Section–by-Section Analysis

LAW ENFORCEMENT PROVISIONS RELATED TO COMPUTER SECURITY

Part 1: The Computer Fraud and Abuse Act (CFAA, at 18 U.S.C. §1030) establishes a series of criminal offenses for attacks on the confidentiality, integrity, and availability of computers. While these crimes apply to the computers and networks that run our critical infrastructure, there is no mandatory minimum penalty for such offenses. While it is reasonable to believe that courts would impose appropriately deterrent prison terms if an attack severely debilitates a critical infrastructure system, it is possible that courts might not impose adequate penalties for attacks that cause less disruption (or none at all in the case of an attempt that is thwarted before it is completed). This proposal would therefore create a mandatory minimum penalty for these sorts of attacks. The language is patterned on the very successful mandatory sentence for identity theft offenses, 18 U.S.C. § 1028A (Aggravated Identity Theft).

Part 2: This proposal would clarify several existing criminal offenses relating to attacks on computers and computer networks and enhance their penalties. Specifically, the proposal:

- Adds offenses under the Computer Fraud and Abuse Act (CFAA at 18 U.S.C. §1030) to the list of Racketeering Influenced and Corrupt Organizations Act (RICO at 18 U.S.C. §1961(1)). This change would increase certain penalties, and make it easier to prosecute certain organized criminal groups who use computer network attacks.
- Clarifies that both conspiracy and attempt to commit a computer hacking offense are subject to the same penalties as completed, substantive offenses.
- Condenses and clarifies the penalty provisions (18 U.S.C. §1030(c)) by removing references to subsequent convictions in favor of setting a maximum sentence for each offense – in general, the maximum would be the number of years currently designated for a second offense.
- Amends 18 U.S.C. § 1030(i) and (j) to (1) create a civil forfeiture provision, (2) designate Chapter 46 of Title 18 as providing the procedures governing civil forfeiture, (3) clarify that the "proceeds" forfeitable under section 1030 are gross proceeds, as opposed to net proceeds, and (4) allow forfeiture of real property used to facilitate offenses under section 1030 in appropriate cases.
- Expands the scope of the offense for trafficking in passwords (18 U.S.C. §1030(a)(6)), for example, to cover passwords for access to any protected computer, not just government computers or where the trafficking affects interstate or foreign commerce.
- Enhances the criminal penalties for several of the offenses under 18 U.S.C. §1030.

Section–by-Section Analysis

DATA BREACH NOTIFICATION

Sec. 1 – Establishes definitions for key terms under this Title. In pertinent part, section 101 defines:

- A "business entity" as any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.
- A "security breach" as a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data through misrepresentation or actions that results in, or there is a reasonable basis to conclude has resulted in, (1) the unauthorized acquisition of sensitive personally identifiable information; or (2) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

Notably, lawfully- authorized investigative, protective, or intelligence activities of a law enforcement agency of the federal, state, or local government are excluded from the definition of "security breach." The section also defines with particularity "sensitive personally identifiable information" (SPII), and authorizes the Federal Trade Commission to amend this definition as needed through the rulemaking process.

Sec. 101 – Sets forth a customer notification requirements for certain business entities. Following the discovery of a security breach, such entities must notify any individual whose SPII has been, or is reasonably believed to have been, accessed or acquired, unless there is no reasonable risk of harm. Business entities covered by this section are those that use, access, transmit, store, dispose of, or collect SPII about more than 10,000 individuals during any 12-month period. Business entities are required to notify owners and licensees of SPII in the event of a security breach, and owners and licensees in such situations are charged with the responsibility of making required notifications.

Notification must be made without unreasonable delay. A reasonable delay is one of 60 days or less, unless the business entity seeking additional time demonstrates to the Federal Trade Commission that such time is reasonably necessary under a multi-factor standard; in such instances, the Commission may extend the period of reasonable delay in 30-day increments.

If a Federal law enforcement agency determines that the notification required would impede a criminal investigation or national security activity, notification shall be delayed upon written notice from such Federal law enforcement agency to the business entity that experienced the

breach. A business entity shall give notice 30 days after the day such delay was invoked unless a Federal law enforcement agency provides written notification that further delay is necessary.

Sec. 102 – Sets forth exemptions from notice to individuals. If the United States Secret Service or Federal Bureau of Investigation determines that notification could be expected to reveal sensitive sources and methods or similarly impede the ability of the agency to conduct law enforcement investigations, such notification is not required. Similarly, if the FBI determines that notification of the security breach could be expected to cause damage to the national security, such notification is not required.

Section 102 also establishes a "safe harbor" exemption in which a business entity is exempt from notice to individuals if a risk assessment conducted by or on behalf of the business entity concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose SPII was subject to the security breach. It also establishes a presumption that no reasonable risk exists where data that was rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted by experts in the field of information security. In order to invoke this "safe harbor", a business entity must notify the Federal Trade Commission within 45 days of the results of the risk assessment and its invocation of the "safe harbor". The section establishes requirements for risk assessments that may be used to invoke the "safe harbor".

For security breaches involving a limited subset of SPII, another exemption discharges a business entity from the notice requirement. A business entity need not notify if it utilizes or participates in a security program that effectively blocks the use of the SPII to initiate unauthorized financial transactions before they are charged to the account of the individual and it provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

Sec. 103 – Sets forth requirements for notice of individuals, permitting notification by mail, telephone, or email (if the individual has consented to receipt by email). It requires media notice in addition to personal notice where the number of affected individuals in any one state exceeds 5,000.

