SECTION-BY-SECTION
Revised Cybersecurity Act of 2012
S. 3414 (introduced on July 19, 2012)

Section 1. Short Title. The short title of the bill is the "Cybersecurity Act of 2012" or the "CSA2012".

Section 2. Definitions. Section 2 defines terms including "commercial information technology product", "commercial item", "critical infrastructure", "critical cyber infrastructure", "critical infrastructure", " Critical Infrastructure Partnership Advisory Council", "Department", "Federal Agency", "Federal information infrastructure", "incident", "information infrastructure", "information sharing and analysis organization", "information system", "institution of higher education", "intelligence community", "member agency", "national information infrastructure", "national laboratory", "national security system", "owner", "operator", "secretary", "significant cyber incident", and "Council".

TITLE I. PUBLIC-PRIVATE PARTNERSHIP TO PROTECT CRITICAL INFRASTRUCTURE

Section 101. National Cybersecurity Council. Section 101 establishes the National Cybersecurity Council ("Council") charged with fulfilling the responsibilities in this title. The Council is comprised of representatives from the Departments of Commerce, Defense, Homeland Security, Justice; appropriate sector-specific Federal agencies, appropriate Federal agencies with responsibilities for regulating the security of covered critical infrastructure, and appropriate representatives of the intelligence community. The Council will be chaired by the Secretary of Homeland Security and will coordinate with owners and operators of critical infrastructure.

Section 102. Inventory of Critical Infrastructure. Section 102 requires the Council to designate a member agency to conduct sector-by-sector top-level risk assessments to determine which sectors face the greatest immediate risk, and beginning with the sectors identified as the highest priority, conduct, on a sector-by-sector basis, cyber risk assessments of critical infrastructure. The selected member agency must coordinate risk assessments with owners and operators of critical infrastructure and other private sector entities and is required to establish a process under which private entities may choose to voluntarily share information with the Council. Section 102 also requires the selected member agency, in consultation with owners and operators, the Critical Infrastructure Partnership Advisory Council, and representatives of State and local governments to identify categories of critical infrastructure as critical cyber infrastructure and to designate owners of such infrastructure, who must report significant cybersecurity incidents to the Council. This section directs the Council to identify categories of critical cyber infrastructure only if a cyber attack to that infrastructure could reasonably result in: (1) interruption of life-sustaining services sufficient to cause a mass casualty event or mass evacuations; (2) catastrophic economic damage to the United States; or (3) severe degradation of national security, and directs the Council to establish procedures for an identified owner to challenge that identification. The section prohibits the Council from identifying a category of critical cyber infrastructure based solely on activities protected by the first amendment to the Constitution, an

information technology product based solely on a finding that the product is capable of, or is actually being used in critical cyber infrastructure, or a commercial item that organizes or communicates information electronically.

Section 103. Voluntary Cybersecurity Practices. Section 103 requires sector coordinating councils, composed of relevant representatives of owners of critical infrastructure, to develop and propose voluntary outcome-based cybersecurity practices ("cybersecurity practices") sufficient to effectively remediate or mitigate cyber risks identified under the risk assessment process in section 102. Cybersecurity practices may be comprised of existing industry best practices, standards and guidelines, or other practices developed by the private sector coordinating council. Upon receipt of such cybersecurity practices, the Council, in consultation with owner and operators, the Critical Infrastructure Partnership Advisory Council, nongovernmental cybersecurity experts, and appropriate information sharing and analysis organizations, and in coordination with appropriate representatives from State and local governments, shall review and approve such cybersecurity practices, or any amendments to or additional cybersecurity practices necessary to ensure adequate remediation or mitigation of the cyber risks identified under section 102. A federal agency with responsibilities for regulating a critical infrastructure sector may adopt the practices as mandatory. The section requires that the cybersecurity practices remain technology neutral. Finally, each cybersecurity practice approved by the Council shall be subject to public review by relevant sector coordinating councils and the Critical Infrastructure Partnership Advisory Council.

