SECTION-BY-SECTION FOR THE
PERSONAL DATA PRIVACY AND SECURITY ACT OF 2011
SUBSTITUTE

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 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

Section109 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 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 additional 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 within 14 days of the breach, if the data security breach involves: (1) more than 10,000 individuals; (2) a database that contains information about more than 1 million individuals; (3) a Federal Government databases; 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 and FBI, of the data security breach.

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 individual. 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 brought under this subtitle.

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 to 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.