S 1353

Cybersecurity Enhancement Act of 2014

Congress: 113 (2013–2015, Ended)
Chamber: Senate
Policy Area: Science, Technology, Communications
Introduced: Jul 24, 2013
Current Status: Became Public Law No: 113-274.
Latest Action: Became Public Law No: 113-274. (Dec 18, 2014)
Law: 113-274 (Enacted Dec 18, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/senate-bill/1353

Sponsor

Name: Sen. Rockefeller, John D., IV [D-WV]
Party: Democratic • **State:** WV • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Thune, John [R-SD]	R · SD		Jul 24, 2013

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Reported By	Jul 24, 2014

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

Bill	Relationship	Last Action
113 HR 756	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 Dec 18, 2014)

(This measure has not been amended since it was passed by the Senate on December 11, 2014. The summary of that version is repeated here.)

Cybersecurity Enhancement Act of 2014 - **Title I: Public-Private Collaboration on Cybersecurity** - (Sec. 101) Amends the National Institute of Standards and Technology Act to permit the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce cyber risks to critical infrastructure.

Requires the Director, in carrying out such activities, to: (1) coordinate regularly with, and incorporate the industry expertise of, relevant private sector personnel and entities, critical infrastructure owners and operators, sector coordinating councils, Information Sharing and Analysis Centers, and other relevant industry organizations; (2) consult with the heads of agencies with national security responsibilities, sector-specific agencies, state and local governments, governments of other nations, and international organizations; (3) identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help identify, assess, and manage cyber risks; and (4) include methodologies to mitigate impacts on business confidentiality, protect individual privacy and civil liberties, incorporate voluntary consensus standards and industry best practices, align with international standards, and prevent duplication of regulatory processes.

Prohibits the Director from prescribing a specific solution or requiring that products or services be designed or manufactured in a particular manner.

Prohibits information provided to NIST for purposes of developing cyber risk standards from being used by federal, state, tribal, or local agencies to regulate the activity of any entity.

Directs the Comptroller General (GAO) to submit biennial reports over a specified period concerning NIST's progress in facilitating the development of such standards and procedures. Requires such reports to address the extent to which such standards: (1) are voluntary and led by industry representatives, (2) have been promoted by federal agencies and adopted by sectors of critical infrastructure, and (3) have protected against cyber threats. Instructs the Comptroller General to include in such reports an assessment of the reasons behind decisions of sectors to adopt or not adopt such standards.

Title II: Cybersecurity Research and Development - (Sec. 201) Directs the following agencies, working through the National Science and Technology Council and the Networking and Information Technology Research and Development Program, to develop, and update every four years, a federal cybersecurity research and development strategic plan:

- Department of Agriculture (USDA),
- Department of Commerce,
- Department of Defense (DOD),
- Department of Education,
- Department of Energy (DOE),
- Department of Health and Human Services (HHS),
- Department of the Interior,

Environmental Protection Agency (EPA),
- National Aeronautics and Space Administration (NASA),
- National Science Foundation (NSF), and
- other agencies as the President or the Director of the Office of Science and Technology Policy (OSTP) considers appropriate under the High-Performance Computing Act of 1991.

Requires the plan to be based on an assessment of cybersecurity risk to guide the overall direction of federal cybersecurity and information assurance research and development for information technology and networking systems.

Directs the agencies to build upon existing programs to meet cybersecurity objectives, such as how to: (1) guarantee individual privacy, verify third-party software and hardware, and address insider threats; (2) determine the origin of messages transmitted over the Internet; and (3) protect information stored using cloud computing or transmitted through wireless services.

Requires the plan to describe how agencies will focus on technologies to protect consumer privacy and enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure.

Requires the agencies to submit the plan and each update to Congress.

Directs the NSF to support cybersecurity research and to review cybersecurity test beds. Permits the NSF, if it determines that additional test beds are necessary, to award grants to institutions of higher education or research and development nonprofit institutions to establish such additional test beds.

Requires the OSTP to coordinate with other ongoing research initiatives.

Amends the Cyber Security Research and Development Act to permit NSF research and development grants for: (1) secure fundamental protocols that are integral to inter-network communications and data exchange; (2) secure software engineering and software assurance; (3) holistic system security to address trusted and untrusted components, reduce vulnerabilities proactively, address insider threats, and support privacy; (4) monitoring, detection, mitigation, and rapid recovery methods; and (5) secure wireless networks, mobile devices, and cloud infrastructure.

Directs specified agencies under the High-Performance Computing Act of 1991 to support research leading to a scientific foundation for the field of cybersecurity.