Section 104. Voluntary Cybersecurity Program for Critical Infrastructure. Section 104 requires the Council to establish a voluntary cybersecurity program for critical cyber infrastructure and any other critical infrastructure approved by the Council. Owners of critical infrastructure may apply for certification in the program by self-certifying to the Council that the owner is satisfying the cybersecurity practices developed under section 103 or submitting to the Council a third-party assessment verifying that the owner is satisfying the cybersecurity practices. Owners that are certified under the program will be entitled to several benefits including: (1) liability protections from any punitive damages arising from an incident related to a cybersecurity risk where the owner is in substantial compliance with the cybersecurity practices at the time of the incident; (2) expedited provision of security clearances to appropriate personnel employed by the certified owner; (3) priority technical assistance on cyber issues; and (4) receipt of relevant real-time cyber threat information. The Council may publicly recognize certified owners, with the owner's consent. The Federal Acquisition Regulatory Council is also required by this section to work with the Council and the private sector to examine the potential benefits of establishing a procurement preference in the federal marketplace for certified entities.

Section 105. Rules of Construction. Section 105 provides that nothing in this title shall be construed to: (1) limit the ability of a Federal agency with responsibilities for regulating the security of critical infrastructure from requiring that the cybersecurity practices under this title be met; (2) provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with responsibilities for regulating the security of critical infrastructure to establish standards that are not otherwise authorized by law; or (3) permit any owner to fail to comply with any other law or regulation, unless specifically authorized.

Section 106. Protection of Information. Section 106 requires that covered information submitted in accordance with this section be treated as voluntarily shared critical infrastructure information under section 214 of the Homeland Security Act. Covered information in this section includes information submitted as part of the risk assessments under section 102, information submitted to assist in the designation of critical cyber infrastructure under section 102, information provided during an assessment under section 104, and information provided through the cybersecurity tip line established in this section. Section 106 also preserves existing whistleblower protections under the Homeland Security Act of 2002.

Section 107. Annual Assessment of Cybersecurity. Section 107 requires the Council to report to Congress on the effectiveness of this title in reducing the risk of cyber attack to critical infrastructure.

Section 108. International Cooperation. Section 108 requires the Secretary of Homeland Security, in coordination with the Secretary of State or the head of sector-specific agencies and others, to: (1) inform owners or operators of information infrastructure located outside of the United States, the disruption of which could result in catastrophic damage within the United States, of information related to cyber risks to such information infrastructure; and (2) coordinate with international governments and owners of such information infrastructure regarding mitigation or remediation of cyber risks.

Section 109. Effect on Other Laws. Section 109 provides that nothing in this Act shall be construed to preempt the applicability of State law or requirements, except as expressly provided in sections 104 and 106.

Section 110. Definitions. Section 110 defines terms including "certified owner", "cyber risk", "sector-coordinating council", and "sector-specific agency."

TITLE II. FEDERAL INFORMATION SECURITY MANAGEMENT AND CONSOLIDATING RESOURCES

Section 201. FISMA Reform. Title II amends the Federal Information Security Management Act of 2002 (FISMA) by striking subchapters II and III of chapter 35 of Title 44, United States Code (44 U.S.C. §§ 3541, et seq.), and inserting the following sections. Many of the original FISMA requirements are retained in this language. The section-by-section analysis below refers to the new sections of Title 44, as amended by this bill.

New Section 3551. Purposes. Section 3551 states the purposes of this subchapter are to provide comprehensive policy and oversight framework for federal agencies' information security, while emphasizing the need for continuous monitoring and streamlined reporting.

New Section 3552. Definitions. Section 3552 defines terms, including: "adequate security", "continuous monitoring", "incident", "information security", "information technology", and "national security system".

New Section 3553. Federal Information Security Authority and Coordination. Section 3553 clarifies and builds on DHS's role of overseeing FISMA to increase security and efficiency across the Federal government. It gives DHS statutory authority to match its current responsibilities given by the White House in 2010 to oversee civilian agency information security policy. It also requires red team exercises and operational testing, gives DHS the ability to streamline agency reporting requirements, and reduces paperwork exercises by moving to continuous monitoring and risk assessment. It gives DHS the authority to issue information security policy and also risk mitigation directives to agencies whose security is lacking. It clarifies the authority and necessary privacy protections for DHS to operate its government-wide intrusion detection and prevention system known as "EINSTEIN," and limits DHS's intrusion prevention role in the case of an imminent threat. Reflecting current law, it would maintain the authority of the Defense Department and Intelligence Community over their own systems, as well as the President's current authorities over national security systems. It requires DHS to coordinate with NIST and the DOD to ensure that its policies are complementary.

New Section 3554. Agency Responsibilities. Section 3554 lays out responsibilities of agency heads to provide adequate security for the information and systems under their control. It requires agency heads to update their information security programs to facilitate a culture of security, rather than a culture of compliance. The programs include continuous monitoring, red team exercises, effective risk management, and information sharing within the Federal space. The section also requires security, privacy, and civil liberties awareness training for agency personnel. Agency heads would report on the effectiveness of their security programs, along with a summary of incidents, and identify significant deficiencies and processes to remediate those deficiencies.

