigger for notice to individuals is "significant risk of identity theft, economic loss or harm, or physical harm," and this trigger includes appropriate checks and balances to prevent over-notification and underreporting of data security breaches.

In this regard, the bill recognizes that there are harms other than identity theft that can result from a data security breach, including harm from other financial crimes, stalking, and other criminal activity. Consequently, the bill adopts a trigger of "significant risk of identity theft, economic loss or harm, or physical harm, rather than a weaker trigger of "significant risk of identity theft," for the notice requirement for individuals in the legislation. There are exemptions to the notice requirements for individuals for national security and law enforcement reasons, as well as an exemption to this requirement for credit card companies that have effective fraud-prevention programs.[13] The bill also includes a safe harbor exemption from the notice requirement if the business entity or agency that suffered the security breach concludes, after conducting a risk assessment, that no significant risk of identity theft, economic harm or loss, or physical harm exists and the FTC concurs with that determination. The bill contemplates that a reasonable delay of notice could include the time necessary for a victimized business or agency to conduct a risk assessment under Section 212(b).

In addition, to strengthen the tools available to law enforcement to investigate data security breaches, combat identity theft and protect cybersecurity, the bill also requires that business entities and Federal agencies notify a new Government office to be established by the Secretary of the Department of Homeland Security of certain major security breaches that are likely to affect law enforcement or national security. Such notice to law enforcement is to be

---

ice provider. This provision does not impose any obligation on service providers to enter into contracts or implement or maintain the requirements of section 201 or 202 or subtitle B.

[13] Some have incorrectly argued that S. 1151 will result in over-notification of consumers and in a lack of clarity for business. To the contrary, the bill contains meaningful checks and balances, including the risk assessment and financial fraud prevention provisions in Section 212, to prevent over-notification and the underreporting of data security breaches. The risk assessment provision in Section 212 furthermore, provides businesses with an opportunity to fully evaluate data security breaches when they occur, to determine whether notice should be provided to consumers. In addition, the bill compliments and properly builds upon other Federal statutes governing data privacy and security to ensure clarity for business in this area. For example, to avoid conflicting obligations regarding the bill's data security program requirements, Section 201(c) specifically exempts financial institutions that are already subject to, and complying with, the data privacy and security requirements under GLB, as well as HIPAA-regulated entities. The bill also builds upon existing Federal laws and guidance, such as the data security protections established by the Office of the Comptroller of the Currency for financial institutions.

provided within 10 days following discovery of the security breach and at least 72 hours before providing notice to individuals. The new Government office will be responsible for disseminating the information that it receives to the Secret Service, FBI and the Federal Trade Commission (FTC), and to other Federal enforcement agencies as warranted. This notice will provide law enforcement with a valuable head start in pursuing the perpetrators of cyber intrusions and identity theft. The bill also empowers the FTC, Secret Service and FBI to obtain additional information about the data breach from business entities and Federal agencies to determine whether notice of the breach should be given to consumers.

This notice mechanism also gives businesses and agencies certainty as to their legal obligation to provide notice and prevents them from sending notices when they are unnecessary, which over time, could result in consumers ignoring such notices. The notice of breach provisions for electronic health records that Congress enacted in the American Reinvestment and Recovery Act (ARRA) apply to information that is accessed or disclosed from personal health records. The notice of breach provisions in this bill are not intended to preempt the notice requirements established by ARRA.

The bill also recognizes the benefits of separating the notice obligations of owners of sensitive personally identifiable information and third parties who use and manage sensitive personally identifiable information on the owner's behalf. The bill imposes an obligation on third parties that suffer a data security breach to notify the owners or licensees of the sensitive personally identifiable information, who would, in turn, notify consumers. If the owner or licensee of the data gives notice of the breach to the consumer, then the breached third party does not have to give notice. The bill also states that it does not abrogate any agreement between a breached entity and a data owner or licensee to provide the required notice in the event of a breach. Separating the notice obligations between data owners and licensees, and third parties, will encourage data owners and licensees to address the notice obligation in agreements with third parties and will help to ensure that consumers will receive timely notice from the entity with which they have a direct relationship. However, this notice can only be effective if the entity that suffers the breach, and any other third parties, provide to the entity who will give the notice complete and timely information about the nature and scope of the breach and the identity of the entity breached.

As discussed above, the bill assigns limited obligations to service providers when solely engaging in certain conduct involving the transmission, routing, intermediate and transient storage, or when connecting to a system or network. A service provider's breach notification obligations under subtitle B of title II are exclusively set out in Section 211(b)(4) of the bill, which provides that if a service provider becomes aware of a security breach of data in electronic form containing sensitive personal information that is owned or possessed by another business entity that connects to or uses the service provider's system or network for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider is only required to notify the business entity who initiated the connection, transmission, routing, or storage.

Such notice is required only in those cases where such business entity reasonably can be identified.

3. Enforcement

Third, the legislation also establishes tough, but fair, enforcement provisions to punish those who fail to notify consumers of a data security breach, or to maintain a data security program. The bill makes it a crime for any individual, with knowledge of the obligation to provide notice of a security breach, to intentionally and willfully conceal the breach that subsequently causes economic harm to consumers. Violators of this provision are subject to a criminal fine under title 18, or imprisonment of up to five years, or both. This provision is no more onerous than criminal provisions for other types of fraudulent conduct that cause similar harm to individuals.

The bill also contains strong but fair civil enforcement provisions. The bill authorizes the Secret Service, FBI and the FTC to investigate data security breaches and to provide guidance to companies that have been the victim of a data security breach on their notice obligations under the bill. The bill also authorizes the FTC to bring a civil enforcement action for violations of the data security program requirements in the bill and to recover a civil penalty of not more than $5,000 per violation, per day and a maximum penalty of $500,000 per violation. Double penalties may be recovered for intentional and willful violations of these requirements. The bill provides that the determination about the amount of the civil penalty is to be made by the court. The bill also allows State Attorneys General to bring civil actions to recover these civil penalties in United States District Court. However if the FTC initiates a civil action to recover penalties, the bill also prohibits State Attorneys General from commencing another civil action against the same defendant, based on the same or related violations.

In addition, the bill contains strong, but fair civil enforcement provisions for the requirements to provide notice of a security breach. The bill authorizes the FTC and the Attorney General of the United States to bring a civil enforcement action to recover a civil penalty of up to $11,000 per day per security breach and a maximum penalty of $1,000,000 for violation of the security breach notice requirements. Double penalties may be recovered for intentional and willful violations. The bill provides that the determination about the amount of the civil penalty is to be made by the court. The bill also allows State Attorneys General to bring civil actions to recover these civil penalties in United States District Court. However, if the Attorney General or the FTC initiates a civil action to recover penalties, the bill prohibits State Attorneys General from commencing another civil action against the same defendant, based on the same or related violations.

It is not uncommon for Congress to authorize both Federal and State regulators to enforce Federal consumer protection laws. In fact, Federal antitrust laws, the CAN–SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003), and the Communications Act of 1934 also authorize State Attorneys General to seek damages or to enjoin further Federal law violations. The State enforcement provisions in this bill are modeled after those laws.

4. Preemption

The legislation also carefully balances the need for Federal uniformity in certain data privacy laws and the important role of States as leaders on privacy issues. Section 204 of the bill (relation to other laws) preempts State laws with respect to requirements for administrative, technical, and physical safeguards for the protection of sensitive personally identifying information. These requirements are the same requirements set forth in Section 202 of the bill. Section 204(b) of the bill also makes clear that the data security requirements in the bill do not preempt the Gramm-Leach-Bliley Act or that law's implementing regulations, including those regulations adopted or enforced by States.

Section 219 of the bill (effect on Federal and State laws) also preempts State laws on breach notification for entities that are subject to the bill. The Committee intends for this provision to preempt State data breach laws only with respect to the business entities and Federal agencies covered by the bill. However, in recognition of the important role that the States have played in developing breach notification, the bill carves out an exception to preemption for State laws regarding providing consumers with information about victim protection assistance that is provided for by the State.

In addition, Section 219 of the bill provides that the notice requirements in the bill supersede "any provision of law of any State relating to notification of a security breach, except as provided in Section 214(b) of the bill." The bill's subtitle on security breach notification applies to "any agency, or business entity engaged in interstate commerce," and the term "agency" is defined in the bill by referencing section 551 of title 5, United States Code, which pertains to Federal Governmental entities. As a result, the security breach notification requirements in the bill have no application to State and local governmental entities, and the Committee does not intend for this provision to preempt or displace State laws that address obligations of State and local governmental entities to provide notice of a security breach.