(Sec. 202) Expands the criteria to be considered by the NSF when evaluating grant applications of institutions seeking to establish Centers for Computer and Network Security Research to include: (1) the applicant's affiliations with private sector entities and existing federal research programs; (2) experience managing public-private partnerships; (3) capabilities to conduct interdisciplinary cybersecurity research in a secure environment; and (4) research in areas such as systems security, wireless security, networking and protocols, formal methods and high-performance computing, nanotechnology, or industrial control systems.

(Sec. 203) Revises provisions under the Cyber Security Research and Development Act concerning NIST's development and dissemination of security risk checklists associated with computer systems that are, or are likely to become, widely used within the federal government.

Requires NIST 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 NIST to ensure that federal agencies are informed of the availability of such standards, reference materials, or checklists.

(Sec. 204) Requires NIST to conduct intramural security research activities under its computing standards program.

Title III: Education and Workforce Development - (Sec. 301) Directs the Department of Commerce, NSF, and the Department of Homeland Security (DHS) to support competitions and challenges to recruit individuals to perform information technology security duties or to stimulate cybersecurity innovations.

Authorizes the Office of Personnel Management (OPM) to support internships or other work experience in the federal government for the winners of such competitions and challenges.

(Sec. 302) Directs NSF to continue the Federal Cyber Scholarship-for-Service program under which recipients agree to work in the cybersecurity mission of a federal, state, local, or tribal agency for a period equal to the length of their scholarship. Limits each scholarship to a maximum of three years. Requires NSF to evaluate and report periodically to Congress on: (1) the success of recruiting individuals for such scholarships, and (2) hiring and retaining those individuals in the public sector workforce.

Title IV: Cybersecurity Awareness and Preparedness - (Sec. 401) Directs NIST to continue coordinating a national cybersecurity awareness and education program to: (1) disseminate technical standards and make best practices usable by individuals, small to medium-sized businesses, educational institutions, and state, local, and tribal governments; (2) increase public awareness and understanding of cybersecurity; (3) support education programs; and (4) evaluate workforce needs. Requires NIST to develop a strategic plan to guide federal activities in support of such program. Directs NIST to transmit such plan to Congress every five years.

Title V: Advancement of Cybersecurity Technical Standards - (Sec. 502) Requires NIST 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 NIST to ensure consultation with appropriate private sector stakeholders.

(Sec. 503) Requires NIST, in coordination with OMB and 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. 504) Requires NIST to continue a program to support the development of voluntary and cost-effective technical standards, metrology, testbeds, and conformance criteria with regard to identity management research and development.

Actions Timeline

- **Dec 18, 2014:** Signed by President.
- **Dec 18, 2014:** Became Public Law No: 113-274.
- **Dec 15, 2014:** Presented to President.
- **Dec 11, 2014:** Measure laid before Senate by unanimous consent. (consideration: CR H6665-6669; text of measure as reported in Senate: CR S6665-6668)
- **Dec 11, 2014:** The committee substitute agreed to by Unanimous Consent.
- **Dec 11, 2014:** Passed/agreed to in Senate: Passed Senate with an amendment by Unanimous Consent.
- **Dec 11, 2014:** Passed Senate with an amendment by Unanimous Consent.
- **Dec 11, 2014:** Received in the House.
- **Dec 11, 2014:** Held at the desk.
- **Dec 11, 2014:** Message on Senate action sent to the House.
- **Dec 11, 2014:** Considered by unanimous consent. (consideration: CR H9294-9299)
- **Dec 11, 2014:** Mr. McCaul asked unanimous consent to take from the Speaker's table and consider.
- **Dec 11, 2014:** Passed/agreed to in House: On passage Passed without objection.(text: CR H9294-9299)
- **Dec 11, 2014:** On passage Passed without objection. (text: CR H9294-9299)
- **Dec 11, 2014:** Motion to reconsider laid on the table Agreed to without objection.
- **Nov 12, 2014:** By Senator Rockefeller from Committee on Commerce, Science, and Transportation filed written report. Report No. 113-270.
- **Jul 24, 2014:** Committee on Commerce, Science, and Transportation. Reported by Senator Rockefeller with an amendment in the nature of a substitute. Without written report.
- **Jul 24, 2014:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 490.
- **Jul 30, 2013:** Committee on Commerce, Science, and Transportation. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Jul 25, 2013:** Committee on Commerce, Science, and Transportation. Hearings held.
- **Jul 24, 2013:** Introduced in Senate
- **Jul 24, 2013:** Sponsor introductory remarks on measure. (CR S5909)
- **Jul 24, 2013:** Read twice and referred to the Committee on Commerce, Science, and Transportation. (text of measure as introduced: CR S5909-5912)

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