HR 1468

SECURE IT

Congress: 113 (2013–2015, Ended)
Chamber: House
Policy Area: Science, Technology, Communications
Introduced: Apr 10, 2013
Current Status: Referred to the Subcommittee on Research and Technology.
Latest Action: Referred to the Subcommittee on Research and Technology. (Jun 24, 2013)
Official Text: https://www.congress.gov/bill/113th-congress/house-bill/1468

Sponsor

Name: Rep. Blackburn, Marsha [R-TN-7]
Party: Republican • **State:** TN • **Chamber:** Senate

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Armed Services Committee	House	Referred to	Apr 19, 2013
Energy and Commerce Committee	House	Referred to	Apr 12, 2013
Intelligence (Permanent Select) Committee	House	Referred To	Apr 10, 2013
Judiciary Committee	House	Referred to	Apr 30, 2013
Oversight and Government Reform Committee	House	Referred To	Apr 10, 2013
Science, Space, and Technology Committee	House	Referred to	Jun 24, 2013

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

Bill	Relationship	Last Action
113 S 1193	Related bill	**Jun 20, 2013:** Read twice and referred to the Committee on Commerce, Science, and Transportation.
113 HR 967	Related bill	**Apr 17, 2013:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.

Summary (as of Apr 10, 2013)

Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2013 or SECURE IT - 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 such entities and governments providing electronic communication, remote computing, or information security services to a federal agency to inform the agency of a significant cyber incident involving the federal information system of that agency that: (1) is directly known as a result of providing such services and directly related to the provision of such services, and (2) has impeded or will impede the performance of a critical mission of the federal agency.

Defines "significant cyber incident" as a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in: (1) the exfiltration from a federal information system (an information system used or operated by an executive agency, contractor, or another organization on behalf of an executive agency) of data essential to the operation of the such a system, or (2) an incident in which an operational or technical control essential to the security or operation of a such a system was defeated.

Directs federal agencies receiving such significant cyber incident information to report the information to a cybersecurity center.

Permits cyber threat information provided to a cybersecurity center to be disclosed to, retained by, or used by, consistent with otherwise applicable federal 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 the disclosure, retention, or use of such information for any use not expressly permitted.

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, through cybersecurity centers, classified and unclassified information.

Authorizes the Council of the Inspectors General on Integrity and Efficiency to review compliance by the cybersecurity centers and federal agencies with required procedures, including privacy and civil liberty protections through anonymization or 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 Office of Management and Budget (OMB), in coordination with the Department of Homeland Security (DHS), to designate an entity to conduct an ongoing security analysis of agency information systems using automated processes. Requires each agency to develop a timeline for the implementation of technology facilitating continuous monitoring and threat assessments. 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 including technical solutions to cybersecurity, health care, energy management, transportation, cyber-physical systems, physical and behavioral phenomena, and privacy protection.

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.

Requires the STP Director to convene a task force to report to Congress on options for the research, development, and organizational structure of cyber-physical systems.

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

Requires the 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. Authorizes various grant programs through FY2015.

Requires commercial entities that acquire, maintain, store, or utilize personal information (covered entities) to take

reasonable measures to protect and secure data in electronic form containing personal information.

Directs a covered entity that owns or licenses such data to give notice of any breach of the security of the system that the entity reasonably believes has caused or will cause identity theft or other financial harm to each individual: (1) who is a U.S. citizen or resident; and (2) whose personal information was, or that the covered entity reasonably believes has been, accessed and acquired by an unauthorized person.

Requires: (1) a covered entity to notify the Secret Service or the Federal Bureau of Investigation (FBI) of a security breach of personal information involving more than 10,000 individuals; (2) a third-party entity contracted to maintain, store, or process data containing personal information to notify the covered entity of a breach of security of a system; and (3) a service provider to notify the covered entity if it becomes aware of a breach of security involving personal information owned or possessed by a covered entity and if such covered entity can be reasonably identified.

Sets forth enforcement authority for the Federal Trade Commission (FTC) along with civil monetary penalties for violations of such information protection and notification requirements. Preempts information security practices of the Communications Act of 1934 applicable to telecommunication carriers, satellite operators, and cable operators. Exempts certain financial institutions and entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Actions Timeline

- **Jun 24, 2013:** Referred to the Subcommittee on Research and Technology.
- **Apr 30, 2013:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
- **Apr 19, 2013:** Referred to the Subcommittee on Intelligence, Emerging Threats & Capabilities.
- **Apr 12, 2013:** Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
- **Apr 10, 2013:** Introduced in House
- **Apr 10, 2013:** Referred to the Committee on Science, Space, and Technology, and in addition to the Committees on Oversight and Government Reform, the Judiciary, Armed Services, Intelligence (Permanent Select), and Energy and Commerce, 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.

Generated by **LegiList** — https://legilist.com · Public data belongs to the public.