Gramm-Leach-Bliley Act-covered and Health Insurance Portability and Accountability Act-covered entities are not subject to the bill. Consequently, the preemption provisions in the bill similarly do not apply to those entities. It is possible, however, that other Federal laws that govern these entities could preempt State law.

5. Criminal provisions

Developing a comprehensive strategy for cybersecurity that includes a response to cybercrime remains a pressing challenge. For this reason, the bill includes, among other things, several cybercrime provisions that update the Computer Fraud and Abuse Act, so that this law remains a viable tool for law enforcement to respond to emerging cyber threats.

First, the bill creates a new criminal offense for causing damage to a critical infrastructure computer that manages or controls national defense, national security, transportation, public health and safety, or other critical infrastructure systems. This new offense includes a three-year mandatory minimum sentence. The mandatory minimum sentence drew bipartisan opposition from several Judiciary Committee members during the Committee's consideration of

the provision. In particular, Chairman Leahy expressed concern that the mandatory minimum sentence would lead to unfair sentencing results, while not adding any deterrence value.[14]

Second, the bill amends title 18, United States Code, section 1961(1) to add violations of the Computer Fraud and Abuse Act to the definition of racketeering activity. This update to the law will make it easier for the Government to prosecute certain organized criminal groups that engage in computer network attacks.

Third, Section 102 of the bill also makes it a crime for a person who knows of a security breach which requires notice to individuals under the bill, and who is under obligation to provide such notice, to intentionally and willfully conceal the fact of, or information related to, that security breach. Punishment is either a fine under title 18, or imprisonment of up to 5 years, or both.

Fourth, the bill contains several other amendments to the Computer Fraud and Abuse Act. Section 103 amends title 18, United States Code, section 1030(c), to streamline and enhance the penalty structure under section 1030. Section 104 expands the scope of the offense for trafficking in passwords under section 1030(a)(6) to include passwords used to access a protected Government or non-government computer. Section 105 amends section 1030(b) to clarify that both conspiracy and attempt to commit a computer hacking offense are subject to the same penalties as completed, substantive offenses. Section 106 amends 1030(i) and (j) to clarify the criminal forfeiture provision in section 1030 and to create a civil forfeiture provision to provide the procedures governing civil forfeiture.

To address civil liberties concerns about the scope of the Computer Fraud and Abuse Act, the bill amends the Computer Fraud and Abuse Act to exclude from criminal liability conduct that exclusively involves a violation of a contractual obligation or agreement, such as an acceptable use policy, or terms of service agreement. In particular, the definition for "exceeds authorization" in the statute is amended by the bill to exclude conduct solely involving a violation of a contractual agreement. The purpose of this amendment is to make clear that Congress does not intend for the Department of Justice to pursue criminal prosecutions under that statue for conduct solely involving a violation of a terms of use agreement or contractual agreement involving a private, non-government computer. The Committee does not, however, intend to prohibit the Department of Justice from using evidence of such contractual violations to support a charge under 1030, when coupled with other evidence.

During the Judiciary Committee hearing, several Members of the Committee, including the Chairman, raised concerns about the Justice Department's decision to bring criminal charges in *United States* v. *Lori Drew*, which involved a Computer Fraud and Abuse Act charge based solely upon a violation of a MySpace terms of service agreement.[15] In his testimony before the Committee, Asso-

---

[14] Full Committee Markup of the Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011) [hereinafter Markup] (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary).

[15] In the *Drew* case, Ms. Drew was alleged to have violated a MySpace terms of service agreement by creating a false user identity, which she used to bully a teenager. The teenager later committed suicide. A jury found Ms. Drew guilty of a misdemeanor violation of the Computer Fraud and Abuse Act, because she exceeded the authorization to use MySpace. A Federal judge subsequently overturned the jury's misdemeanor conviction. *United States* v. *Lori Drew*, No CR 08–0582–GW (C.D. Cal. Aug. 28, 2009). In doing so, the court concluded that permitting a viola-

Continued

ciate Deputy Attorney General James Baker responded to concerns about the *Drew* prosecution by noting that the case was an anomaly. Specifically, Mr. Baker noted that if Congress responded to the *Drew* case by "restricting the statute [by prohibiting claims bases solely upon a violation of terms of use or contractual agreements] . . . [that] would make it difficult or impossible to deter and address serious insider threats through prosecution." In addition, Mr. Baker cautioned against treating violations of contractual agreements in cyberspace any differently from violations of such agreements in other context. For example, he noted the fact that law enforcement can prosecute an employee who acts in violation of an office policy. Mr. Baker conceded that the Department of Justice would not appeal the court's decision to overturn the conviction in the *Drew* case.

Finally, to further address this issue, Section 107 of the bill amends section 1030(g) to preclude civil claims based exclusively on conduct that involves a violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement. Section 108 also adds a new reporting requirement to section 1030 that requires that the Attorney General annually report to Congress on the number of criminal cases brought under section 1030(a) in which the sole basis for the Government determining that access to the non-governmental computer was unauthorized, or in excess of authorization, was that the defendant violated a contractual obligation or agreement.

II. History of the Bill and Committee Consideration

A. Introduction of the Bill

Chairman Leahy introduced the Personal Data Privacy and Security Act of 2011 on June 7, 2011. This privacy bill is cosponsored by Senators Schumer, Cardin, Franken and Blumenthal.

This legislation is very similar to the Personal Data Privacy and Security Act of 2009, S. 1490, which Senator Leahy introduced on July 22, 2009, the Personal Data Privacy and Security Act of 2007, S. 495, which Senators Leahy and Specter introduced on July 6, 2007, and to the Personal Data Privacy and Security Act of 2005, S. 1789, which Senators Leahy and Specter introduced on September 29, 2005. The Judiciary Committee favorably reported S. 1490 by a bipartisan vote of 14 Yeas and 5 Nays on November 5, 2009; S. 495 on May 3, 2007, by voice vote and S. 1789 on November 17, 2005, by a bipartisan vote of 13 to 5.

The Committee has held two hearings related to S. 1151. On June 21, 2011, the Judiciary Committee's Subcommittee on Crime and Terrorism held a hearing entitled, "Cybersecurity: Evaluating the Administration's Proposals." This hearing examined the data breach and cybercrime proposals contained in the Obama administration's legislative package on cybersecurity. The following witnesses testified at this hearing: The Honorable Jim Langevin (D–RI), Member, United States House of Representatives; James A.

---

tion of a website's terms of service to constitute an intentional access of a computer without authorization or exceeding authorization under the Computer Fraud and Abuse Act would "result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals." Id. at 29. The Justice Department did not appeal the decision.

Baker, Associate Deputy Attorney General, U.S. Department of Justice; Greg Schaffer, Acting Deputy Under Secretary, National Protection and Programs Directorate, Department of Homeland Security; and Ari Schwartz, Senior Internet Policy Advisor, National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

On September, 7, 2011, the Judiciary Committee held a hearing entitled, "Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats." This hearing examined the cybercrime proposals contained in the Obama administration's cybersecurity proposal, including the criminal proposals contained in S. 1151. The following witnesses testified at this hearing: James A. Baker, Esq., Associate Deputy Attorney General, U.S. Department of Justice and Pablo A. Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, and United States Secret Service.

B. COMMITTEE CONSIDERATION

On September 7, 2011, S. 1151 was placed on the Judiciary Committee's agenda. The Committee considered this legislation on September 15 and 22, 2011.

During the Committee's consideration of S. 1151, six amendments to the bill were offered and five amendments were adopted by the Committee:

First, the Committee adopted, without objection, a complete substitute bill for S. 1151 (ALB11637), which Chairman Leahy offered. The substitute bill made several changes to the bill, including (1) striking the data broker and Government use titles in the bill; (2) adding a new criminal provision making it a felony to intentionally damage a critical infrastructure computer; (3) adding a knowledge requirement and economic harm requirement in the amount of at least $1,000 to the criminal provision on concealment of a security breach; (4) clarifying that the definition of security breach excludes public records and information obtained from public records; (5) modifying the trigger for breach notice to "substantial risk of identity theft, economic loss or harm, or physical harm"; (6) clarifying that enforcement actions brought by State Attorneys General may only be brought in U.S. District Court; and (7) making technical corrections to the bill.

