

## HR 756

Cybersecurity Enhancement Act of 2013

**Congress:** 113 (2013–2015, Ended)

**Chamber:** House

**Policy Area:** Science, Technology, Communications

**Introduced:** Feb 15, 2013

**Current Status:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transp

**Latest Action:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation. (Apr 17, 2013)

**Official Text:** <https://www.congress.gov/bill/113th-congress/house-bill/756>

### Sponsor

**Name:** Rep. McCaul, Michael T. [R-TX-10]

**Party:** Republican • **State:** TX • **Chamber:** House

### Cosponsors (13 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Hall, Ralph M. [R-TX-4]	R · TX		Feb 15, 2013
Rep. Langevin, James R. [D-RI-2]	D · RI		Feb 15, 2013
Rep. Lipinski, Daniel [D-IL-3]	D · IL		Feb 15, 2013
Rep. Lujan, Ben Ray [D-NM-3]	D · NM		Feb 15, 2013
Rep. Matsui, Doris O. [D-CA-6]	D · CA		Feb 15, 2013
Rep. Meehan, Patrick [R-PA-7]	R · PA		Feb 15, 2013
Rep. Smith, Lamar [R-TX-21]	R · TX		Feb 15, 2013
Rep. Garrett, Scott [R-NJ-5]	R · NJ		Feb 25, 2013
Rep. Miller, Candice S. [R-MI-10]	R · MI		Feb 25, 2013
Rep. Rogers, Mike J. [R-MI-8]	R · MI		Feb 25, 2013
Rep. Stewart, Chris [R-UT-2]	R · UT		Feb 27, 2013
Rep. Thornberry, Mac [R-TX-13]	R · TX		Feb 27, 2013
Rep. Esty, Elizabeth H. [D-CT-5]	D · CT		Mar 12, 2013

### Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Referred To	Apr 17, 2013
Science, Space, and Technology Committee	House	Reported By	Apr 11, 2013

### Subjects & Policy Tags

#### Policy Area:

Science, Technology, Communications

## Related Bills

Bill	Relationship	Last Action
113 S 1353	Related bill	<b>Dec 18, 2014:</b> Became Public Law No: 113-274.

**(This measure has not been amended since it was reported to the House on April 11, 2013. The summary of that version is repeated here.)**

Cybersecurity Enhancement Act of 2013 - **Title I: Research and Development** - (Sec. 103) Directs specified federal agencies participating in the National High-Performance Computing Program to: (1) transmit to Congress a cybersecurity strategic research and development plan and triennial updates, and (2) develop and annually update an implementation roadmap for such plan.

Instructs the participating agencies, in developing and updating the strategic plan, to solicit recommendations and advice from the advisory committee on high-performance computing and a wide range of specified stakeholders.

Directs such agencies to establish a mechanism to track ongoing and completed federal cybersecurity research and development projects and associated funding. Requires such information to be made available to the public.

(Sec. 104) Provides for the award of computer and network security research grants by the National Science Foundation (NSF) in the research areas of social and behavioral factors, including human-computer interactions, identity management, as well as the detection, investigation, and prosecution of cyber-crimes involving organized crime and crimes against children. Authorizes appropriations for FY2014-FY2016 for such grants.

(Sec. 105) Requires applications for the establishment of Computer and Network Security Research Centers to include a description of how such Centers will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions. Authorizes appropriations for FY2014-FY2016 for such Centers.

Authorizes appropriations to NSF for FY2014-FY2016 for: (1) computer and network security capacity building grants, (2) grants under the Scientific and Advanced Technology Act for the national advanced scientific and technical education program and national centers of scientific and technical education, and (3) grants for graduate traineeships programs in computer and network security research.

Repeals the Cyber Security Faculty Development Traineeship Program.

(Sec. 106) Requires the NSF Director to continue carrying out a Scholarship for Service program under the Cyber Security Research and Development Act to recruit and train the next generation of federal cybersecurity professionals and to increase the capacity of the higher education system to produce an information technology workforce with the skills necessary to enhance the security of the nation's communications and information infrastructure.

Requires the program to: (1) provide scholarships for tuition, fees, and a stipend for up to two years to students pursuing a bachelor's or master's degree and up to three years to students pursuing a doctoral degree in a cybersecurity field upon condition that a scholarship recipient, upon the completion of the degree, serves as a cybersecurity professional within the federal workforce (or in another specified cybersecurity capacity) for a specified period of time; (2) provide scholarship recipients with summer internships or other temporary appointments in the federal information technology workforce; and (3) increase, through competitive grants, the capacity of U.S. higher education institutions to produce highly qualified cybersecurity professionals.