New Section 3555. Annual Assessments. Section 3555 codifies the annual assessments of agencies' security programs that DHS is currently conducting. These holistic reviews assist agencies in understanding their strengths and weaknesses.

New Section 3556. Independent Evaluations. Section 3556 makes the current inspector general reviews under FISMA more consistent and effective. The updates to this section assist the auditors in focusing on security rather than compliance, resulting in more consistent, risk-based, and cost-effective reviews.

New Section 3557. National Security Systems. Section 3557 maintains the language under current FISMA to ensure that agencies provide security for national security systems.

New Section 3560. Effect on Existing Law. This section clarifies that nothing within the title interferes with other existing laws.

Section 202. Management of Information Technology. Section 202 maintains NIST's current role under FISMA to develop binding information security standards for Federal agencies.

Section 203. Savings Provisions. Section 203 protects the current information security policies of OMB and NIST until they expire or are repealed.

Section 204. Consolidation of Existing Departmental Cyber Resources and Authorities. Section 301 amends Title II of the Homeland Security Act (HSA) of 2002 to add the sections described below.

New Section 241 of the HSA. Definitions. Section 241 defines terms including "agency information infrastructure", "covered critical infrastructure", "damage", "Federal cybersecurity center", "Federal information infrastructure", "incident", "information security", "information system", "national security and emergency preparedness communications infrastructure", "national information infrastructure", and "national security system".

New Section 242 of the HSA. Consolidation of Existing Resources. Section 242 consolidates several existing functions within DHS—the National Cyber Security Division, the Office of Emergency Communications, and the National Communications Systems—into a newly established National Center for Cybersecurity and Communications (NCCC or the Center). The Center would be headed by a Director appointed by the President and confirmed by the Senate. The Director would be responsible for managing Federal efforts to secure, protect, and ensure the resiliency of cyber networks in the United States. The Center would have two Deputy Directors, one of whom would be an employee of the Intelligence Community identified by the Director of National Intelligence, in concurrence with the Secretary of Homeland Security. This intelligence-focused deputy would ensure that the knowledge and expertise that resides in the Intelligence Community is integrated into the NCCC from the outset. The Center would also have staff detailed from the Departments of Defense, Justice, and Commerce, as well as the Intelligence Community. To ensure that privacy and civil liberties are taken into account in every aspect of the Center's policy and operations, it would also have a full-time Chief Privacy Officer.

New Section 243 of the HSA. DHS Information Sharing. Section 243 requires the Director of the NCCC to establish a program to facilitate cybersecurity information sharing of both classified and unclassified cybersecurity information with other Federal agencies, the private sector, state and local governments, and international partners. Information shared with the Federal government will receive special protections from further disclosure. Additionally, the Director of the NCCC, in consultation with the Attorney General, the DNI, and the NCCC's privacy officer must establish and implement guidelines to ensure the protection of privacy and civil liberties.

New Section 247 of the HSA. Prohibited Conduct. This section prohibits the Federal government from compelling the disclosure of information from a private entity relating to an incident unless otherwise authorized by law and from intercepting a wire, oral, or electronic communication relating to an incident unless otherwise authorized by law.

TITLE III. RESEARCH AND DEVELOPMENT

Section 301. Federal Cybersecurity Research and Development. Section 301 requires the Director of Science and Technology Policy, in coordination with the Secretary of Homeland Security and the head of any relevant Federal agency, to develop a national cybersecurity research and development plan. The section also requires the establishment of a program to

provide grants to institutions of higher education and development non-profit institutions to establish cybersecurity test beds capable of realistic modeling of cyber attacks to support development of new cybersecurity defenses; reauthorizes the Cybersecurity Faculty Development and Traineeship Program through 2014; and authorizes the development of standards and guidelines for enhanced cybersecurity as part of the Networking and Information Technology Research and Development Program.

Section 302. Homeland Security Cybersecurity Research and Development. Section 302 amends Subtitle D of title II of the Homeland Security Act of 2002 by adding the following section.

New Section 238 of HSA. Cybersecurity Research and Development. Section 238 requires DHS to carry out a research and development program to improve the security of the nation's information infrastructure.

Section 303. Research Centers for Cybersecurity. Section 303 requires the Director of the National Science Foundation to establish cybersecurity research centers based at institutions of higher learning or other entities.