Sec. 104 – Sets forth requirements for the content of notifications, which includes a description of the SPII at risk, several contact toll-free telephone numbers (including one to assist with consumer inquiries concerning the security breach), and the name of the business entity that has a direct business relationship with the individual.

Sec. 105 – Requires that in breaches involving the SPII of more than 5,000 individuals, a business entity must notify all consumer reporting agencies of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the

distribution of notices to the affected individuals. Reasonable delay shall not exceed 60 days, unless the business entity seeking additional time demonstrates to the Federal Trade Commission that such time is reasonably necessary under a multi-factor standard; in such instances, the Commission may extend the period of reasonable delay in 30-day increments.

Sec. 106 – Requires business entities to notify the a DHS entity identified by the Secretary of Homeland Security if the security breach involves (1) the SPII of more than 5,000 individuals; (2) a database or other data system containing SPII of more than 500,000 individuals nationwide; (3) databases owned by the Federal Government; or (4) primarily the SPII of individuals known to be employees and contractors of the Federal Government involved in national security or law enforcement. The DHS entity that receives the reports shall then promptly notify and provide that same information to the United States Secret Service, the Federal Bureau of Investigation, and the Federal Trade Commission for civil law enforcement purposes, and shall make it available as appropriate to other federal agencies for law enforcement, national security, or computer security purposes.

This section also requires the Federal Trade Commission to promulgate regulations defining what these specified information notifications must contain. The Commission may also adjust as necessary the thresholds for notice to law enforcement, after consultation with the Attorney General.

The notice required under this section shall be provided as promptly as possible, but must occur 72 hours before notification of an individual or 10 days after discovery of the events requiring notice, whichever comes first.

Sec. 107 – Compliance with the requirements of this shall be enforced under the Federal Trade Commission Act by the Federal Trade Commission with respect to business entities subject to this Title. A violation of any requirement or prohibition imposed under this Title will constitute an unfair or deceptive act or practice in commerce and shall be subject to enforcement by the Commission, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act. In enforcing compliance with the requirements imposed by the Title, the Commission can use all its functions and powers. Such investigations shall not be initiated without prior consultation with the Attorney General, and the Commission may issue such other regulations as it determines to be necessary to carry out this Title.

Sec. 108 – Permits enforcement by State attorneys general (or their local designees) when they have reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this Title. The State attorney general (or local designee) may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to enjoin that

practice, enforce compliance with this Title, or seek civil penalties of not more than $1,000 per day per individual whose sensitive SPII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation unless such conduct is found to be willful or intentional.

Before filing an action, written notice must be provided to the Attorney General and the Federal Trade Commission. The Commission may move to stay the action, intervene in the action, initiate its own action, and file petitions for appeal. Institution of an action by the Commission precludes the filing of subsequent parallel actions by State attorneys general. Federal venue for any action by a State attorney general (or local designee) is controlled by the general civil venue statute. Process may be served in such an action wherever the defendant is an inhabitant or is found.

Finally, section 108 makes clear that nothing in this Title establishes a private cause of action against a business entity for violation of any of its provisions.

Sec. 109 – States that the provisions of this Title shall supersede any state or local law relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data, except to the extent that a State requires that notice to an individual shall also include information regarding victim protection assistance provided for by that State.

Sec. 110 – Requires the United States Secret Service, Federal Bureau of Investigation, and Federal Trade Commission to report to Congress not later than 18 months after the date of enactment of this Title on matters related to the Title's implementation within their area of expertise or control.

Sec. 111 – Excepts business entities from coverage under the Title to the extent that they act (1) as covered entities and business associates, or (2) as vendors of personal health records and third party service providers, that are subject to the Health Information Technology for Economic and Clinical Health Act, including the data breach notification requirements and implementing regulations of that Act.

Sec. 112 – The effective date of the Title is 90 days after the date of enactment.

Section–by-Section Analysis

DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AUTHORITY AND INFORMATION SHARING

Sec. 1. Department of Homeland Security Cybersecurity Authority

Section 1(a) amends Title II of the Homeland Security Act of 2002 (HSA) (6 United States Code 121 et seq.) by updating the assignment of the infrastructure protection responsibilities under the HSA from the Assistant Secretary for Infrastructure Protection to the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department. The reassignment reflects the creation of the Under Secretary position in prior amendments to the HSA and is consistent with current Department structure and organization.

Section 1(b) adds a new Subtitle E in Title II of the Homeland Security Act which includes the following:

Subtitle E – Cybersecurity Programs

Sec. 241. Short Title.

This section provides the short title of this Act as the "Department of Homeland Security Cybersecurity Authority and Information Sharing Act."

Sec. 242. Definitions.

This section defines the following terms for the purposes of the subtitle: agency, communication, countermeasure, critical infrastructure, critical information infrastructure, cybersecurity services, cybersecurity threat, electronic communication, electronic communication service, federal systems, incident, information security, information system, governmental entity, national security system, private entity, protect, and wire communication.

Sec. 243. Enhancement of National Cybersecurity and Cyber Incident Response.

Section 243(a) directs the Secretary to engage in cybersecurity and other infrastructure protection activities under this title to support the functioning of federal systems and critical information infrastructure in the interests of national security, national economic security, and national public health and safety.