(Sec. 107) Directs the President to transmit a report to Congress addressing the cybersecurity workforce needs of the federal government.

(Sec. 108) Requires the Director of the Office of Science and Technology Policy to convene a cybersecurity university-industry task force to explore mechanisms for carrying out collaborative research, development, education, and training activities through a consortium or other appropriate entity. Terminates the task force upon transmittal of a report to Congress.

(Sec. 109) Revises provisions under the Cyber Security Research and Development Act concerning the development and dissemination by the National Institute of Standards and Technology (NIST) of security risk checklists associated with computer systems that are, or are likely to become, widely used within the federal government.

Requires the NIST Director to establish priorities for the development, and revision as necessary, of security automation standards, associated reference materials (including protocols), and checklists associated with such systems in order to enable standardized and interoperable technologies, architectures, and frameworks to continuously monitor information security within the federal government.

Instructs the NIST Director to ensure that federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed pursuant to this section.

(Sec. 110) Requires NIST to conduct intramural security research activities under its computing standards program.

(Sec. 111) Directs NSF and NIST to support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics.

**Title II: Advancement of Cybersecurity Technical Standards** - (Sec. 202) Requires the NIST Director to ensure the coordination of federal agencies engaged in the development of international technical standards related to information system security. Requires the development and transmittal to Congress of a plan to ensure coordination by such federal agencies. Instructs the Director to ensure consultation with appropriate private sector stakeholders.

(Sec. 203) Requires the NIST Director, in collaboration with the federal Chief Information Officers Council, to continue to develop and encourage implementation of a comprehensive strategy for the use and adoption of cloud computing services by the federal government.

Requires consideration to be given to activities that: (1) accelerate the development, in collaboration with the private sector, of standards that address the interoperability and portability of cloud computing services; (2) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and (3) support, in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for federal agencies to use in addressing security and privacy requirements.

(Sec. 204) Requires the NIST Director, in collaboration with the National Coordination Office of the Networking and Information Technology Research and Development program, to continue the coordination of a cybersecurity awareness and education program for increasing the knowledge, skills, and awareness of cybersecurity risks, consequences, and best practices through: (1) the widespread dissemination of cybersecurity technical standards and best practices identified by NIST; (2) efforts to make cybersecurity best practices usable by individuals, small to medium-sized businesses, state, local, and tribal governments, and educational institutions; (3) improving the state of cybersecurity education at all educational levels; and (4) efforts to attract, recruit, and retain qualified professionals to the federal cybersecurity workforce and improve the skills and training of such workforce. Requires the NIST Director to implement

and transmit a strategic plan to Congress to guide federal programs and activities in support of a specified comprehensive cybersecurity awareness and education program.

(Sec. 205) Requires the NIST Director to continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria with regard to identity management research and development.

(Sec. 206) Prohibits the authorization of any additional funds to carry out this Act and the amendments made by this Act. Requires this Act and the amendments made by this Act to be carried out using otherwise authorized or appropriated amounts.

## Actions Timeline

---

- **Apr 17, 2013:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.
- **Apr 16, 2013:** Mr. Smith (TX) moved to suspend the rules and pass the bill, as amended.
- **Apr 16, 2013:** Considered under suspension of the rules. (consideration: CR H2042-2048)
- **Apr 16, 2013:** DEBATE - The House proceeded with forty minutes of debate on H.R. 756.
- **Apr 16, 2013:** At the conclusion of debate, the Yeas and Nays were demanded and ordered. Pursuant to the provisions of clause 8, rule XX, the Chair announced that further proceedings on the motion would be postponed.
- **Apr 16, 2013:** Considered as unfinished business. (consideration: CR H2054)
- **Apr 16, 2013:** Passed/agreed to in House: On motion to suspend the rules and pass the bill, as amended Agreed to by the Yeas and Nays: (2/3 required): 402 - 16 (Roll no. 107).(text: CR H2042-2045)
- **Apr 16, 2013:** On motion to suspend the rules and pass the bill, as amended Agreed to by the Yeas and Nays: (2/3 required): 402 - 16 (Roll no. 107). (text: CR H2042-2045)
- **Apr 16, 2013:** Motion to reconsider laid on the table Agreed to without objection.
- **Apr 11, 2013:** Reported (Amended) by the Committee on Science, Space, and Technology. H. Rept. 113-33.
- **Apr 11, 2013:** Placed on the Union Calendar, Calendar No. 19.
- **Mar 14, 2013:** Committee Consideration and Mark-up Session Held.
- **Mar 14, 2013:** Ordered to be Reported (Amended) by Voice Vote.
- **Feb 15, 2013:** Introduced in House
- **Feb 15, 2013:** Referred to the House Committee on Science, Space, and Technology.