Second, the Committee adopted, without objection, a manager's amendment (ALB11713) to S. 1151 which Chairman Leahy also offered. The manager's amendment made several changes to the bill, including: (1) adopting an amendment filed by Senator Grassley (HEN11631) to strike language authorizing the Federal Trade Commission to modify the definition for sensitive personally identifiable information in the bill through rulemaking; (2) making several technical changes to Section 202(d) regarding service providers; (3) adding limitation on liability language; (4) amending the State Attorney General Enforcement provisions in Section 203 to clarify that if a Federal civil or criminal action has been filed, a State cannot bring another action for the same violation; (5) striking the technical requirements for the risk assessment; (6) amending Sections 217 and 218 to clarify that civil penalties are calculated per security breach, per day and adding limitation on liability language; (7) amending the State Attorney General Enforce-

ment provisions in Section 218 to clarify that if a Federal civil or criminal action has been filed, a State cannot bring another action for the same violation; and (8) clarifying the preemption provision in Section 219, so that the bill does not preempt the Gramm-Leach-Bliley Act, or the Health Insurance Portability and Accountability Act; (9) clarifying that the preemption provision governing State data breach laws applies only to the entities subject to the bill; (10) clarifying the GLB carve-outs for the data security program and data breach provisions in Sections 201 and 211; and (11) making other technical changes to the bill.

Third, the Committee adopted by voice vote an amendment offered by Senator Grassley (JEN11A19) to amend the definition of "exceeds authorized access" in title 18, United States Code, section 1030, to exclude conduct that only involves violating a terms of use agreement, or other contractual agreement governing the use of a non-government computer.

Fourth, when the Committee resumed consideration of the bill on September 22, 2011, Senator Grassley offered an amendment (ALB11652) to add a mandatory minimum sentence to the damage of critical infrastructure computers offense in Section 109 of the bill. The amendment was accepted on a roll call vote. The vote record is as follows:

Tally: 11 Yeas, 7 Nays

Yeas (11): Feinstein (D–CA), Schumer (D–NY), Whitehouse (D–RI), Klobuchar (D–MN), Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (D–AL), Graham (R–SC), Cornyn (R–TX), and Coburn (R–OK).

Nays (7): Leahy (D–VT), Kohl (D–WI), Durbin (D–IL), Franken (D–MN), Coons (D–DE), Blumenthal (D–CT), and Lee (R–UT).

Fifth, the Committee adopted by voice vote a second degree amendment offered by Senator Franken (HEN11688) to Senator Grassley's amendment (HEN11637) that added a data minimization requirement to the data security program requirements in the bill.

Sixth, the Committee rejected by voice vote an amendment offered by Senator Grassley (HEN11637) that would have struck the data security program requirements in the bill.

Seventh, Senator Grassley offered an amendment (ALB11646) to prohibit State Attorneys General from retaining private counsel on a contingency fee basis to enforce the civil enforcement provisions in the bill. The amendment was rejected on a roll call vote. The vote record is as follows:

Tally: 7 Yeas, 11 Nays

Yeas (7): Feinstein (D–CA), Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (D–AL), Cornyn (R–TX), and Lee (R–UT).

Nays (11): Leahy (D–VT), Kohl (D–WI), Schumer (D–NY), Durbin (D–IL), Whitehouse (D–RI), Klobuchar (D–MN), Franken (D–MN), Coons (D–DE), Blumenthal (D–CT), Graham (R–SC), and Coburn (R–OK).

The Committee then voted to report the Personal Data Privacy and Security Act of 2011, as amended, favorably to the Senate. The Committee proceeded by roll call vote as follows:

Tally: 10 Yeas, 8 Nays

Yeas (10): Leahy (D–VT), Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Durbin (D–IL), Whitehouse (D–RI), Klobuchar (D–MN), Franken (D–MN), Coons (D–DE), and Blumenthal (D–CT).

Nays (8): Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (R–AL), Graham (R–SC), Cornyn (R–TX), Lee (R–UT), and Coburn (R–OK).

III. Section-by-Section Summary of the Bill

Section 1—Short title

This section provides that the legislation may be cited as the "Personal Data Privacy and Security Act of 2011."

Section 2—Findings

Section 2 provides Congressional findings on the threats posed by data security breaches and cybercrime.

Section 3—Definitions

Section 3 contains the definitions used in the bill.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

Section 101—Organized criminal activity in connection with unauthorized access to personally identifiable information

Section 101 amends 18 U.S.C. § 1961(1) to add violations of the Computer Fraud and Abuse Act to the definition of racketeering activity. This change would increase certain penalties, and make it easier for the Government to prosecute certain organized criminal groups who engage in computer network attacks.

Section 102—Concealment of security breaches involving personally identifiable information

Section 102 makes it a crime for a person who knows of a security breach which requires notice to individuals under Title II of this Act, and who is under obligation to provide such notice, to intentionally and willfully conceal the fact of, or information related to, that security breach. Punishment is either a fine under Title 18, or imprisonment of up to 5 years, or both.

Section 103—Penalties for fraud and related activity in connection with computers

Section 103 amends title 18, United States Code, section 1030(c) to streamline and enhance the penalty structure under section 1030.

Section 104—Trafficking in passwords

Section 104 expands the scope of the offense for trafficking in passwords under title 18, United States Code, section 1030(a)(6) to include passwords used to access a protected government or non-government computer, and to include any other means of unauthorized access to a government computer.

Section 105—Conspiracy and attempted computer fraud offenses

Section 105 amends title 18, United States Code, section 1030(b) to clarify that both conspiracy and attempt to commit a computer hacking offense are subject to the same penalties as completed, substantive offenses.

Section 106—Criminal and civil forfeiture for fraud and related activity in connection with computers

Section 106 amends title 18, United States Code, sections 1030(i) and (j) to clarify the criminal forfeiture provision in section 1030 and to create a civil forfeiture provision to provide the procedures governing civil forfeiture, to clarify that the proceeds that may be forfeited under section 1030 are gross proceeds, as opposed to net proceeds, and to allow for the forfeiture of real property used to facilitate section 1030 offenses.

Section 107—Limitations on civil actions

Section 107 amends title 18, United States Code, section 1030(g) to preclude civil claims based exclusively on conduct that involves a violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement. The purpose of the amendment is to prevent civil claims based on innocuous conduct.

Section 108—Reporting of certain criminal cases

Section 108 adds a new reporting requirement to section 1030, requiring that the Attorney General annually report to Congress on the number of criminal cases brought under section 1030(a) in which the defendant either exceeded authorized access to a non-governmental computer, or accessed a non-governmental computer without authorization, and in which the sole basis for the Government determining that access to the non-governmental computer was unauthorized, or in excess of authorization, was that the defendant violated a contractual obligation or agreement with a service provider or employer. The purpose of the provision is to address concerns that the Government could bring criminal cases under section 1030 for relatively innocuous conduct, such as violating a terms of use agreement.

Section 109—Damage to critical infrastructure computers

Section 109 adds a new criminal provision to tile 18 specifically making it a felony to damage a computer that manages or controls national defense, national security, transportation, public health and safety, or other critical infrastructure systems or information. Violations are subject to a fine and/or imprisonment of at least three years and up to 20 years.

TITLE II—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

SUBTITLE A—A DATA PRIVACY AND SECURITY PROGRAM

Section 201—Purpose and applicability of data privacy and security program

Section 201 addresses the data privacy and security requirements of Section 202 for business entities that compile, access, use, process, license, distribute, analyze or evaluate personally identifiable information in electronic or digital form on 10,000 or more U.S. persons. Section 201 exempts from the data privacy and security requirements of Section 202 businesses already subject to, and complying with, similar data privacy and security requirements under GLB and implementing regulations, as well as examination for compliance by Federal functional regulators as defined in GLB, and HIPPA regulated entities.

Section 202—Requirements for a data privacy and security program

Section 202 requires covered business entities to create a data privacy and security program to protect and secure sensitive data. The requirements for the data security program are modeled after those established by the Office of the Comptroller of the Currency for financial institutions in its *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 12 C.F.R. § 30.6 Appendix B (2005).

A data privacy and security program must be designed to ensure security and confidentiality of personal records, protect against anticipated threats and hazards to the security and integrity of personal electronic records, protect against unauthorized access and use of personal records, and ensure proper back-up storage and disposal of personally identifiable information. In addition, Section 202 requires a covered business entity to: (1) regularly assess, manage and control risks to improve its data privacy and security program; (2) provide employee training to implement its data privacy and security program; (3) conduct tests to identify system vulnerabilities; (4) ensure that overseas service providers retained to handle personally identifiable information, but which are not covered by the provisions of this Act, take reasonable steps to secure that data; and (5) periodically assess its data privacy and security program to ensure that the program addresses current threats. Section 202 also requires that the data security program include measures that allow the data broker (1) to track who has access to sensitive personally identifiable information maintained by the data broker and (2) to ensure that third parties or customers who are authorized to access this information have a valid legal reason for accessing or acquiring the information.