Section 243(b) directs the Secretary to carry out risk-informed approaches that: (1) improve the information security of federal systems and critical information infrastructure; (2) consider the economic competitiveness of United States industry; (3) promote the development and implementation of technical capabilities to operate in cyberspace in support of national goals; (4)

protect privacy and civil liberties; (5) promote greater research, innovation, training, education, outreach, public awareness, and investment in cybersecurity; and (6) foster the development of secondary markets and widespread adoption of cybersecurity technology by critical information infrastructure.

Section 243(c) authorizes the Secretary to conduct cybersecurity activities to protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against cybersecurity threats. Responsibilities of the Secretary include: (1) creating appropriate programs; (2) developing and conducting risk assessments of federal systems and critical information infrastructure, in consultation with the heads of other agencies and governmental and private entities that own and operate such systems and infrastructure; (3) fostering the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting federal systems and critical information infrastructure; (4) acquiring, integrating, and facilitating the adoption of new cybersecurity technologies and practices to keep pace with emerging cybersecurity threats and developments; (5) designating and maintaining a center to serve as a focal point within the federal government for cybersecurity. The cybersecurity center will:

(A) facilitate information sharing among and between agencies, State, local, tribal and territorial governments, the private sector, academia, and international partners; (B) work with appropriate federal and non-federal partners to prevent and respond to cybersecurity threats and incidents involving federal systems and critical information infrastructure; (C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation and warning information to appropriate federal and non-federal partners; (D) integrate information from federal government and non-federal network operation centers to provide situational awareness of the Nation's information security posture and foster information security collaboration among system owners and operators; (E) compile and analyze information about risks and incidents that threaten federal systems and critical information infrastructure; and (F) provide incident detection, analysis, mitigation, and response information;

(6) assisting in national efforts to mitigate communications and information technology supply chain vulnerabilities to enhance the security and the resiliency of federal systems and critical information infrastructure; (7) developing and leading a nationwide cybersecurity awareness and outreach effort; (8) establishing, in cooperation with the Director of the National Institute of Standards and Technology, benchmarks and guidelines for making the critical information infrastructure more secure; (9) developing a national cybersecurity incident response plan and supporting cyber incident response and restoration plans; (10) developing and conducting cybersecurity exercises and simulations; and (11) taking other necessary and appropriate lawful actions..

Section 243(d) directs the Secretary to (1) coordinate with the heads of relevant federal agencies; representatives of State, local, tribal, territorial, and foreign governments; the private sector,

including owners and operators of critical information infrastructure; academia; and international organizations in carrying out this section; (2) coordinate the activities undertaken by agencies to protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against risk of incidents involving such systems and infrastructure; and (3) ensure that activities authorized in this section are coordinated with other infrastructure protection and cybersecurity programs in DHS.

Section 243(e) ensures that the provision of certain assistance or information to one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

Section 243(f) is a savings clause for law enforcement and intelligence authorities.

Sec. 244. National Cybersecurity Protection Program.

Sec 244(a) directs the Secretary to carry out a program to protect federal systems from cybersecurity threats, which may include: (1) operation of consolidated intrusion detection, prevention, or other protective capabilities; (2) conducting risk assessments of federal systems; (3) remote or on-site technical assistance; (4) ensuring common situational awareness across federal systems; (5) pursuant to section 249, directing agencies that own or operate a federal system to take specified action with respect to the operation of such system for the purpose of protecting that system or mitigating a cybersecurity threat; (6) discharging the responsibilities for federal information security set forth in chapter 35 of title 44, United States Code (as amended); and (7) testing and evaluating information security improvements within the Department.

Sec 244(b) authorizes the Secretary, notwithstanding any other provision of law, under specified conditions and when necessary in furtherance of the program authorized in subsection (a), to acquire, intercept, use, and disclose incoming, outgoing, and stored communications and other federal system traffic and deploy countermeasures on such communications and traffic to protect federal systems from cybersecurity threats. Retention and disclosure of intercepted information will be limited, and users of federal systems must be notified of the authorized activities. The program must be implemented pursuant to policies and procedures issued by the Secretary and approved by the Attorney General. The Secretary must certify that activities carried out under this subsection are compliant with all requirements in this subsection.

Sec 244(c) authorizes agencies, notwithstanding any other provision of law to permit the Secretary to acquire, intercept, retain, use, and disclose communications, system traffic, records, or other information transiting to or from or stored on a federal system to the Secretary for the purpose of protecting against or mitigating cybersecurity threats to federal systems in connection with the program authorized in subsection (a) and activity under subsection (b).

Sec 244(d) limits the authorization under subsection (b) to one year periods and requires the Secretary to renew any certifications made under subsection (b) annually.

Sec 244(e) authorizes the Secretary to request and obtain the assistance of private entities that provide electronic communications or cybersecurity services in order to implement this program.

Sec 244(f) prohibits the acquisition, interception, use, or disclosure of communications and other system traffic by DHS not authorized in subsection (b) or otherwise in accordance with law.

Sec 244(g) directs the Secretary to coordinate with heads of appropriate agencies and consult with heads of all agencies responsible for federal systems to accomplish the purposes of this section.

Sec. 245. Voluntary Disclosure of Cybersecurity Information

Sec 245(a) authorizes state, local, and tribal governments and private entities that lawfully intercept, acquire, or otherwise obtain or possess any communication, record, or other information, notwithstanding any other provision of law and under specified conditions, to disclose that information to the DHS cybersecurity center designated by the Secretary under section 243(c)(5) for the purpose of protecting an information system from cybersecurity threats or mitigating such threats.

