S 773

Cybersecurity Act of 2010

Congress: 111 (2009–2011, Ended)
Chamber: Senate
Policy Area: Science, Technology, Communications
Introduced: Apr 1, 2009
Current Status: By Senator Rockefeller from Committee on Commerce, Science, and Transportation filed written report.
Latest Action: By Senator Rockefeller from Committee on Commerce, Science, and Transportation filed written report. Report No. 111-384. (Dec 22, 2010)
Official Text: https://www.congress.gov/bill/111th-congress/senate-bill/773

Sponsor

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

Cosponsors (4 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Nelson, Bill [D-FL]	D · FL		Apr 1, 2009
Sen. Snowe, Olympia J. [R-ME]	R · ME		Apr 1, 2009
Sen. Bayh, Evan [D-IN]	D · IN		Apr 2, 2009
Sen. Mikulski, Barbara A. [D-MD]	D · MD		Apr 22, 2010

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Reported By	Dec 17, 2010

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of Dec 17, 2010)

Cybersecurity Act of 2010 - (Sec. 3) Defines "cybersecurity" as "information security" which is defined (in federal code provisions related to the coordination of federal information policy) as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, availability, and authentication, as those terms are further defined in specified federal code provisions related to information security. Defines "information system" as any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, including certain industrial control systems.

(Sec. 4) Requires the President to initiate a rulemaking to establish a procedure for the designation, as a critical infrastructure information system under this Act, any information system the infiltration, incapacitation, or disruption of which would have a debilitating impact on national security, including national economic security and national public health or safety. Requires such a final rule to: (1) set forth criteria for such designations; (2) provide for emergency and temporary designations; (3) ensure the protection of confidential and proprietary information associated with nongovernmental systems from disclosure; (4) ensure the protection of classified and sensitive security information; and (5) establish a procedure for the owner or operator of an information system to appeal, or request modification of, such designation of that system or network.

Title I: Workforce Development - (Sec. 101) Directs the President to enter into an agreement with the National Academies to conduct a study, and submit a related report to the President and Congress, evaluating government, academic, and private-sector accreditation, training, and certification programs for personnel working in cybersecurity and recommending improvements for such programs. Requires the President, in consultation with sector coordinating councils and relevant governmental agencies, regulatory entities, industry sectors, and nongovernmental organizations, to: (1) develop and annually review and update guidance for the identification and categorization of positions for cybersecurity personnel (with certification requirements) within the federal government; (2) direct owners and operators of U.S. critical infrastructure information systems to develop and annually review and update guidance for the identification and categorization of positions for cybersecurity personnel (with certification requirements) within their respective information systems; and (3) convene sector specific working groups to establish auditable private-sector developed accreditation, training, and certification programs for critical infrastructure information system personnel.

Directs the President to require each owner or operator of a U.S. critical infrastructure information system to semiannually report the results of independent audits that evaluate compliance with specified accreditation, training, and certification programs. Authorizes the President to publicly recognize owners and operators of systems whose independent audits comply with such programs. Requires owners or operators of systems that fail to demonstrate substantial compliance with such programs (through two consecutive independent audits) to collaboratively, in consultation with sector coordinating councils, relevant governmental agencies, and regulatory entities, develop and implement a remediation plan. Directs the President to publish an annual noncompulsory reference list of cybersecurity accreditation, training, and certification programs whose rigor and effectiveness are beneficial to cybersecurity.

(Sec. 102) Directs the Director of the National Science Foundation (NSF) to establish a Federal Cyber Scholarship-for-Service program to recruit and train information technology professionals and security managers for federal, state, local, and tribal governments. Requires scholarship recipients, as a condition of receiving such a scholarship, to serve in a federal, state, local, or tribal information technology workforce for a period equal to the length of the scholarship following graduation if offered employment in that field by such an agency.

Sets forth hiring authority and scholarship eligibility provisions. Requires the NSF Director to periodically report to Congress on scholarship recruitment, hiring, and retention of individuals in the public sector workforce.

Authorizes appropriations to NSF for FY2010-FY2014.