Section 203—Enforcement

Section 203 gives the Federal Trade Commission the right to bring an enforcement action for violations of Sections 201 and 202 in Subtitle A. Business entities that violate sections 201 and 202 are subject to a civil penalty of not more than $5,000 per violation, per day and a maximum penalty of $500,000 per violation. Intentional and willful violations of these sections are subject to an addi-

tional civil penalty of $5,000 per violation, per day and an additional maximum penalty of $500,000 per violation. This section also grants States the right to bring civil actions on behalf of their residents in U.S. district courts, and requires States to give advance notice of such court proceedings to the FTC, where practicable. There is no private right of action under this subtitle.

Section 204—Relation to other laws

Section 204 preempts State laws relating to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information. The requirements referred to in this Section are the same requirements set forth in Section 202.

SUBTITLE B—SECURITY BREACH NOTIFICATION

Section 211—Notice to individuals

Section 211 requires that a business entity or Federal agency give notice to an individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, compromised, following the discovery of a data security breach. The notice required under Section 211 must be made without unreasonable delay and no more than 60 days after the discovery of the breach, unless extended by the Federal Trade Commission.

Section 211(b) requires that a business entity or Federal agency that does not own or license the information compromised as a result of a data security breach notify the owner or licensee of the data. The owner or licensee of the data would then provide the notice to individuals as required under this Section. However, agreements between owners, licensees and third parties regarding the obligation to provide notice under Section 211 are preserved. In addition, Section 211(b) provides that service providers who only transmit or route electronic data that is subject to a security breach must notify the owner of the data of the security breach. The owner of the data has the obligation to notify the individuals whose data was breached.

Section 212(d) allows the Secret Service or FBI to delay the notice required under Section 211, if notice would impede a criminal investigation, or harm national security. The delay period is for 30 days, unless extended by law enforcement.

Section 212—Exemptions

Section 212 provides for certain exemptions to the notice requirements under Section 211, for national security and law enforcement purposes, a safe harbor, and financial fraud programs.

Section 212(a) allows the Secret Service, or Federal Bureau of Investigation to prevent notice if the providing of such notice would reveal sensitive sources and methods, impede a criminal investigation, or damage national security.

Section 212(b) exempts a business entity or Federal agency from providing notice, if the business or Federal agency conducts a risk assessment and determines that there is no significant risk that the security breach will result in harm or fraud to the individuals whose sensitive personally identifiable information has been compromised. The business entity or Federal agency must notify the Federal Trade Commission of the results of the risk assessment

within 45 days of the security breach and if the Federal Trade Commission concurs with the determination, notice is not required. Under Section 212(b) a rebuttable presumption exists that the use of encryption technology, or other technologies that render the sensitive personally identifiable information indecipherable means that there is no significant risk of harm, or fraud. The provision also provides certain requirements for the risk assessment and states that a failure to satisfy these requirements, or submitting a risk assessment with false information, constitutes a violation of the provision.

Section 212(c) also provides a financial fraud prevention exemption from the notice requirement, if a business entity has a program to block the fraudulent use of information—such as credit card numbers—to avoid fraudulent transactions. Debit cards and other financial instruments are not covered by this exemption.

Section 213—Methods of notice

Section 213 provides that notice to individuals may be given in writing to the individuals' last known address, by telephone or via email notice, if the individual has consented to email notice. Media notice is also required if the number of residents in a particular State whose information was, or is reasonably believed to have been compromised exceeds 5,000 individuals.

Section 214—Content of notification

Section 214 requires that the notice detail the nature of the personally identifiable information that has been compromised by the data security beach, a toll free number to contact the business entity or Federal agency that suffered the breach, and the toll free numbers and addresses of major credit reporting agencies. Section 214 also preserves the right of States to require that additional information about victim protection assistance be included in the notice.

Section 215—Coordination of notification with credit reporting agencies

Section 215 requires that, for situations where notice of a data security breach is required for 5,000 or more individuals, a business entity or Federal agency must also provide advance notice of the breach to consumer reporting agencies.

Section 216—Notice to law enforcement

Section 216 requires that the Secretary of Homeland Security designate a Federal Government entity to receive all of the notices (law enforcement, risk assessment and national security) required under Sections 212 and 216 within 60 days of the enactment of the Act. The Section further requires that business entities and Federal agencies notify this Federal entity of the fact that a security breach has occurred as promptly as possible, but at least 72 hours before notice is given to individuals and no less than 10 days after discovery of the security breach, if the data security breach involves: (1) more than 5,000 individuals; (2) a database that contains information about more than 500,000 individuals; (3) a Federal Government database; or (4) individuals known to be Federal Government employees or contractors involved in national security

or law enforcement. The entity designated by the Secretary of Homeland Security is responsible for promptly notifying Federal law enforcement agencies, including the Secret Service, FBI and FTC, of the data security breach. The FTC, in consultation with the Attorney General and Secretary of Homeland Security, shall promulgate regulations to clarify the reporting required by this section and to adjust the thresholds.

Section 217—Enforcement

Section 217 provides that the Attorney General and Federal Trade Commission may bring a civil action to recover penalties for violations of the notification requirements in Subtitle B. Violators are subject to a civil penalty of up to $11,000 per day, per security breach. There is a maximum penalty cap of $1 million per security breach. Intentional or willful conduct is subject to an additional penalty of up to $11,000 per day, per security breach, with a maximum penalty of an additional $1 million. The provision also requires that the Department of Justice and FTC coordinate enforcement of this provision and also coordinate with other Federal enforcement agencies as warranted.

Section 218—Enforcement by State Attorneys General

Section 218 allows State Attorneys General to bring a civil action in U.S. district court to enforce Subtitle B. The Attorney General may stay, or intervene in, any State action.

Section 219—Effect on Federal and State law

Section 219 preempts State laws on breach notification, with the exception of State laws regarding providing consumers with information about victim protection assistance that is available to consumers in a particular State. Because the breach notification requirements in the bill do not apply to State and local government entities, this provision does not preempt State or local laws regarding the obligations of State and local government entities to provide notice of a data security breach.

Section 220—Reporting on risk assessment exemptions

Section 220 requires that, no later than 18 months after enactment, the Federal Trade Commission report to Congress on the number and nature of data security breach notices invoking the risk assessment exemption and that the Secret Service and FBI report to Congress on the number and nature of data security breaches subject to the national security and law enforcement exemptions.

Section 221—Effective date

Subtitle B takes effect 90 days after the date of enactment of the Personal Data Privacy and Security Act.

TITLE III—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

Section 301—Budget compliance

Section 301 contains the language required to comply with the Pay-As-You-Go Act.

IV. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The Committee sets forth, with respect to the bill, S. 1151, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

OCTOBER 27, 2011.

Hon. PATRICK J. LEAHY,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1151, the Personal Data Privacy and Security Act of 2011.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Matthew Pickford (for federal costs), and Marin Randall (for the impact on the private sector).

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

S. 1151—Personal Data Privacy and Security Act of 2011

Summary: S. 1151 would establish new federal crimes relating to unauthorized access to sensitive personal information. The bill also would require most federal agencies and businesses that collect, transmit, store, or use such personal information to establish a data privacy and security program and to notify any individuals whose information has been unlawfully accessed.

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 1151 would cost $14 million over the 2012–2016 period. Enacting S. 1151 could increase civil and criminal penalties and could affect direct spending by agencies not funded through annual appropriations; therefore, pay-as-you-go procedures apply. CBO estimates, however, that any changes to revenues and net direct spending would be negligible.

S. 1151 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the cost of complying with the requirements would be small and would not exceed the threshold established in UMRA ($71 million in 2011, adjusted annually for inflation).

S. 1151 also would impose several private-sector mandates. Much of the private sector already complies with many of the bill's requirements. However, a large number of entities in the private sector would need to implement new or enhanced security standards if the bill is enacted. Consequently, CBO estimates that the aggregate direct cost of the mandates in the bill would probably exceed the annual threshold established in UMRA for private-sector mandates ($142 million in 2011, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

Estimated cost to the Federal Government: The estimated budgetary impact of S. 1151 is shown in the following table. The costs of this legislation fall within budget functions 050 (national defense), 370 (commerce and housing credit), 750 (administration of

justice), 800 (general government), and other budget functions that contain salaries and expenses.