Under this subsection, federal agencies that lawfully obtain information are authorized, notwithstanding any other provision of law and under specified conditions, to share that information with individuals with cybersecurity responsibilities within that agency, the DHS cybersecurity center designated under section 243(c)(5), or a private entity that is acting as a service provider to the agency. Disclosures made under this subsection must be for the purpose of protecting an information system from cybersecurity threats or mitigating such threats.

Sec 245(b) permits DHS to further disclose information obtained under this section to appropriate governmental and private entities in order to protect information systems against cybersecurity threats, mitigate cybersecurity threats, or with the approval of the Attorney General, to law enforcement entities when the information is evidence of a crime. Disclosure under this subsection shall be conducted in a manner consistent with policies and procedures under section 248. In addition, agencies receiving information under this section shall only use or retain it for the same purposes and consistent with policies and procedures under section 248.

Sec 245(c) requires that agencies ensure that when disclosing communications, records or other information to non-federal governmental or private entities, these entities only use or retain such communications, records or other information consistent with policies and procedures under section 248(a) and only for the purpose of protecting information systems from cybersecurity threats, mitigating cybersecurity threats, or for law enforcement purposes when the information

is evidence of a crime which has been, is being, or is about to be committed. The Attorney General must approve any disclosures for law enforcement purposes prior to disclosure.

Sec 245(d) affirms that nothing in this section limits or prohibits otherwise lawful disclosures by a private entity to the Department or any other governmental or private entity not conducted under this section.

Sec 245(e) affirms that nothing in this section permits the unauthorized disclosure of classified information, information related to intelligence sources and methods, or information that is specifically subject to a court order or a certification, directive or other authorization by the Attorney General precluding such disclosure.

Sec 245(f) exempts information disclosed to the Department pursuant to subsection (a) from disclosure under section 552(b)(3) of title 5, United States Code or comparable state law.

Sec 245(g) prohibits any use or disclosures of information not authorized under this section.

Sec. 246. Limitation on Liability and Good Faith Defense for Cybersecurity Activities.

Sec 246(a) prohibits a civil or criminal cause of action in a federal or state court against any non-federal governmental or private entity for (1) a disclosure of any communication, record, or other information authorized by this subtitle; and (2) any assistance provided to the Department in accordance with the requirements of section 244(e).

Sec 246(b) establishes that a good faith determination that this subtitle permitted conduct that forms the basis of any civil or criminal action shall be a complete defense to such causes of action.

Sec. 247. Federal Preemption, Exclusivity, and Law Enforcement Activities

Sec 247(a) states that this subtitle supersedes any State or local law that regulates the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities or governmental entities to the extent such statute is inconsistent with this subtitle.

Sec 247(b) states that Section 244 shall constitute an additional exclusive means for the domestic interception of wire or electronic communications, in accordance with section 1812(b) of title 50, United States Code.

Sec 247(c) affirms that this subtitle does not authorize the Secretary to engage in law enforcement or intelligence activities that the Department is not otherwise authorized to conduct under existing law.

Sec. 248. Privacy and Civil Liberties, Oversight, Penalties For Misuse.

Sec 248(a) directs the Secretary to develop and periodically review, with the approval of the Attorney General and in consultation with privacy and civil liberties experts, policies and procedures governing the acquisition, interception, retention, use, and disclosure of information obtained by DHS in connection with activities authorized in this subtitle. The policies and procedures shall minimize the impact on privacy and civil liberties; reasonably limit the acquisition, interception, retention, use and disclosure of information related to specific persons consistent with the need to carry out the responsibilities of this subtitle; include requirements to safeguard information that can be used to identify specific persons from unauthorized access or acquisition; and protect the confidentiality of disclosed information to the greatest extent practicable and informs recipients that the information may only be used for specified purposes.

Sec 248(b) directs the agencies to develop and periodically review with the approval of the Attorney General and in consultation with privacy and civil liberties experts, policies and procedures governing the acquisition, interception, retention, use, and disclosure of information obtained or disclosed by the agency in connection with activities authorized in this subtitle. The policies and procedures must be consistent with the requirements in 248(a).

Sec 248(c) directs the agencies to establish a program to monitor and oversee compliance with the policies and procedures issued under subsection (a) or (b) as well as promptly notify the Attorney General of significant violations of such policies and procedures.

Sec 248(d) directs the agencies to provide to Congress the policies and procedures established in subsection (a) or (b).

Sec 248(e) requires the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Department, in consultation with the most senior privacy and civil liberties officer or officers of appropriate agencies to submit a joint, annual report to the Congress assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this subtitle.

Sec 248(f) requires the Privacy and Civil Liberties Oversight Board to submit a report to Congress and the President two years after enactment providing its assessment of the privacy and civil liberties impact of the government's activities under this subtitle and recommending improvements to or modifications of the law to address privacy and civil liberties concerns.

Sec 248(g) affirms that no communications, records, system traffic or other information acquired or collected pursuant to this subtitle may be used, retained or disclosed by governmental or private entities except as authorized under this subtitle.

Sec 248(h) affirms that no otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subtitle shall lose its privileged character.

Sec 248(i) requires the agencies to develop and enforce appropriate sanctions for officers, employees or agents of the agency who conduct activities under this subtitle without authorization.