(Sec. 103) Requires the Director of the National Institute of Standards and Technology (NIST) to establish cybersecurity competitions and challenges with cash prizes to recruit individuals for the federal information technology workforce and stimulate innovation (in basic and applied cybersecurity research, technology development, and prototype demonstration) that has potential for application to such federal government activities. Establishes competitions and challenges for middle school, high school, undergraduate, and graduate students, and academic and research institutions. Sets forth provisions related to prize eligibility, judges, and competition administration.

Authorizes appropriations to NIST for FY2010-FY2014.

(Sec. 104) Requires the head of each federal agency to develop an annual strategic cybersecurity workforce plan (based on guidance from the President, the Office of Personnel Management [OPM], the Chief Human Capital Officers Council, and the Chief Information Officers Council) as part of the agency performance plan, including: (1) hiring projections (with occupation and grade levels); (2) strategic planning to address skill deficiencies; (3) recruitment strategies; (4) talent assessments; (5) hiring process streamlining; (6) contractor management capabilities; (7) recruiting and hiring barrier analyses (including analyses of compensation, classification, hiring flexibilities, and the hiring process, and recommendations to overcome those barriers); and (8) training and development for current employees.

Directs the President to coordinate the establishment of new job classifications for cybersecurity functions in government and certification requirements for each job category.

(Sec. 105) Requires each agency to measure and collect information on cybersecurity hiring effectiveness with respect to the: (1) ability to reach and recruit well-qualified talent from diverse talent pools; (2) use and impact of special hiring authorities and flexibilities (including student internship and scholarship programs) to recruit the most qualified and diverse candidates (including veteran, minority, and disabled candidates); and (3) age, education level, and source of applicants. Requires related hiring process assessments by hiring managers, applicants, and new hires. Directs OPM to provide such information (in a consistent format to allow for a comparison of hiring effectiveness and experience across demographic groups and agencies) first to Congress and then on OPM's public website.

Title II: Plans and Authority - (Sec. 201) Directs the President to develop and implement a comprehensive national cybersecurity strategy, including: (1) a long-term vision of the nation's cybersecurity future; and (2) a plan that addresses all aspects of national security, as it relates to cybersecurity, including the proactive engagement of, and collaboration between, the federal government and the private sector.

Requires the President to: (1) review critical functions likely to be impacted by a cyber attack and develop a strategy for the acquisition, storage, and periodic replacement of assets to support those functions; (2) direct an annual review of all federal cyber technology research and development investments; and (3) promulgate rules for federal professional responsibilities regarding cybersecurity, and provide to Congress an annual report on federal agency compliance with such rules.

Directs the President, in collaboration with owners and operators of U.S. critical infrastructure information systems, sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations, to develop and rehearse detailed response and restoration plans that clarify specific roles, responsibilities, and authorities of

government and private sector actors during cybersecurity emergencies, and that identify the types of events and incidents that would constitute a cybersecurity emergency.

Authorizes the President, in the event of an immediate threat to strategic national interests involving compromised federal government or U.S. critical infrastructure information systems, to: (1) declare a cybersecurity emergency; and (2) implement such collaborative emergency response and restoration plans.

Requires the President, in the event of a declaration of cybersecurity emergency, to: (1) within 48 hours submit to Congress a written report setting forth the circumstances necessitating the emergency declaration and the estimated scope and duration of the emergency; and (2) report to Congress at least every 30 days on the status, scope, and duration of the emergency for as long as the declaration remains in effect.

Prohibits the preceding provisions from being construed as authorizing an expansion of existing Presidential authorities.

(Sec. 202) Directs the President to complete biennial reviews of the cyber posture of the United States, including: (1) an unclassified summary of roles, missions, accomplishments, plans, and programs; (2) an examination of the cyber strategy, force structure, personnel, modernization plans, infrastructure, budget plan, and the nation's ability to recover from a cyber emergency; and (3) other elements of the cyber program and policies to determine and express the U.S. cyber strategy and establish a revised cyber program for the next two years.

Requires the President to apprise the Cybersecurity Advisory Panel (established in title IV of this Act) of the work undertaken in the conduct of such reviews and to submit a related report to Congress every two years.