	By fiscal year, in millions of dollars—					
	2012	2013	2014	2015	2016	2012–2016
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	3	3	3	3	3	15
Estimated Outlays	2	3	3	3	3	14

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted early in 2012, that the necessary amounts will be provided each year, and that spending will follow historical patterns for similar programs.

Spending subject to appropriation

Most of the provisions of the bill would codify the current practices of the federal government regarding data security and procedures for notifying individuals whose personal information may have been disclosed. In general, a data breach occurs when sensitive, protected, or confidential information is copied, transmitted, viewed, or stolen by someone not authorized to do so. The federal government is one of the largest providers, collectors, consumers, and disseminators of personal information in the United States. Although CBO cannot anticipate the number or extent of breaches, a significant breach of security involving a major collector of personal information, such as the Internal Revenue Service or the Social Security Administration, could involve millions of individuals and result in significant costs to notify those individuals of such a breach. Existing laws generally do not require federal agencies to notify affected individuals of such security breaches; however, agencies that have experienced security breaches have generally provided such notification. Therefore, CBO expects that codifying this practice would probably not lead to a significant increase in spending.

The legislation also would require a business entity or federal agency—under certain circumstances—to notify the Department of Homeland Security that a security breach has occurred but would permit entities or agencies to apply to the federal government for a delay or exemption from the requirements if the personal data were encrypted or similarly protected or if notification would threaten national security. Other provisions of the bill would require the Federal Trade Commission (FTC) to develop and enforce regulations to implement the bill's new requirements for data security programs and policies. Finally, S. 1151 would require federal agencies to provide several reports to the Congress, which would include the number and type of data breaches.

Based on information from the Department of Homeland Security, the Federal Bureau of Investigation, the FTC, and other agencies with a significant information technology presence, CBO estimates that additional investigative and administrative work under the bill would cost about $3 million annually, subject to the availability of appropriated funds.

Direct spending and revenues

S. 1151 would establish new federal crimes relating to unauthorized access to sensitive personal information. Enacting the bill 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 result. Civil fines are recorded as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and subsequently spent without further appropriation.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting S. 1151 would have a negligible effect on direct spending and revenues.

Estimated impact on state, local, and tribal governments: S. 1151 contains intergovernmental mandates as defined in UMRA because it would explicitly preempt laws in at least 46 States regarding the treatment of personal information and impose notification requirements and limitations on State Attorneys General. Because the limits on State authority would impose no duties with costs and because the notification requirements would result in minimal additional spending, CBO estimates that the costs of the mandates would be small and would not exceed the threshold established in UMRA for intergovernmental mandates ($71 million in 2011, adjusted annually for inflation).

Estimated impact on the private sector: S. 1151 would impose several private-sector mandates as defined in UMRA by:

- Requiring certain business entities that handle personally identifiable information for 10,000 or more individuals to establish and maintain a data privacy and security program;
- Requiring any business entity engaged in interstate commerce to notify individuals if a security breach occurs in which such individuals' sensitive personally identifiable information is compromised;
- Requiring providers of electronic communication services to inform any user that initiated transmission of data on their network if they become aware of a data breach; and
- Limiting existing rights to seek damages against a person if the only basis for the suit is the violation of a contractual obligations involving the use of computers or access to personal information.

The majority of businesses already comply with data security standards and breach notification procedures similar to many of the bill's requirements. However, some of the requirements in the bill would impose new standards for data maintenance and security on a large number of entities in the private sector. Consequently, CBO estimates that the aggregate direct cost of all the mandates in the bill would probably exceed the annual threshold established in UMRA for private-sector mandates ($142 million in 2011, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

Data privacy and security requirements

Subtitle A of title II would require businesses engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more individuals to establish and maintain a program for data privacy and security. The program would be designed to protect against both unauthorized access and any anticipated vulnerabilities. Business entities would be required to conduct periodic risk assessments to identify such vulnerabilities and assess possible security risks in establishing the program. Additionally, businesses would have to train their employees in implementing the data security program.

The bill would direct the FTC to develop rules that identify privacy and security requirements for the business entities covered under subtitle A. Some businesses would be exempt from the requirements of subtitle A. Those include certain financial institutions that are subject to the data security requirements under the Gramm-Leach-Bliley Act, entities that are subject to the data security requirements of the Health Insurance Portability and Accountability Act, and providers of electronic communications services to the extent that they are exclusively engaged in the temporary storage, transmission, or routing of data.

The cost per entity of the data privacy and security requirements would depend on the rules to be established by the FTC, the size of the entity, and its current ability to secure, record, and monitor access to data, as well as on the amount of sensitive, personally identifiable information maintained by the entity. The majority of States already have laws requiring business entities to utilize data security programs, and it is the current practice of many businesses to use security measures to protect sensitive data. However, some of the new standards for data security in the bill could impose additional costs on a large number of private-sector entities.

For example, under the bill, businesses covered under subtitle A would be required to enhance their security standards to include the ability to trace access and transmission of all records containing sensitive personally identifiable information. The current industry standard on data security has not reached that level. According to industry experts, information on a particular individual can be collected from several places and, for large companies, can be accessed by thousands of people from several different locations. The ability to trace each transaction involving data containing personally identifiable information would require a significant enhancement of data management hardware and software for the majority of businesses. Further, the bill's definition of sensitive personally identifiable information is broader than the current industry standard.

This definition would significantly increase the number of entities that would be required to implement new or enhanced data security standards. The aggregate cost of implementing such changes could be substantial.

Notification of security breaches

Subtitle B of title II would require business entities engaged in interstate commerce that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information to notify indi-

viduals in the event of a security breach if the individuals' sensitive, personally identifiable information is compromised. Entities would be able to notify individuals using written letters, the telephone, or email. If a business does not own or license the information, it would have to notify the owner or licensee of the information following a breach. A notice in major media outlets serving a State or jurisdiction also would have to be provided for any breach of more than 5,000 residents' records within a particular State. In addition, businesses would be required to notify other entities and agencies in the event of a large security breach.

Entities that experience the breach of such data would have to notify the affected victims and consumer reporting agencies if the breach involves more than 5,000 individuals. The bill, however, would exempt business entities from the notification requirements under certain circumstances.

According to industry sources, the sensitive personally identifiable information of millions of individuals is illegally accessed or otherwise breached every year. However, according to those sources, 46 states already have laws requiring notification in the event of a security breach. In addition, it is the standard practice of most business entities to notify individuals if a security breach occurs. Therefore, CBO estimates that the notification requirements would not impose significant additional costs on businesses.

The subtitle also contains a provision requiring providers of electronic communication services (such as Internet service providers) to inform the entity that began a transmission of information using their systems if they become aware that a breach of sensitive personally identifiable information has occurred. This would constitute a mandate on those service providers. The cost to inform business entities of a breach would probably be small.

Elimination of existing rights of action

Title I would eliminate certain existing rights of action against individuals for violating contractual agreements involving the use of computers or access to personal information. Currently, a lawsuit may be filed against an individual for exceeding authorized access (obtaining or altering information without the proper authorization) and computer fraud if that individual violates the terms of a related contractual agreement. The bill would eliminate any right of action alleging someone has exceeded authorized access or committed computer fraud when the only basis for the suit is the violation of a related agreement. Because there are few such cases, CBO estimates that the cost of the mandate would be minimal.

Estimate prepared by: Federal costs: Department of Homeland Security—Jason Wheelock; Federal Trade Commission—Susan Willie; U.S. Secret Service—Mark Grabowicz; Other Federal agencies—Matthew Pickford.

Impact on State, local, and Tribal Governments: Elizabeth Cove Delisle.

Impact on the private sector: Marin Randall.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

V. Regulatory Impact Evaluation

In compliance with rule XXVI of the Standing Rules of the Senate, the Committee finds that no significant regulatory impact will result from the enactment of S. 1151.

VI. Conclusion

The Personal Data Privacy and Security Act of 2011, S. 1151, provides greatly needed privacy protections to American consumers and businesses, to ensure that all Americans have the tools necessary to protect themselves from identity theft and other data security risks. This legislation will also ensure that the most effective mechanisms and technologies for dealing with the underlying problem of lax data security are implemented by the Nation's businesses to help prevent data breaches from occurring in the first place. The passage and enactment of this important privacy legislation is long overdue.

VII. Additional and Minority Views

ADDITIONAL VIEWS FROM SENATOR COONS

I was pleased to support the Personal Data Privacy and Security Act of 2011, which will bolster the security of sensitive personal data held by companies and improve notice to consumers in the event of a data breach. In this age of digital commerce, the stakes surrounding data security are high and will only increase. This legislation will help promote consumer trust and corporate accountability.