Sec 248(j) directs that any person who knowingly and willfully violates restrictions under this subtitle with respect to acquisition, interception, use, retention or disclosure of communications, records, system traffic or other information, or the related procedures established pursuant to section 248 shall be guilty of a misdemeanor and fined not more than $5,000 per incident.

Sec. 249. Required Security Action.

Sec 249(a) authorizes the Secretary to direct federal agencies to take any lawful action with respect to the operation of its federal system for the purpose of protecting that system or mitigating a cybersecurity threat. The Secretary shall establish, in coordination with the Director of the Office of Management and Budget (OMB), procedures governing the circumstances under which such directive may be issued under this section, including thresholds and other criteria; privacy and civil liberties protections; and notice to potentially affected third parties as may be applicable.

In order to take action under this section, the Secretary must specify the reasons for the required action and the duration of the directive; minimize the impact of directives under this section; and notify the Director of OMB and head of any affected agency.

Sec 249(b) authorizes the Secretary to use protective capabilities under the Secretary's control on federal systems without prior consultation with that agency for the purpose of ensuring the security of that system if the Secretary determines there is an imminent threat to federal systems and a directive under subsection (a) is not likely to result in a timely response to the threat. The authorities under this subsection may not be delegated below the level of Assistant Secretary. The Director of OMB, head of the affected agencies, and associated Chief Information Officers, must be immediately notified of any action taken under this subsection.

Section–by-Section Analysis

CYBERSECURITY REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE ACT

Sec. 1. Short Title.

This section provides the short title of this Title as the "Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act."

Sec. 2. Purposes.

Section 2 outlines the purposes of this Title. Generally, the purpose of this Title is to enhance the cybersecurity of infrastructures determined by the Secretary to be critical to national security, national economic security, and national public health and safety. Provisions of this Title provide for consultation on cybersecurity matters among all interested stakeholders, including sector-specific agencies with responsibility for critical infrastructure, agencies with responsibilities for regulating critical infrastructure, agencies with expertise regarding services provided by critical infrastructure, and the private sector. With significant involvement from the private sector, this Title facilitates the consultation in, and development of, best cybersecurity practices, while harmonizing the designation of entities as covered critical infrastructure with already existing infrastructure protection activities authorized by law. While the overall goal is to enhance the cyber security of critical infrastructures and protect security and vulnerability-related information, this Title also preserves principles of open government and supports the free flow of information. Moreover, this Title maintains a cyber environment that encourages efficiency and cost-effectiveness, innovation, and economic prosperity while also promoting safety, security, civil liberties, and privacy rights.

Sec. 3. Designation of Covered Critical Infrastructure.

Section 3(a) (Authority) authorizes the Secretary of Homeland Security (herein referred to as "the Secretary") to establish a process, through rulemaking, for designating entities as covered critical infrastructure.

Section 3(b) (Requirements) outlines the parameters for designating an entity as covered critical infrastructure. An entity may not be designated as covered critical infrastructure unless: (1) the incapacity or disruption of the reliable operation of the entity would have a debilitating effect on national security, national economic security, national public health or safety; and (2) the entity is dependent upon information infrastructure to operate. Thus, only the most critical entities would be regulated under this Title. In addition, the Secretary must consider a number of factors in order to evaluate cybersecurity risks and consequences by sector, including: interdependencies among components of covered critical infrastructure; the relative size of the entity; and the

potential for destruction or disruption of the entity to cause severe, negative consequences to the nation.

Section 3(c) (Establishment of Risk-based Tiers) requires the Secretary to establish risk-based tiers within the designation process for covered critical infrastructure. Risk-based tiering recognizes that some systems, assets, or operations, for example, are more critical than others and thus need to be protected at a higher level. Subsection (c) requires the Secretary to assign entities into the appropriate risk-based tier based on the severity of the threat of a cyber attack, the entity's vulnerabilities to a cyber attack, the extent of consequences of a cyber attack, and such other factors as the Secretary determines to be appropriate.

Section 3(d) (Lists of Covered Critical Infrastructure) requires the Secretary to establish lists of covered critical infrastructure, which shall be periodically reviewed and updated. Inclusion on a list would be subject to judicial review under the Administrative Procedures Act (APA).

Sec. 4. Risk Mitigation for Covered Critical Infrastructure.

Section 4(a) (Cybersecurity Risks) requires the Secretary, through rulemaking, to establish a process for identifying specific cybersecurity risks that must be mitigated to ensure the security of covered critical infrastructure. The Secretary must review and designate frameworks to address such identified risks, and update such risks on a regular basis. The cybersecurity risks must account for the criticality of specific systems.

Section 4(b) (Frameworks for Addressing Cybersecurity Risks) requires the Secretary to work with a wide range of interested parties (including, for example, representatives of organizations that coordinate the development of voluntary consensus standards, State and local governments, agencies, and the private sector) to propose standardized frameworks to address cybersecurity risks.

The Secretary must, in consultation with appropriate private sector representatives, consider the extent to which such proposed frameworks enhance security in practice, including criteria such as whether they reasonably address the cybersecurity risks, are cost effective, emphasize outcome-based metrics for measuring the effectiveness of mitigating identified cybersecurity risks, and include practical evaluation focusing on performance.

The Secretary, in consultation with the appropriate agencies, must review the proposed standardized frameworks, and designate and periodically update the designation of one or more frameworks selected.

If the Secretary determines that no proposed standardized framework meets the required criteria, the Secretary must adopt a framework that meets such criteria. As part of this process, the Secretary must invite the Director of NIST to provide advice and guidance on possible alternative frameworks. The frameworks adopted cannot require the use of a particular measure

to mitigate the risk.