(Sec. 203) Directs the Secretary of Commerce to implement a system to provide dynamic, comprehensive, real-time cybersecurity status and vulnerability information of all federal government information systems managed by the Department of Commerce (including an inventory of such systems, vulnerabilities of such systems, and corrective action plans for those vulnerabilities) and submit a related report to Congress.

(Sec. 204) Requires NIST to: (1) recognize and promote auditable, private-sector developed cybersecurity risk measurement techniques, risk management measures and best practices for all federal government and U.S. critical infrastructure information systems; and (2) review and reconsider those recognitions, at least semiannually, in order to account for advances in such cybersecurity risk management techniques, measures, and best practices. Directs all federal agencies to measure their risk in each operating unit using such techniques and to comply with or exceed such cybersecurity risk management measures and best practices.

Authorizes the President to publicly recognize those owners and operators of U.S. critical infrastructure information systems whose independent audits demonstrate compliance with cybersecurity risk measurement techniques, risk management measures, and best practices.

Directs the President to require owners or operators of U.S. critical infrastructure information systems that fail to demonstrate substantial compliance with such cybersecurity risk measurement techniques, measures, and best practices (through two consecutive independent audits) to collaboratively, in consultation with sector coordinating councils, relevant governmental agencies, and regulatory entities, develop and implement a remediation plan.

Requires the NIST Director to: (1) direct U.S. cybersecurity efforts before all international standards development bodies related to cybersecurity; (2) develop and implement a strategy to engage international standards bodies with respect to the development of technical standards related to cybersecurity; and (3) submit such strategy to Congress.

Directs NIST to adopt a risk-based approach in the development of federal cybersecurity guidance for federal information systems.

Requires the Federal Communications Commission (FCC) to report to Congress on the cybersecurity of commercial broadband networks related to public safety, consumer welfare, healthcare, education, energy, government, security and other national purposes, including consumer education considerations and outreach programs to assist individuals in protecting home and personal computers and other devices.

(Sec. 205) Directs the Comptroller General to review federal laws applicable to U.S. cybersecurity-related activities, including: (1) the Privacy Protection Act of 1980; (2) Electronic Communications Privacy Act of 1986; (3) Computer Security Act of 1987; (4) Federal Information Security Management Act of 2002; (5) E-Government Act of 2002; (6) Defense Production Act of 1950; (7) specified provisions related to administrative procedures for federal agencies; (8) Federal Advisory Committee Act; and (9) other federal laws and applicable Executive Orders or agency rules, regulations, or guidelines bearing upon cybersecurity-related activities. Requires a related report to Congress including recommended changes to advance cybersecurity and protect civil liberties.

(Sec. 206) Requires the Director of National Intelligence (DNI), the Secretary of Commerce, the Secretary of Homeland Security (DHS), the Attorney General (DOJ), the Secretary of Defense (DOD), and the Secretary of State to submit to the Congress a joint assessment of, and report on, cybersecurity threats to and vulnerabilities of federal information systems and U.S. critical infrastructure information systems.

(Sec. 207) Directs the President to work with representatives of foreign governments, private sector entities, and nongovernmental organizations to: (1) develop norms, organizations, and other cooperative activities for international engagement to improve cybersecurity and encourage international cooperation in improving cybersecurity on a global basis; and (2) provide an annual report to Congress on the progress of such international initiatives.

(Sec. 208) Requires the Administrator of the General Services Administration (GSA) to require that requests for information and requests for proposals for federal information systems products and services include: (1) cybersecurity risk measurement techniques, risk management measures, and best practices; and (2) cybersecurity professional certifications.

(Sec. 209) Directs the President to conduct an annual evaluation of the sufficiency of present access to classified information among owners and operators of U.S. critical infrastructure information systems and submit a related report to Congress. Allows the President, if necessary to enhance public-private information sharing and cybersecurity collaboration, to: (1) grant additional security clearances to such owners and operators; and (2) delegate original classification authority to appropriate federal officials on cybersecurity matters.