As I mentioned during Committee consideration, I believe the bill could be further improved if the preemption standards were strengthened. In particular, I believe it is counterproductive to subject banks and financial services entities already regulated under the Gramm-Leach-Bliley Act to a patchwork of differing or conflicting state laws governing data breach and consumer notice. Accordingly, as this bill moves forward to full Senate consideration, I will work to ensure that the preemption provisions in S. 1151 are broadened to establish uniform preemption of state laws where Congress has established a national regime for data security and breach notification.

CHRISTOPHER A. COONS.

MINORITY VIEWS FROM SENATORS GRASSLEY, KYL, SESSIONS, GRAHAM, CORNYN, AND COBURN

This legislation seeks a solution to a real problem, but it fails to deliver. Protecting an individual's sensitive personal identifying information, recognizing vulnerabilities to information and providing notification when a breach of information has occurred must be addressed. We support a clear, uniform, national standard that directs when notice to consumers and law enforcement should be provided. Consumers should have access to alerts identifying threats that pose a significant risk of identity theft. When appropriate notice is given, consumers can work with other entities to limit risk and protect their identity. This also means that businesses will possess the ability to minimize risk and protect their consumers' sensitive personal information from any further threats.

Yet at the same time, we must not numb a consumer's senses to risk notification. Legislation should not encourage or foster an environment where the default response from a business is to always issue notice. Requiring notice for trivial security incidents will lead to over-notification, which in turn will create broad apathy as consumers are inundated with inconsequential warnings. Moreover, the security breach that does threaten an individual's identity may be ignored. While the purpose of this bill is to protect individuals, the effect will be the exact opposite as consumers will suffer due to constant notification.

Additionally, the financial and bureaucratic costs associated with this bill will burden small and medium sized businesses at exactly the wrong time. We know that excessive government regulation has a detrimental effect on businesses, imposing heavy burdens on small business which must comply or face substantial liability penalties. Such regulations may have the effect of bankrupting these businesses. During these difficult economic times and unemployment northward of 9%, this costly legislation is not prudent.

While we commend the Chairman's efforts on this particular subject, we cannot support S. 1151 at this time. We believe it is counterproductive to our shared goal of consumer protection, as it will lead to consumer over-notification, increased financial costs due to new regulations, while imposing excessive liability penalties for failure to comply, ultimately leading to further job losses throughout the economy.

BACKGROUND

Identity theft is a problem for both consumers and businesses. This problem intensifies as criminals become increasingly sophisticated at breaching businesses' security systems in order to obtain sensitive information. This threat is not just limited to private business but to the government as well. Business and government work to understand past and present incidents so as to prevent fu-

ture attacks. Law enforcement at the federal, state and local levels work together and with private business to enhance controls, protect information, and improve cooperation should a breach occur. Private businesses, which ultimately bear the major cost of fraud resulting from an attack, have spent billions of dollars to strengthen data security, seeking ways to stop fraud before it happens.

Underlying the need for a uniform, federal standard is the expansive growth of State government activity on this matter. Since 2002, 46 states and the District of Columbia have enacted laws that seek to prevent identity theft, while requiring businesses who suffer a data breach to provide notice to consumers detailing the risk to their sensitive personal information.[1] Moreover, the trend continues this year as 14 states have introduced legislation that expands the scope of the laws, creating new and additional notification requirements as well as new penalties for those responsible for a breach.[2] Due to the ever changing differences between the various state laws, there is a need for a single, uniform, federal standard.

However, as Congress works to craft legislation we must ensure there are tools in place to assist consumers in protecting themselves should a breach occur. It is important that consumers know when their information is compromised so they can obtain resources in order to protect themselves. For notice to be effective, consumers should be notified when their sensitive personal information is compromised in a way that jeopardizes their identities. Otherwise, over-notification will lead to consumer apathy and, therefore, will expose consumers to greater risk.

MANDATED "ONE SIZE FITS ALL" DATA PRIVACY AND SECURITY PROGRAMS

Section 202 of this bill creates a prescriptive, one size fits all data security program requirement that businesses with sensitive personal information of more than 5,000 individuals must follow. Many small businesses, which can easily acquire data on more than 5,000 individuals, will be unduly burdened, facing increased compliance costs that may force a small business to close its doors. Moreover, this burden becomes greater given the bill's expanded definition of sensitive personally identifiable information in section 3. Instead, we believe a more flexible approach should be provided to businesses, appropriate to the size and nature of the respective business.

We agree that businesses should have a plan in place to ensure the safety of sensitive information. Unfortunately, rather than avoid the pitfalls of over regulation, which is a legitimate concern to many businesses already facing economic hardships, this bill adds to the problem. The Congressional Budget Office recognizes this fact in its cost estimate contained in this report. It is disappointing that this bill fails to recognize that there are tremendous differences and other factors present with various businesses. This bill fails to take into account those differences in two ways.

---

[1] National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/Default.aspx?TabId=13489 (last visited Oct. 31, 2011).

[2] National Conference of State Legislatures, Security Breach Legislation 2011, http://www.ncsl.org/default.aspx?tabid=22295 (last visited Oct. 31, 2011).

First, this bill applies complex requirements from Congress to all businesses that exceed current industry practices. For example, over the span of almost seven pages, section 202 lists detailed requirements for a personal data privacy and security program that must be implemented. A business must perform risk assessments, risk management and control, and training and vulnerability testing, among other requirements. A small business with one or two employees, that finds itself subject to these requirements, must take the time to be sure it is complying with these requirements, otherwise it will be subject to exorbitant liability penalties.

In addition to the specific requirements set forth in this bill, the checklist for compliance is not complete. Section 202 punts to the Federal Trade Commission the authority to add further, ever changing, requirements for businesses that must have data privacy and security programs in place. The Federal Trade Commission, through a routine rulemaking process, can add "any other administrative, technical, or physical safeguards" deemed necessary. Again, ever changing rules will unduly burden small and medium sized businesses that not only must comply with the congressional requirements, but new requirements from the federal bureaucracy. The combination of congressional and agency requirements will unduly harm small businesses.

We recognize, as do others, that increased government regulation can suppress a business's ability to survive and grow. As the Congressional Budget Office cost estimate contained in this report points out, the new requirements in section 202 go beyond the scope of the security measures many businesses currently have in place. Imposing new requirements that exceed the industry standard, coupled with Federal Trade Commission rulemaking of those requirements and an expansive definition of sensitive personally identifiable information, will create substantial costs to businesses already struggling against over regulation and a weak economy. Before a bill on this matter becomes law, it is important that the requirements in section 202 are reexamined in order to avoid what would be a legislative nightmare for many businesses.

OVER-NOTIFICATION

This bill provides in section 211 a default rule that notice should always be given to consumers of any breach, "following the discovery" of a security breach. Only if after conducting a risk assessment, under section 212(b), may a business entity be exempt from providing notice. The burden that is placed on businesses will inevitably lead to consumer over-notification. As discussed above, the bill's definition of sensitive personally identifiable information is broader than the current industry standard. This means breached information that otherwise would not previously have required notice due to its inability to pose a risk of identity theft, will now require consumer notification. The costs associated with the risk assessment, which must be coordinated with bureaucrats at the Federal Trade Commission, will exact a high toll on small businesses that are not differentiated in any manner from large businesses. Rather than face high liability penalties for failure to comply, the result will be simply to provide notification for trivial incidents

that will have the effect of desensitizing the public, while also punishing the business which is a victim as well.

The "safe harbor" provision in section 212(b) attempts to limit instances where notification is required. However, the end result will remain the same due to the way this provision is drafted. Rather than risk the penalties for failure to notify, a business will in most instances err on the side of caution and give notice. Again, the bill's default rule is that notice should always be given following the discovery of a security breach. However, an entity can perform a risk assessment, in consultation with the Federal Trade Commission, to determine that there is "no significant risk that a security breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm" to the individuals whose personal information was subject to the breach. Thus, a business must make the determination that in no instance could there be a significant risk of "identity theft, economic loss or harm, or physical harm." Rather than play offense against a breach, a business will always find itself on defense. The business will try and anticipate several steps into the future to determine whether to provide notice. This is an impossible task which renders the risk assessment worthless as there may always be an unknown and unforeseen risk that cannot be predicted. A business will therefore do what is in its best interest, which may not necessarily be in an individual consumer's best interest, and issue notice whenever a security incident occurs.