Section 304. Centers of Excellence. Section 304 permits the Secretary, jointly with the Secretary of Defense, to establish Centers of Excellence in cybersecurity for the protection of critical infrastructure in conjunction with academic and professional partners from countries that may include allies of the United States.

TITLE IV. EDUCATION, OUTREACH, AND WORKFORCE

Section 401. Definitions. Section 401 defines the terms "cybersecurity mission" and "cybersecurity mission of a Federal agency."

Section 402. Education and Outreach. Section 402 requires the Director of the National Science Foundation report to Congress on the state of cybersecurity education in the United States and requires the Secretary of Homeland Security and the Director of the National Institute of Standards and Technology to develop and implement an outreach and awareness program on cybersecurity to increase understanding of the benefits of cybersecurity measures.

Section 403. National Cybersecurity Competition and Challenge. Section 403 requires the Secretary of Homeland Security and the Secretary of Commerce to establish a program to advance national and statewide competitions and challenges that seek to identify, develop, and recruit talented individuals to work in federal, state, and local governments, and the private sector on cybersecurity.

Section 404. Federal Cyber Scholarship-for-Service Program. Section 404 directs the Director of the National Science Foundation to establish a Federal Cyber Scholarship-for-Service program to recruit and train cybersecurity professionals to meet the needs of the Federal government's cybersecurity mission.

Section 405. Assessment of Cybersecurity Federal Workforce. Section 405 requires the Director of the Office of Personnel Management (OPM), in coordination with various Federal agencies and others, to assess the readiness and capacity of the Federal workforce to meet the needs of the Federal government's cybersecurity mission.

Section 406. Federal Cybersecurity Occupation Classifications. Section 406 requires the Director of OPM to develop and issue comprehensive occupation classifications for Federal employees engaged in the cybersecurity mission.

Section 407. Training and Education of Federal Employees. Section 407 requires the Director of OPM, in coordination with various Federal agencies, to establish a cybersecurity awareness and education curriculum program for all Federal employees and Federal contractors and a program to provide training to improve the technical skills and capabilities of Federal employees engaged in the cybersecurity mission.

Section 408. National Center for Cybersecurity and Communications Acquisition Authorities. Amends the Homeland Security Act to give the NCCC the same procurement flexibilities currently available to the Department of Defense, NASA, and the Coast Guard, which allow narrow exceptions to normal competitive procedures for procurements that may be satisfied by a limited number of responsible sources, or for follow-on contracts for the continued provision of highly specialized services. To ensure these exceptions are used only when necessary, this section subjects them to justification and approval procedures, and the authorities would terminate three years after the date of enactment of this Act. The Director must report on a semiannual basis to Congress on the use of the authority granted under this section.

Section 409. Reports on Cyber Incidents Against Government Networks. Section 410 requires DHS to report annually to Congress summarizing major cyber incidents against civilian government networks, discussing the risk of cyber sabotage against those networks, and providing aggregate statistics regarding breaches of executive networks. It also requires the Department of Defense to report annually to Congress the same information regarding military networks.

Section 410. Reports on Prosecution for Cybercrime. Section 411 directs the Attorney General and Director of the FBI to submit an annual report to Congress describing investigations and prosecutions relating to cybercrimes in the preceding year, and discussing any impediments under US or international law to such prosecutions.

Section 411. Report on Research Relating to Secure Domain. Section 412 requires the Secretary to contract with the National Research Council, or other federally funded research and development corporation, to submit to Congress annual reports on available constitutionally sound technical options for enhancing the security of information networks of entities that own or manage critical infrastructure.

Section 412. Report on Preparedness of Federal Courts to Promote Cybersecurity. Section 413 requires the Attorney General to submit to Congress a report on whether Federal courts are granting timely relief in matters relating to cybercrime, including recommendations on changes

to the Federal Rules of Civil Procedure and Criminal Procedure, training of the Federal judiciary, the specialization of courts, and federal law.

Section 413. Report on Impediments to Public Awareness. Section 414 requires the Secretary to submit an annual report to Congress on the legal or other impediments to public awareness of cybersecurity threats and mitigation methods, a summary of the Secretary's plans to enhance public awareness, and recommendations for congressional action to address these impediments.

Section 414. Report on Protecting the Electrical Grid of the United States. Section 415 requires the Secretary, in consultation with the Secretary of Defense and the Director of National Intelligence, to submit to Congress a report on the threat, implications, options available in the event of, and a plan to prevent disruption of the electric grid of the United States caused by a cyber attack.