Sec. 5. Cybersecurity Plans.

Section 5 requires owners or operators of covered critical infrastructure to develop cybersecurity plans that identify the measures selected by the covered critical infrastructure to address the identified cybersecurity risks. Company officers would certify that plans are being implemented, and DHS, or an agency with responsibility for regulating the entity, would have the option to review the cybersecurity plans.

Sec. 6. Evaluations.

Section 6(a) (In General) requires the Secretary, through rulemaking, to establish a process for evaluating the covered critical infrastructure's mitigation of identified risks to include: the selection of accreditors responsible for certifying evaluators to perform evaluations of covered critical infrastructure; the accreditation process for evaluators; the roles and responsibilities of evaluators in measuring the effectiveness of covered critical infrastructure in managing and mitigating cybersecurity risks; and generally-accepted evaluation practices.

Section 6(b) (Accreditation and Evaluation Process) requires the Secretary to enter into an agreement with a selected accreditor(s) with expertise in managing or implementing accreditation and evaluation programs for consensus standards. The selected accreditor(s) will conduct activities to carry out accreditations and oversee the evaluation process of covered critical infrastructure. The Secretary and the selected accreditor(s) may monitor and inspect the operations of any evaluator to ensure that the evaluator is complying with the procedures and requirements established through the rulemaking process. The Secretary and the selected accreditor(s) may revoke the accreditation of any evaluator that does not meet or comply with the established procedures and requirements, and may review any evaluation conducted by the evaluator.

Section 6(c) (Evaluations) requires covered critical infrastructure to be regularly evaluated by evaluators. The evaluations must produce outcome-based metrics that measure the effectiveness of the measures selected by the covered critical infrastructure to mitigate the identified cybersecurity risks. The evaluations must be conducted on at least an annual basis.

Sec. 7. Disclosure.

Section 7(a) (Annual Certifications) authorizes the Secretary, through rulemaking, to require company leaders to certify annually (in SEC filings or directly to the Secretary) that the cybersecurity plan required by section 5 has been developed and is being implemented, the evaluation of the company's efforts in mitigating identified cybersecurity risks required by

section 6 has been completed according to schedule, and whether the evaluation has concluded that the covered critical infrastructure is effectively mitigating identified cybersecurity risks.

Section 7(b) (Public Disclosure of Cybersecurity Plans and Certifications) requires the Secretary, through rulemaking, to require owners or operators of covered critical infrastructure to publicly disclose high-level summaries of the cybersecurity plans and evaluations. Such disclosures cannot include proprietary information or other information indicating a weakness of the covered critical infrastructure.

Section 7(c) (Notification of Cybersecurity Incidents) authorizes the Secretary, through rulemaking, to require owners or operators of covered critical infrastructure to promptly report to the Secretary any significant cybersecurity incident. Subsection (c) also requires the Secretary to develop, with the approval of the Attorney General, internal reporting and dissemination procedures to notify appropriate agencies of any significant cybersecurity incidents. These internal procedures will ensure that the appropriate agency is notified of the incident and can promptly initiate an investigation into the incident.

Section 7(d) (Protection from Public Disclosure) authorizes protection from public disclosure. For example, security and vulnerability-related information developed or collected under this Title and provided to the Federal government – including aggregated data and analysis – is exempted from disclosure under the Freedom of Information Act. Subsection (d) also authorizes a rulemaking process to prohibit the public disclosure of security and vulnerability-related information developed or collected under this Title, with exceptions provided for the sharing of information as appropriate to mitigate cybersecurity threats or further the official functions of a government agency, and with a committee of Congress authorized to have the information. Subsection (e) recognizes the continued protection from unauthorized disclosure for classified information. The purpose of these provisions is to prevent the unauthorized disclosure of cybersecurity vulnerability and security information that would be used by those seeking to exploit such vulnerabilities.

Sec. 8. Enforcement.

Section 8(a) (In General) requires the Secretary, through rulemaking, to determine if the covered critical infrastructure is sufficiently addressing the identified cybersecurity risks by reviewing the cybersecurity plan developed under Section 5 and the evaluation conducted under Section 6 and by conducting periodic quality control reviews. If the Secretary determines, after conducting such a review, that covered critical infrastructure is <u>not</u> sufficiently addressing identified risks, the Secretary may enter into discussions, or request another agency with sector-specific expertise to enter into discussions, with the owner or operator on ways to improve the cybersecurity plan or evaluation, after having such discussions, issue a public statement that the covered critical infrastructure is not sufficiently addressing the risks, and take such other action as may be appropriate. Subsection (a), however, prevents the Secretary from issuing a shutdown order,

requiring the use of a particular measure to address the cybersecurity risk, or imposing fines, civil penalties or monetary liabilities. The Secretary must establish an administrative review process for covered critical infrastructure to appeal the Secretary's finding that covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks.

Section 8(b) (Special Provisions for Federal Contracts) requires the Secretary to work with the Federal Acquisition Council to amend the FAR, as necessary, in conjunction with the implementation of provisions under this Title. The purpose of this provision is to ensure that cyber security is considered in Federal contracting.

Section 8(c) (Judicial Review) establishes what is a final agency action for purposes of judicial review under the APA.

Sec. 9. Rulemaking.

Section 9(a) (In General) requires the Secretary to issue regulations under APA notice-and-comment rulemaking to carry out the provisions of this Title.