Unfortunately, there is no relief for a weary business faced with making a determination whether notice is required, while trying to limit any further security incidents. In order to perform a risk assessment and take advantage of the safe harbor, a business must consult with the Federal Trade Commission, another layer in the bureaucratic minefield, which must be informed of a business's decision to invoke the safe harbor following the risk assessment. If the Federal Trade Commission "does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given[,]" then no notice is required. However, it is not unreasonable to anticipate the exact opposite effect occurring as a result of this provision. Instead, it is reasonable to question whether the Federal Trade Commission will be able to process the potentially high number of risk assessment results that will inundate its office as a result of this bill's mandate. This is because the expansive definition of sensitive personally identifiable information, along with the trigger for when notice should be provided, will inevitably lead to greater notification and risk assessment reports. Unless the Federal Trade Commission operates efficiently and timely when reviewing risk assessments, then the risk of over-notification will only continue to rise. An over worked Commission staffer may face a quickly approaching 10-day deadline and choose to err on the side of caution and instruct a business to provide notice.

Rather than attempt to limit notification to security breaches that pose a significant risk of identity theft, S. 1151 will create serious over-notification problems which will desensitize consumers and lead to widespread apathy. A business must always give notice unless after performing a risk assessment in consultation with the Federal Trade Commission it is determined there is no significant risk of "identity theft, economic loss or harm, or physical harm."

The initial decision a business will make is whether it is beneficial to jump through the risk assessment hoops, which will involve dealing with a federal agency, and instead simply issue notice. Assuming a business does decide to try and invoke the safe harbor, it is quite possible that an over-burdened Federal Trade Commission will simply instruct a business to issue notice. Rather than placing a default rule that notice must always be given, unless a risk assessment determines otherwise, perhaps a better approach would be to require notice only when there is a significant risk of identity theft. This subtle burden shifting may work to eliminate all but those notifications that pose the greatest threat to a consumer's sensitive personal information.

EXCESSIVE PENALTIES

Another troubling aspect of this bill is its excessive penalties. Under section 203, businesses that make a mistake in complying with the requirements of sections 201 and 202 may be held liable at a rate of "$5,000 per violation per day while such violation exists with a maximum of $500,000 per violation." Section 202 imposes no less than seven requirements on businesses, not counting the numerous subsections. A mistake in compliance with any one of those requirements is a potential violation, running at a rate of $5,000 per day. Moreover, that business would likely be facing arguments by government attorneys that its conduct was willful or intentional, thereby deserving an additional penalty of up to $500,000 more.

Under sections 217 and 218, if a business makes a mistake in providing notice to a person whose information may have been compromised, that business will be facing a penalty of "$11,000 per day per security breach" up to $1 million. That business will also be facing arguments by government attorneys that its conduct was intentional or willful, deserving an additional penalty of up to $1 million.

The Chairman has made an effort to address the problem of "stacked damages," which existed in the original version of his bill. The potential for stacked damages increases the amount of the already excessive penalties. By his manager's amendment, the Chairman has inserted "penalty limits" into the enforcement sections of the bill. For example, under section 203, "the total sum of civil penalties assessed against a business entity for all violations . . . resulting from the same or related acts or omissions shall not exceed $500,000, unless such conduct is found to be willful or intentional."

The purpose of these "penalty limit[ation]" provisions is to prevent the situation where a business makes a mistake which results in it "violating" all seven requirements under section 202 and thereby facing liability at a rate of $35,000 per day, and up to $3.5 million. Under the "penalty limit[ation]" provision, if a business makes multiple mistakes, as part of the same conduct, it will be facing a potential penalty of $5,000 per day, up to $500,000. Similarly, under sections 217 and 218, if a business suffers a security breach and makes a mistake in notifying ten individuals, whose information was compromised, that business will be facing penalties of $11,000 per day, up to $ 1 million. It will not be facing a potential penalty of $110,000 per day and up to $10 million.

The "penalty limit[ation]" provisions and some of the other changes made by the Chairman are a step in the right direction. Hopefully, the changes signal a willingness to further refine this bill, which covers a significant and complex issue. However, in its current form, the bill's penalties remain excessive, especially when applied to small and medium sized businesses. Many businesses facing these penalties will be forced into bankruptcy.

Remarkably, during the debate on this bill, the majority never expressed any concern about bankrupting businesses or that the businesses facing these excessive penalties are victims of a crime as their computers will have been hacked. This is a disturbing omission given that as of September 2011, 14 million Americans were unemployed and another 9.3 million were underemployed.[3]

In addition to facing these excessive penalties, businesses will be forced to hire defense attorneys, who are well versed in computer and cybersecurity issues. There are only a handful of law firms that are fully versed in the subject matter, and which have the experience and manpower to defend a business in a lawsuit filed by the Department of Justice, the Federal Trade Commission and/or State Attorneys General. Those few multinational or large businesses that might consider defending themselves will spend money on attorneys, computer experts and litigation costs, as opposed to hiring new employees and creating jobs.

Our concerns are not a matter of protecting businesses that have committed wrongs. We strongly believe that it is important to protect our citizens from identity theft. However, our approach must be fair and balanced. And again, it should not be forgotten that we are talking about businesses that have made a "mistake" in complying with this law. Consequently, the amount of a penalty should be a reasonable deterrent. It should not be destructive. Indeed, during these difficult economic times, Congress should be helping businesses to create jobs, not passing legislation that has the real potential to bankrupt businesses and kill jobs.

ETHICAL ISSUES

Another troubling aspect of this bill is the fact that it allows State Attorneys Generals to hire private law firms on a contingency fee basis to enforce it. This raises serious ethical concerns. A neutral and impartial government is a fundamental requirement for due process. Employing trial lawyers on a contingency fee basis will result in governmental power being wielded by lawyers primarily interested in benefiting themselves, rather than in doing justice. At the very minimum, the appearance of State Attorneys General handing out valuable contracts with a chance for private attorneys to receive contingency fees is disconcerting. As former Alabama Attorney General Bill Pryor (now a judge on the U.S. Court of Appeals for the Eleventh Circuit) once explained that "[t]hese [contingency] contracts . . . create the potential for out-

[3] Bureau of Labor Statistics, U.S. Department of Labor, News Release, "The Employment Situation—September 2011" (Oct. 7, 2011) (available at http://www.bls.gov/news.release/pdf/empsit.pdf) (last visited Oct. 31, 2011).

rageous windfalls or even outright corruption for political supporters of the officials who negotiated the contracts."[4]

Personal financial interest should not affect the judgment of an attorney representing the government. The faith and trust of the public in the government's fair and impartial use of its powers is critical to our system of government. Accordingly, an attorney who represents the government must be neutral and impartial, with no personal or financial stake in the case. Neutral and impartial justice is not merely a goal. It is a matter of well-established federal and state law. An Executive Order forbids the federal government from hiring private attorneys on a contingency basis.[5] Also, 28 U.S.C. § 528 disqualifies any employee of the Department of Justice from participating in case that may result in a personal, financial, or political conflict of interest, or the appearance thereof.

The practice of hiring trial lawyers on a contingency fee basis should be ended altogether and it certainly should not be extended into this new law. Accordingly, Senator Grassley offered Amendment ALB11646 to the bill. That amendment would have prohibited State Attorneys General from hiring private law firms on a contingency fee basis to enforce this new federal law. Contrary to the claims of the majority, this issue is not a matter of states' rights. Nor is it a question of states with budget problems needing to hire trial lawyers on a contingent fee basis.

This issue is a matter of basic and fundamental ethics and it is a matter of due process. The focus of this bill should be about creating a reasonable national standard to protect Americans from identity theft. It should not be about creating revenue for trial lawyers. Senator Grassley's amendment should have been adopted.

MULTIPLE LAWSUITS

Another concern with the enforcement provisions is the likelihood that they will breed multiple lawsuits against businesses, which are all based on the same mistake or conduct. Specifically, under the bill as introduced, a business could have been subjected to lawsuits by the Department of Justice or the Federal Trade Commission and anywhere between one and fifty States Attorneys General. No small or medium size business could defend against that onslaught, let alone survive it.

The Chairman's manager's amendment begins to address this problem by providing that if the Department of Justice or Federal Trade Commission commences an enforcement action, "no attorney general of a State may bring an action for a violation . . . that resulted from the same or related acts or omissions against a defendant named in the Federal criminal proceeding or civil action. . . ." The purpose of this provision is to prevent businesses from having to defend against lawsuits by both the Federal and State governments. If there is an enforcement action, there should only be one lawsuit and preferably, it should be a federal enforcement action.

