HR 4263

SECURE IT Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: House
Policy Area: Science, Technology, Communications
Introduced: Mar 27, 2012
Current Status: Referred to the Subcommittee on Emerging Threats and Capabilities.
Latest Action: Referred to the Subcommittee on Emerging Threats and Capabilities. (Jul 10, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/house-bill/4263

Sponsor

Name: Rep. Bono Mack, Mary [R-CA-45]
Party: Republican • **State:** CA • **Chamber:** House

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Blackburn, Marsha [R-TN-7]	R · TN		Mar 27, 2012

Committee Activity

Committee	Chamber	Activity	Date
Armed Services Committee	House	Referred to	Jul 10, 2012
Intelligence (Permanent Select) Committee	House	Referred To	Mar 27, 2012
Judiciary Committee	House	Referred to	Apr 9, 2012
Oversight and Government Reform Committee	House	Referred To	Mar 27, 2012
Science, Space, and Technology Committee	House	Referred To	Mar 27, 2012

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

Bill	Relationship	Last Action
112 S 3342	Related bill	**Jun 28, 2012:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 438.
112 HR 2096	Related bill	**May 7, 2012:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.
112 HR 3834	Related bill	**May 7, 2012:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.
112 S 2151	Related bill	**Mar 1, 2012:** Read twice and referred to the Committee on Commerce, Science, and Transportation.
112 S 2111	Related bill	**Feb 16, 2012:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 324.
112 S 1152	Related bill	**Jun 7, 2011:** Read twice and referred to the Committee on Commerce, Science, and Transportation.

Summary (as of Mar 27, 2012)

Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 or SECURE IT Act of 2012 - Authorizes private entities to employ countermeasures and use cybersecurity systems to obtain, identify, or possess cyber threat information on its own networks or the networks of another entity with such entity's authorization.

Allows private entities, nonfederal government agencies, or state, tribal, or local governments to voluntarily disclose cyber threat information to designated cybersecurity centers or to each other to assist with preventing, investigating, or mitigating threats to information security.

Requires federal contractors of electronic communication, remote computing, or cybersecurity services to immediately provide the contracting agency with any cyber threat information directly related to the contract. Permits contractors to also provide such information to a cybersecurity center.

Directs federal agencies receiving such contractor-provided information to disclose it immediately to a cybersecurity center.

Declares that such contractor information requirements and procedures shall not apply with respect to services provided under a contract in effect on the date of enactment of this Act.

Permits cyber threat information provided to a cybersecurity center to be disclosed to, or used by, consistent with otherwise applicable law, the federal government for a cybersecurity or national security purpose or to prevent, investigate, or prosecute various criminal offenses for which law enforcement officials are authorized, under existing law, to seek a court order authorizing an interception of wire, oral, or electronic communications.

Prohibits federal, state, tribal, or local agencies from directly using such information to regulate an entity's lawful activities.

Sets forth conditions with regard to information provided to a cybersecurity center including: (1) the disclosure of such information to state, tribal, or local governments; (2) the use, distribution, and any prerequisite consent necessary for sharing such information; and (3) the legal treatment of such information under specified privileges, exemptions, ex parte communications rules, and requirements for disclosing public information and records.

Provides legal protections to entities engaged in authorized cybersecurity activities.

Directs the Director of National Intelligence (DNI) and Secretary of Defense (DOD) to develop procedures for sharing classified and unclassified information through cybersecurity centers.

Authorizes the Council of the Inspectors General on Integrity and Efficiency to review compliance by cybersecurity centers and federal agencies with required procedures, including privacy and civil liberty protections through anonymization and other methods.

Amends the Federal Information Security Management Act of 2002 to replace existing information security procedures for federal agencies with a new framework for coordinating and securing federal information.

Directs the Secretary of Commerce to issue compulsory and binding policies and directives governing agency information security operations. Requires that national security systems be overseen as directed by the President.

Requires each agency to comply with such policies and provide risk-commensurate information security protections for information systems used or operated by the agency or a contractor or other organization on an agency's behalf.

Requires each agency's Chief Information Officer to develop an agencywide information security program.

Directs the Secretary of Homeland Security (DHS) to: (1) designate a DHS entity to conduct an ongoing security analysis of agency information systems using automated processes, and (2) develop a timeline for each agency to adopt continuous monitoring systems. Sets forth separate requirements for national security systems.

Requires that federal information systems be based on National Institute of Standards and Technology (NIST) standards.

Amends the Computer Fraud and Abuse Act to increase and further delineate the criminal penalties for computer fraud and related activities.

Establishes an offense for aggravated damage to a public or private critical infrastructure computer that manages or controls systems or assets vital to national defense, national security, national economic security, or public health or safety.

Amends the High-Performance Computing Act of 1991 to re-designate the National High-Performance Computing Program as the Networking and Information Technology Research and Development Program.

Requires the Director of the Office of Science and Technology Policy (STP) to establish goals for inter-agency collaborative research and development with Program Component Areas, industry, institutions of higher education, federal laboratories, and international organizations. Directs agencies to develop a five-year strategic plan.

Requires that agencies be encouraged under the Program to address application areas with potential for contributions to national economic competitiveness and other societal benefits.

Directs the STP Director to continue a National Coordination Office (NCO) with a Director and full-time staff to: (1) provide technical and administrative support to agencies implementing the Program and to the advisory committee on networking and information technology, and (2) serve as the primary point of contact on federal networking and information technology activities.

Requires the NCO Director to convene: (1) a task force (with participants from institutions of higher education, federal laboratories, and industry) to report to Congress on options for the research, development, and organizational structure of cyber-physical systems; and (2) an interagency working group to report to Congress on the potential use of cloud computing for federally funded science and engineering research.

Defines "cyber-physical systems" as physical or engineered systems whose networking and information technology functions and physical elements are integrated and actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions.

Directs the STP Director to convene a university-industry task force to report to Congress on mechanisms for carrying out collaborative research, development, education, and training activities for cybersecurity.

Requires the National Science Foundation (NSF) to continue a Federal Cyber Scholarship-for-Service program.

Requires NIST to coordinate federal agencies engaged in the development of international technical standards.

Amends the Cyber Security Research and Development Act to add research areas eligible for NSF computer and network security research grants and to revise the application requirements for the establishment of a research center. Authorizes various grant programs, traineeships, and research centers through FY2014. Repeals the cyber security faculty development traineeship program.

Requires NIST to expand its checklist of requirements for government hardware and software systems to include security automation standards and protocols enabling standardized and interoperable technologies for continuous monitoring of information security within the federal government.

Requires NIST to conduct intramural security research activities under its computing standards program.

Actions Timeline

- **Jul 10, 2012:** Referred to the Subcommittee on Emerging Threats and Capabilities.
- **Apr 9, 2012:** Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
- **Mar 27, 2012:** Introduced in House
- **Mar 27, 2012:** Referred to the Committee on Science, Space, and Technology, and in addition to the Committees on Oversight and Government Reform, the Judiciary, Armed Services, and Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.