Section 415. Evaluation and Reports on Marketplace Information. Section 415 requires the Securities and Exchange Commission (SEC) to evaluate existing guidance to companies related to requirements to disclose to investors "material risks" that pertain to information security, in order to provide quality information to the marketplace and enable informed investor decisions. In light of the evaluation, the SEC will determine whether the existing guidance should be updated or issued as formal Commission guidance. Section 415 also requires various reports on the implementation and effects of this guidance.

TITLE V. FEDERAL ACQUISTION RISK MANAGEMENT STRATEGY.

Section 501. Federal Acquisition Risk Management Strategy. Section 501 requires the Secretary of Homeland Security to coordinate with private sector experts, the Secretaries of Defense, Commerce and State, the Director of National Intelligence, and other Federal agencies, to develop an acquisition risk management strategy to ensure the security of Federal networks. The section specifies that this strategy must incorporate all-source intelligence analysis of the integrity of the supply chain for Federal networks, as well as private sector standards, guidelines and best practices.

Section 502. Amendments to Clinger-Cohen Provisions to Enhance Agency Planning for Information Security Needs. Section 502 amends the Clinger-Cohen Act, the Federal law that governs the Federal government's acquisition and management of information technology resources, to enhance agency planning for information security needs. Section 502 is intended to further the practical implementation of the strategy developed in Section 501 and to modernize the law's approach to cybersecurity by ensuring that agencies prioritize security in information technology purchases, keep mandatory security standards up to date, use security best practices, train acquisition officers in information security, root out bureaucratic impediments to purchasing secure technologies, and take new steps to eliminate purchases of counterfeit products.

TITLE VI – INTERNATIONAL COOPERATION

Section 601. Definitions. Section 601 defines the terms "computer systems," "computer data," "Convention on Cybercrime," "cybercrime," "cyber issues" and "relevant federal agencies."

Section 602. Findings. Section 602 contains several Congressional findings demonstrating the integral role coordinating and collaborating with international partners plays in protecting cyberspace.

Section 603. Sense of Congress. Section 603 expresses the sense of the Congress that international engagement to advance U.S. cyberspace objectives should be an integral part of U.S. foreign relations and diplomacy and that the Secretary of State should lead this U.S. effort.

Section 604. Coordination of International Cyber Issues Within the United States Government. Section 604 authorizes the Secretary of State to designate a senior level State Department official to coordinate U.S. diplomatic engagement on international cyber issues, provide strategic direction and coordination for U.S. policy on international cyber issues, and coordinate with relevant Federal agencies to develop interagency plans regarding international cybersecurity.

Sec. 605. Consideration of Cybercrime in Foreign Policy and Foreign Assistance Programs. Section 605 requires the Secretary of State to provide a comprehensive annual briefing and periodic updates to Congress on global issues, trends, and actors considered to be significant with respect to cybercrime, the means of enhancing multilateral or bilateral efforts to prevent, investigate, and prosecute cybercrime, and describe U.S. steps to promote the multilateral or bilateral efforts to reach the goals described above. The Secretary of State is also authorized to prioritize foreign assistance programs designed to combat cybercrime in a region or program of significance in order to better combat cybercrime.

TITLE VII. INFORMATION SHARING.

Section 701. Affirmative Authority to Monitor and Defend Against Cybersecurity Threats. Section 701 reduces legal barriers that deter and prevent a private entity from monitoring its own networks for malicious cyber activity and using defensive countermeasures on its networks to protect its rights or property from cybersecurity threats. In the course of these defensive activities, private entities must abide by important conditions and restrictions that safeguard privacy and limit such activities to defending against cybersecurity threats.

Section 702. Voluntary Disclosure of Cybersecurity Threat Indicators among Private Entities. Section 702 permits private entities to disclose and receive lawfully obtained cybersecurity threat information, provided they use the information only to protect an information system, make reasonable efforts to safeguard information that can be used to identify specific persons from unauthorized access or acquisition, and adhere to other conditions.