Section 9(b) (Consultation) requires that the regulations include coordination with sector-specific agencies with responsibility for critical infrastructure, agencies with responsibility for regulating critical infrastructure, and agencies with expertise regarding services provided by critical infrastructure. In addition, the regulations must include consultation with the private sector and appropriate State and local government representatives.

Section 9(c) (Exemptions) authorizes the Secretary, in coordination with OMB, to exempt covered critical infrastructure from the requirements of this Title if the Secretary determines that a sector-specific regulatory agency has sufficient specific requirements in place to effectively mitigate identified cybersecurity risks.

Sec. 10. Definitions.

This Title defines the following terms: "Agency," "Cybersecurity Threat," "Critical Infrastructure," "Incident," "Secretary," and "Sector-Specific Agency".

Section-by-Section Analysis

AMENDMENTS TO THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

Sec. 1. Coordination of Federal Information Security Policy.

Sec 1(a) amends Chapter 35 of title 44, U.S.C., (the Federal Information Security Management Act of 2002) striking subchapters II and III and inserting the following new subchapter:

SUBCHAPTER II—INFORMATION SECURITY

Sec. 3551. Purposes.

The purpose of this subchapter is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations. The subchapter recognizes the highly networked nature of the current federal computing environment and endeavors to provide effective government-wide management of policies, directives, standards and guidelines, as well as effective and nimble oversight of and response to information security risks. Additionally, the subchapter provides for the development and maintenance of controls required to protect agency information and information systems and establishes a mechanism for improved security of federal agency information security programs and systems through a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than over prescriptive manual reporting. This subchapter attempts to maintain many of the goals and policies established in the Federal Information Security Management Act of 2002 (FISMA) while refining provisions that proved slow or cumbersome in implementation.

Sec. 3552. Definitions.

This section defines the following terms for the purposes of this subchapter: agency, information system, adequate security, incident, information security, information technology, national security system, and Secretary.

Sec. 3553. Federal Information Security Authority and Coordination.

Section 3553**(**a) authorizes the Secretary of Homeland Security (herein referred to as "the Secretary"), to exercise primary responsibility within the executive branch for information security. This includes implementation of information security policies and directives and compliance with the requirements of this subchapter, except as provided in subsections (d) and (e). This authority is consistent with recent FISMA practice and OMB guidance.

Section 3553(b) directs the Secretary to: (1) issue, compulsory and binding policies and directives governing agency information security operations and require implementation of information security policies and directives; (2) review agency information security programs

required under section 3554(b) annually; and (3) designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems. [Binding policies and directives shall include: (1) policies and directives consistent with the standards promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems; (2) minimum operational requirements for federal government network operations centers and security operations centers to protect agency information systems and provide common situational awareness across all agency information systems; (3) reporting requirements regarding information security incidents; (4) requirements for agency-wide information security programs; (5) performance requirements and metrics for the security of agency information systems; (6) training and minimum security clearance requirements to ensure that agencies are able to fully and timely comply with direction issued by the Secretary under this subchapter; (7) training requirements regarding privacy, civil rights and civil liberties, and information oversight for agency information security personnel; and (8) requirements for the annual reports to the Secretary under section 3554(c).

Section 3553(c) directs the Secretary to consider any applicable guidelines created under the National Institute of Standards and Technology Act, 15 U.S.C. 278g–3 and to consult with the Director of the National Institute of Standards and Technology (NIST) when policies and directives implement standards or guidelines developed by NIST under 40 U.S.C. § 11331.

Section 3553(d) exempts national security systems from the authorities of the Secretary under this section.

Section 3553(e) exempts the Department of Defense (DoD) from the responsibilities of the Secretary under paragraphs (1) and (2) of subsection (b) and subsection (c). The DoD Secretary will carry out these authorities and responsibilities for DoD.

Section 3553(f) states that nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any Head of a federal agency over such agency.

Sec. 3554. Agency Responsibilities.

Section 3554(a) directs the head of each agency to provide information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems belonging to such agency. Each agency head will maintain the responsibility for ensuring its agency complies with the requirements of this subchapter, including: reporting and sharing appropriate incident, threat, and vulnerability information with the DHS cybersecurity center designated under 3553(b)(3) and other appropriate entities; ensuring that senior agency officials provide security for information and information systems under their control; assessing and maintaining the resiliency of information technology systems critical to agency mission and operations; designating the

Inspector General or another independent evaluator to conduct the annual independent evaluation required under section 3556; delegating to a senior agency official the authority and responsibility to implement an agency-wide information security program; delegating to appropriate agency officials who are responsible for particular agency systems or subsystems the responsibility to ensure and enforce compliance with all requirements of the agency's information security program in coordination with the senior agency official in charge of the agency-wide program; ensuring that the agency has trained and cleared personnel sufficient to assist the agency in complying with the requirements of this subchapter; ensuring that the designated senior agency official, in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions; and ensuring that the designated senior agency official possesses the necessary qualifications to administer the functions described in this subchapter.

The responsibilities of the senior agency official designated to implement the agency-wide information security program shall include: overseeing the establishment and maintenance of an enterprise security operations and continuous monitoring capability; developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under sections 3552 and 3553 and section 11331 of title 40; training and overseeing agency personnel with significant responsibilities for information security; and assisting senior agency officials concerning their respective information security responsibilities.

