Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012

Bill Summary

Title I – Facilitating Sharing of Cyber Threat Information

- This title provides specific authorities relating to the voluntary sharing of cyber threat information among private entities, between a private entity and a non-federal government agency, and between any entity and a Federal cybersecurity center. This title does not create new bureaucracy, but instead allows entities to voluntarily share cyber threat information with the government through existing Federal cybersecurity centers.

- Federal contractors, specifically those providing electronic communication services, remote computing services, or cybersecurity services to a Federal agency or department, are required to share with such agency or department any cyber threat information that is directly related to their contractual services. The contractors may also share that information with a cybersecurity center. Once a Federal agency or department receives cyber threat information from a contractor, that agency or department is required to immediately provide the information to a cybersecurity center. These federal contractors often experience the same threats, vulnerabilities, and attacks as exclusively private network operators. Through this provision, the government will be privy to important cyber threat and real-time attack data to develop an informed threat picture without mandatory requirements on privately owned and operated networks.

- This title includes a limited exemption from antitrust laws that restrict the exchange of information between private entities. It also includes comprehensive liability protections for the private sector for defending its own networks.

- This title contains important protections for privacy and civil liberties. For example, the definition of cyber threat information is precisely tailored to apply only to certain types of information. Information that falls outside of this definition cannot be used, disclosed, or received under this title, nor can a private entity use its cybersecurity systems to obtain, identify, or possess any other types of information. In addition, the specific legal protections in this title only apply to information that falls within this definition. Further, this title includes numerous instances in which consent is required for subsequent use or disclosure of cyber threat information by the government and requires that the Federal government handle all cyber threat information in a reasonable manner that considers the need to protect privacy, including through anonymization, while fully accomplishing the title's objectives. The title also limits the Federal government's ability to use cyber threat information for certain serious criminal law enforcement purposes, while still preserving full use for cybersecurity and national security purposes.

- This title requires a comprehensive report to be prepared by the heads of each agency containing a cybersecurity center, in coordination with relevant privacy officials and the Privacy and Civil Liberties Oversight Board, which will consider, among other things, the privacy impact of this title as well as the adequacy of any steps taken to protect

privacy. This report will be due one year after enactment, and then bi-annually thereafter.

- This title requires procedures to be developed for the immediate sharing of classified, declassified, and unclassified information to ensure that information needed to secure networks is shared as fully as possible while still protecting intelligence sources and methods.

- This title also confirms that no person can have access to classified information relating to cyber security threats and vulnerabilities without appropriate security clearances. The Federal government, however, is directed to provide timely assistance in providing appropriate security clearances, in accordance with applicable procedures and requirements and as otherwise deemed appropriate, for individuals who are determined to be eligible for clearances and have a need-to-know classified information in order to carry out the title.

Title II – Coordination of Federal Information Security Policy

- This title updates the Federal Information Security Management Act (FISMA) to improve the security of Federal information systems.

- The federal government's current reliance on annual static checklists and manual reporting is outdated. This title instead directs the Secretary of Homeland Security to carry out an ongoing, automated threat assessment to maintain timely and actionable knowledge of the state of the security of Federal information systems, providing the federal government with a continuously updated agency-wide threat picture.

- Existing resources at the Department of Homeland Security (DHS) are leveraged by requiring federal civilian agencies to report information about security incidents and cyber threat information to a cybersecurity center.

- Under the current FISMA statute, the National Institute of Standards and Technology (NIST) has successfully ensured that federal civilian networks maintain security standards complementary to those implemented by national security networks. This title codifies and strengthens the current roles and activities NIST undertakes in disseminating cybersecurity standard setting for government networks. Under this title, the Secretary of Commerce, in consultation with the Secretary of Homeland Security, is directed to issue compulsory policies and directives for government agency information security operations and controls. Such policies do not apply to national security systems.

- Under this title, agency heads are required to delegate to their Chief Information Officer the authority and primary responsibility for implementing and maintaining the agency-wide information security program and providing information security protections commensurate with the risk and impact resulting from unauthorized access, use, disclosure, disruption, or destruction of agency information or information systems.

Title III – Criminal Penalties

- This title amends the Computer Fraud and Abuse Act (CFAA) to update federal criminal statutes and streamline existing, confusing penalties to facilitate the prosecution of cyber related crimes and of aggravated damage to critical infrastructure systems.

- This title fills a void in existing criminal law by establishing a criminal violation for aggravated damage to a critical infrastructure computer under the CFAA.

- This title limits enforcement of CFAA violations when the sole basis for a violation is an individual exceeding authorized access of a computer or website by violating the terms of a service agreement.

Title IV – Cybersecurity Research and Development

- This title reauthorizes the federal government-wide program on supercomputing, networking and information technology research and development, with a special emphasis on cybersecurity and supply chain security.

- The progress and funding levels of government-wide research and development projects are tracked and made publically available.

- Agencies are required to outline a strategic plan to encourage interdisciplinary research and development projects and address multi-agency, multi-faceted challenges of national importance, such as cybersecurity.

- The National Science Foundation (NSF) is directed to use its existing programs to improve education, as well as carry out the existing Federal Cyber Scholarship-for-Service program to recruit and train the next generation of information technology professionals.

- This title directs a task force to explore mechanisms to carry out collaborative research and development activities for cyber-physical systems with participants from universities, federal laboratories, and industry. Cyber-physical systems are systems found in infrastructure, healthcare, transportation, energy, and manufacturing, where the system's information technology and physical elements are tightly integrated. The task force will terminate upon submittal of its report to Congress, and task force members will serve without compensation,

- This title directs NIST to continue to ensure the coordination of federal agencies engaged in the development of international technical standards related to information system security.

- This title amends the Cybersecurity Research and Development Act to update grant-eligible areas and reauthorize existing grant programs for fiscal years 2012-2014 with existing funds made available by the America COMPETES Reauthorization Act of 2010.