Section 703. Cybersecurity Exchanges. Section 703 establishes a process to designate "cybersecurity exchanges." The purpose of a cybersecurity exchange is to receive and distribute, in as close to real time as possible, cybersecurity threat indicators, and to thereby avoid

unnecessary and duplicative Federal bureaucracy for information sharing. Specifically, this section requires the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, to establish (1) a process for designating appropriate civilian Federal and non-Federal entities as cybersecurity exchanges, (2) procedures to facilitate and encourage the sharing of classified and unclassified cybersecurity threat indicators in as close to real time as possible, and (3) a process for identifying entities capable of receiving classified cybersecurity threat information. Section 703 also requires the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, to designate a lead Federal cybersecurity exchange to serve as the focal point within the Federal Government to facilitate and encourage information sharing with both Federal and non-Federal entities.

Section 704. Voluntary Disclosure of Cybersecurity Threat Indicators to a Cybersecurity Exchange. Section 704 authorizes a non-Federal entity to disclose lawfully obtained cybersecurity threat indicators to a cybersecurity exchange, and authorizes non-Federal entities to receive such information from a cybersecurity exchange, provided entities use the information only to protect an information system, make reasonable efforts to safeguard information that can be used to identify specific persons from unauthorized access or acquisition, and adhere to other conditions.

A cybersecurity exchange that receives information under this title may only use, retain, or further disclose the information to protect information systems from cybersecurity threats or mitigate cybersecurity threats, or to law enforcement under certain narrow circumstances. A cybersecurity exchange may only disclose information to a law enforcement entity if the disclosure is permitted under the procedures developed by the Secretary of Homeland Security and approved by the Attorney General Law, and the information appears to pertain to a cybersecurity crime which has been, is being, or is about to be committed, an imminent threat of death or serious bodily harm, or a serious threat to children. Law enforcement may only use such information for these purposes. Any Federal entity that receives information under this title must adhere to a robust privacy and civil liberties oversight regime. Finally, this section establishes a new cause of action against the Federal government if a Federal entity intentionally or willfully violates a provision of this title or a regulation promulgated under this title

Section 705. Sharing of Classified Cybersecurity Threat Indicators. Section 705 provides that procedures developed to facilitate and encourage information sharing must provide that classified cybersecurity threat information may only be shared with certified entities and appropriately cleared persons in a manner that protects national security. This section directs the Director of National Intelligence to issue guidelines providing that appropriate Federal officials may grant security clearances to certified entities and employees of certified entities.

Section 706. Limitation on Liability and Good Faith Defense for Cybersecurity Activities. Section 706 provides that no cause of action shall lie or be maintained based on the cybersecurity monitoring activities permitted under section 701 or for the voluntary disclosure of lawfully obtained cybersecurity threat information (1) to a cybersecurity exchange, (2) by a provider of cyber services to its customers, (3) to an owner or operator of critical infrastructure, or (4) to a non-Federal entity provided that the information is shared with a cybersecurity exchange within

a reasonable time. This section also provides that a reasonable, good faith reliance that this title permitted the conduct complained of is a complete defense against any cause of action brought, and other limitations on liability. Finally, the section provides that any person who, knowingly or acting in gross negligence, violates this title receives none of the limitations on liability afforded by this title and may be subject to any criminal or civil cause of action that may arise under any other State or Federal law prohibiting the conduct in question.

Section 707. Construction and Federal Preemption. Section 707 provides that nothing in the title may be construed to limit any other existing authority or lawful requirement to monitor information systems and information that is stored on, processed by, or transiting such information systems, operate countermeasures, and retain, use or disclose lawfully obtained information. It also provides that nothing in the title may be construed to provide additional authority to, or modify an existing authority of, the Department of Defense or the National Security Agency or any other element of the intelligence community; limit or modify an existing information sharing relationship; prohibit a new information sharing relationship; require a new information sharing relationship between a Federal entity and a private entity; limit the ability of a non-Federal entity or a Federal entity to receive data about its information systems, including lawfully obtained cybersecurity threat indicators; authorize or prohibit any law enforcement, homeland security, or intelligence activities not otherwise authorized or prohibited under another provision of law; permit price-fixing or market allocation between competitors; authorize or limit liability for actions that would violate the regulations adopted by the Federal Communications Commission on preserving the open Internet, or any successor regulations thereto, nor to modify or alter the obligations of private entities under such regulations; or prevent a governmental entity from using information not acquired through a cybersecurity exchange for regulatory purposes.

Additionally, this section provides that this title preempts any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the provision of cybersecurity services or the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities to the extent such law contains requirements inconsistent with this Title, but preserves all other state laws or requirements.

Section 708. Definitions. Section 708 defines terms including, “countermeasure”, “cybersecurity crime”, “cybersecurity threat”, “cybersecurity threat indicator”, “Federal entity”, “private entity”, and other key terms.