Section 3554 (b) states that the agency-wide information security programs described in subsection (a) shall include: (1) the development and maintenance of a risk management strategy for information security; (2) security testing commensurate with risk and impact; (3) mitigation of information security vulnerabilities commensurate with risk and impact; (4) risk-based, cost-effective policies and procedures that ensure adequate security throughout the lifecycle of each agency information system and are compliant with the requirements of this subchapter; (5) information security, privacy, civil rights, civil liberties, and information oversight training to inform information security personnel with access to agency information systems; (6) continuous monitoring of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices; (7) a process for ensuring that remedial actions have been taken to address any deficiencies in the information security policies, procedures, and practices of the agency; (8) operation of appropriate technical capabilities to detect, mitigate, report, and respond to information security incidents, consistent with policies and directives issued under section 3553(b); and (9) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Section 3554(c) requires each agency to submit an annual report on their information security program and information systems to the Secretary.

Sec. 3555. Periodic assessments

Section 3555(a) directs the Secretary to prepare periodic summaries of agency security programs and practices. Such summaries shall assess the effectiveness of agency information security policies, procedures, and practices; provide an overall assessment of federal government-wide agency information system security posture; and include recommendations for improving agency specific and federal government-wide agency information system security. Section 3555(b) directs that periodic summaries relating to national security systems will be prepared as specified by the President and periodic summaries related to agency information systems under the control of the Department of Defense shall be prepared by the Secretary of Defense.

Section 3555(c) directs assessors to take appropriate actions to ensure the protection of information which, if disclosed, may adversely affect information security.

Section 3555(d) directs the Secretary, in coordination with the Secretary of Defense, to evaluate and report to Congress annually on the adequacy and effectiveness of the information security summaries established under this section.

Sec. 3556. Independent Evaluations.

Section 3556(a) directs the Council of Inspectors General on Integrity and Efficiency, in consultation with the Director of Office of Management and Budget and Secretary, to issue and maintain criteria for cost-effective, risk-based, and independent evaluations for agency information security programs and practices in order to determine the effectiveness of such programs and practices. It directs that reports prepared under this section be provided to the Secretary upon delivery of the report to the agency head. It also directs that evaluations involving national security systems be conducted as directed by President.

Sec. 3557. Savings Provisions and Technical and Conforming Amendments.

Section 3557 contains savings provisions to maintain the effect of various OMB and Department of Commerce policies, standards, and compliance guidance.

Section 3557 (b) makes technical and conforming amendments to chapter 35 of title 44.

Sec. 2. Management of Information Technology.

Section 2(a) amends section 11331 of title 40, U.S.C., by revising the entire section as follows:

Sec. 11331. Responsibilities for Federal Information Systems Standards.

Section 11331(a) authorizes the Secretary of Commerce, in consultation with the Secretary of Homeland Security, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to federal information systems. However, standards and

guidelines for national security systems will be developed, prescribed, enforced, and overseen in a manner directed by the President.

Section 11331(b) directs the Secretary of Commerce to make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of federal information systems. Standards prescribed under subsection (a)(1) shall include standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

Section 11331(c) authorizes the President to disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may be delegated to the Director of Office of Management and Budget. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President or the Director of Office of Management and Budget.

Section 11331(d) directs the Secretary of Commerce to exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget to ensure fiscal and policy consistency.

Section 11331(e) authorizes the head of any executive agency to employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary of Commerce prescribes under this section.

Section 11331(f) directs the Secretary of Commerce to make any decision regarding the promulgation of any standard under this section not later than 6 months after the submission of the proposed standard to the Secretary of Commerce by NIST.

Section 11331(g) defines the following terms for the purpose of this section: federal information system, information security, and national security system.

Section 2(b) makes technical and conforming amendments to section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4).

Section-by-Section Analysis

PERSONNEL AUTHORITIES RELATED TO CYBERSECURITY POSITIONS

Part 1: This proposal would give the Secretary of Homeland Security hiring and compensation authorities commensurate with those of the Secretary of Defense. Specifically, this proposal would authorize the Secretary of Homeland Security to establish positions in the excepted service, such that the Secretary could make direct appointments (10 U.S.C. §1601), set rates of basic pay (10 U.S.C. §1602), and provide additional compensation, benefits, incentives, and allowances (10 U.S.C. §1603). The Secretary would also be authorized to establish a scholarship program for employees to pursue an associate, baccalaureate, or advanced degree, or a certification, in an information assurance discipline (10 U.S.C. §2200a).

Part 2: This proposal would expand existing authorities to allow for the reactivation of a USG-wide exchange framework for private sector talent to be assigned to a department or agency in substantive roles, and USG employees to be assigned to private sector companies. Through this program, Federal departments or agencies will be able to assign Federal information technology (IT) workers to positions within private sector companies or receive private sector IT workers for positions within the Federal Department or agency. Eligible workers must: (1) work in IT; (2) be a highly skilled and valued employee who would excel in the performance of the employee's duties and who would excel in the assignment; and (3) be expected to assume increased IT management responsibilities in the future. This proposal seeks to scale the Department of Defense's IT Exchange Program (ITEP) pilot for the USG writ large.

Section-by-Section Analysis

PREVENTING RESTRICTIONS ON DATA CENTER LOCATIONS

To promote efficiency and innovation, this proposal would bar, except where expressly authorized by federal law, U.S. States from passing a law or adopting a regulation that would require private sector data centers to be located in that state as a condition of doing business. Data centers that serve solely governmental purposes could be required to be within the state.