These provisions in sections 203 and 218 of the bill are a step in the right direction. To fully address the issue, the bill should be amended to also require state lawsuits to be withdrawn with preju-

[4] William H. Pryor, Jr., *Curbing the Abuses of Government Lawsuits Against Industries*, Speech Before the American Legislative Exchange Council, Aug. 11, 1999, at 8.

[5] Exec. Order No. 13433, 72 Fed. Reg. 28441 (May 16, 2007).

dice, if the Department of Justice or Federal Trade Commission commences an enforcement action after one or more State Attorneys General files a lawsuit. In the end, all of the concerns about the enforcement and liability provisions are well-founded and must be resolved before we can support this bill.

To further address multiple lawsuits, this bill amends the Computer Fraud and Abuse Act to bar civil claims and criminal charges resulting from a violation of a "Term of Service Agreement" with a non-government employer. This amendment is intended to bar all contract-based CFAA litigation, except when based on a government employment contract, while allowing the Department of Justice to bring charges under 18 U.S.C. 1030 when based on other evidence.

CRIMINAL PROVISIONS

The bill does establish a new criminal offense for damage to a critical infrastructure computer system such as electrical power grids, water supply systems and nuclear power plants. Unfortunately, the majority report blatantly mischaracterizes the provision of the bill passed by the Committee, which includes an amendment Senator Grassley offered that imposes a mandatory minimum sentence of three years' imprisonment for the newly created crime of aggravated damage to a critical infrastructure computer. The majority, while noting that the Chairman opposed the mandatory minimum, fails to mention that the President himself included that mandatory minimum in the cyber-security bill he proposed to the Congress earlier this year.

The Chairman's original draft of S. 1151 removed the President's proposed mandatory minimum for a violation of aggravated damage to a critical infrastructure computer. Senator Grassley offered his amendment to recognize the serious nature of a cyber-attack damaging critical infrastructure and restore the mandatory minimum in line with the President's proposal. Furthermore, during Associate Deputy Attorney General James A. Baker's testimony, in his appearance before the Committee on September 7, 2011, he explicitly endorsed, on behalf of the DOJ, the three-year mandatory minimum.

Thus, in support of the President and with DOJ's endorsement, the Committee voted in favor of the Grassley amendment by a vote of 11–7. In an attempt to diminish the significance of this vote, the majority characterizes the 7 votes in opposition to the amendment as "bi-partisan," because one Republican member voted against it. It is far more noteworthy, however, that four members of the Chairman's party agreed with Senator Grassley and his Republican colleagues.

CONCLUSION

Protecting an individual's sensitive personally identifiable information is of the utmost importance. However, this must be done in a way that will ensure individuals are notified when there are actual threats to their identity. Unfortunately, this bill fails to accomplish this goal as individuals will find their email inboxes full every morning with notifications of security incidents that a business issues for fear of violating one of the requirements in this bill. The

prescriptive regulation and high penalties will likely end up forcing some businesses to shut their doors. As drafted, this bill punishes businesses, while providing no real benefit for consumers.

CHARLES E. GRASSLEY.
JON KYL.
JEFF SESSIONS.
LINDSEY GRAHAM.
JOHN CORNYN.
TOM COBURN.

VIII. CHANGES TO EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, 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 material is printed in italic, existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

PART I—CRIMES

* * * * * * *

CHAPTER 47—FRAUD AND FALSE STATEMENTS

* * * * * * *

* * * * * * *

SEC. 1030A. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) DEFINITIONS.—In this section—

(1) the terms "computer" and "damage" have the meanings given such terms in section 1030; and (2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

(A) gas and oil production, storage, and delivery systems;

(B) water supply systems;

(C) telecommunication networks;

(D) electrical power delivery systems;

(E) finance and banking systems;

(F) emergency services;

(G) transportation systems and services; and

(H) government operations that provide essential services to the public

(b) OFFENSE.—It shall be unlawful to, during and in relation to a felony violation of section 1030, intentionally cause or attempt to cause damage to a critical infrastructure computer, and such damage results in (or, in the case of an attempt, would, if completed have resulted in) the substantial impairment—

(1) of the operation of the critical infrastructure computer; or

(2) of the critical infrastructure associated with the computer.

(c) PENALTY.—Any person who violates subsection (b) shall be fined under this title, imprisoned for not less than 3 years nor more than 20 years, or both.

(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

(1) a court shall not place on probation any person convicted of a violation of this section;

(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation section 1030;

(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any

way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

* * * * * * *

SEC. 1041. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

* * * * * * *

(a) IN GENERAL.—Whoever, having knowledge of a security breach and of the fact that notice of such security breach is required under title II of the Personal Data Privacy and Security Act of 2011, intentionally and willfully conceals the fact of such security breach, shall, in the event that such security breach results in economic harm to any individual in the amount of $1,000 or more, be fined under this tile or imprisoned for not more than 5 years, or both.

(b) PERSON DEFINED.—For purposes of subsection (a), the term "person" has the same meaning as in section 1030(e)(12) of title 18, United States Code.

(c) NOTICE REQUIREMENT.—Any person seeking an exemption under section 212(b) of the Personal Data Privacy and Security Act of 2011 shall be immune from prosecution under this section if the Federal Trade Commission does not indicate, in writing, that such notice be given under section 212(b)(3) of such Act.

* * * * * * *

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) 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) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

[(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;**]**

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in—

(A) any password or similar information through which a protected computer as defined in subparagraphs (A) and (B) of subsection (e)(2) may be accessed without authorization; or

(B) any means of access through which a protected computer as defined in subsection (e)(2)(A) may be accessed without authorization;

(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 obtain information from a protected computer without authorization or in excess of authorization or 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;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided *for the completed offense* 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), 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 this section, 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) 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 subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

[(i) 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 an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

[(VI) damage affecting 10 or more protected computers during any 1-year period; or

[(ii) an attempt to commit an offense punishable under this subparagraph;

[(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

[(i) 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 subclauses (I) through (VI) of subparagraph (A)(i); or

[(ii) an attempt to commit an offense punishable under this subparagraph;

[(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

[(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

[(ii) an attempt to commit an offense punishable under this subparagraph;

[(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

[(i) an offense or an attempt to commit an offense under subsection (a) (5)(C) that occurs after a conviction for another offense under this section; or

[(ii) an attempt to commit an offense punishable under this subparagraph;

[(E) 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, imprisonment for not more than 20 years, or both;

[(F) 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, imprisonment for any term of years or for life, or both; or

[(G) a fine under this title, imprisonment for not more than 1 year, or both, for—

[(i) any other offense under subsection (a)(5); or

[(ii) an attempt to commit an offense punishable under this subparagraph.]

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

(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under paragraph (a)(2) of this section, if—

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

(ii) the offense was committed in the 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, or that would have been obtained if the offense was completed, exceeds $5,000;

(3) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(3) of this section;

(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

(5)(A) except as provided in subparagraph (D), 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) of this section, if the offense 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 on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(vi) damage affecting 10 or more protected computers during any 1-year period;

(B) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

(C) 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, imprisonment for any term of years or for life, or both; or

(D) a fine under this title, imprisonment for not more than 1 year, or both, for another offense under subsection (a)(5);

(6) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

(7) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.

* * * * * * *

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

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

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(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;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a Financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or ⟦alter;⟧ *alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;*

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any State, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution financial institution, governmental entity, or legal or other entity.

* * * * * * *

(g)*(1)* 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 subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(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.

(2) No action may be brought under this subsection if a violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, constitutes the sole basis for determining that access to the protected computer is unauthorized, or in excess of authorization.

* * * * * * *

[(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—**]**

[(A) such 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 that such person obtained, directly or indirectly, as a result of such violation.

[(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.**]**

(i) CRIMINAL FORFEITURE.—

(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

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

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

(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

[(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

[(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

[(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section.]

(j) CIVIL FORFEITURE.—

(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

(2) Seizures and forfeitures under this subsection shall be governed by the provisions in 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, United States Code, shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.

(k) REPORTING CERTAIN CRIMINAL CASES.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the Attorney General shall report to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives the number of criminal cases brought under subsection (a) that involve conduct in which—

(1) the defendant—

(A) exceeded authorized access to a non-governmental computer; or

(B) accessed a non-governmental computer without authorization; and

(2) the sole basis for the Government determining that access to the non-governmental computer was unauthorized, or in excess of authorization was that the defendant violated a contractual obligation or agreement with a service provider or employer, such as an acceptable use policy or terms of service agreement.

* * * * * * *

CHAPTER 96—RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS

* * * * * * *

SEC. 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) if the act is a felony*, 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 phone records computer programs 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 229–229F (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);

* * * * * * *

○