(Sec. 210) Requires the President to review, and report to Congress, on the feasibility of an identity management and authentication program, with civil liberties and privacy protections, for federal government and U.S. critical infrastructure information systems.

(Sec. 211) Requires NIST to issue a public report evaluating identity authentication solutions to determine the necessary level of functionality and privacy protection, based on risk, commensurate with the level of data assurance and sensitivity, as defined by OMB e-Authentication Guidance Memorandum 04-04.

Title III: Cybersecurity Knowledge Development - (Sec. 301) Directs the Secretary of Commerce to develop and implement a national cybersecurity awareness campaign. Requires the Secretary of Education to identify and promote

age appropriate information and programs for grades K-12 regarding cyber safety, cybersecurity, and cyber ethics.

(Sec. 302) Requires the NSF Director to develop a national cybersecurity research and development plan encouraging computer and information science and engineering research to meet specified cybersecurity challenges, including how to design and build software, test and verify third-party software, and guarantee the privacy of an individual's identity, information, or lawful transactions when stored in distributed systems or transmitted over networks.

Directs the NSF Director to: (1) submit to Congress a report on the state of secure coding education in certain schools that received NSF funding; and (2) establish a program to award grants to institutions of higher education to establish cybersecurity testbeds capable of realistic modeling of real-time cyber attacks and defenses to support the rapid development of new cybersecurity defenses, techniques, and processes.

Amends the Cybersecurity Research and Development Act to include as grant-eligible research areas: (1) secure fundamental protocols in inter-network communications and data exchange; (2) secure software engineering and software assurance; (3) holistic system security that addresses the building of secure systems from trusted and untrusted components, reduces vulnerabilities, addresses insider threats, and supports privacy in conjunction with improved security; (4) monitoring and detection; and (5) mitigation and rapid recovery methods.

Authorizes increasing appropriations to NSF in FY2010-FY2014 for: (1) computer and network security research grants; (2) computer network security research centers; (3) computer and network security capacity building grants; (4) Scientific and Advanced Technology Act of 1992 grants; and (5) graduate traineeships in computer and network security research. Maintains, for FY2010-FY2014, the current statutory level of authorization of appropriations for the Cyber Security Faculty Development Traineeship Program.

Directs NIST, as part its specified responsibilities related to the National High-Performance Computing Program, to develop and propose standards and guidelines, and develop measurement techniques and test methods, for enhanced cybersecurity for computer networks and common user interfaces to systems.

(Sec. 303) Requires the NSF Director to establish a grant program to fund public and private educational institutions to develop graduate and undergraduate level curricula that address cybersecurity in modern industrial control systems. Authorizes appropriations for FY2011-FY2012.

Title IV: Public-Private Collaboration - (Sec. 401) Directs the President to establish or designate a Cybersecurity Advisory Panel (CAP) with representatives of industry, academic, nonprofit organizations, interest groups and advocacy organizations, and state and local governments qualified to provide advice and information on cybersecurity research, development, demonstrations, education, personnel, technology transfer, commercial application, or societal and civil liberty concerns.

Requires CAP to advise the President on the national cybersecurity program and strategy matters including: (1) trends and developments in science research and development; (2) the readiness and capacity of federal and national workforces to implement the program, and steps necessary to improve workforce readiness and capacity; (3) the balance among the components of the national strategy, including funding for program components; (4) whether the strategy, priorities, and goals are helping to maintain U.S. leadership and defense in cybersecurity; (5) the management, coordination, implementation, and activities of the strategy; (6) concerns of federal, state, and local law enforcement entities; and (7) societal and civil liberty concerns.

Directs CAP to report to the President at least every two years.

Exempts CAP from sunset provisions of the Federal Advisory Committee Act.

(Sec. 402) Directs the Secretary of Commerce to provide assistance for the creation and support of Regional Cybersecurity Centers to: (1) promote private-sector developed cybersecurity risk measurement techniques, risk management measures, and best practices; and (2) enhance the cybersecurity of small and medium sized businesses. Requires each center to be affiliated with a U.S.-based nonprofit institution or organization, or consortium, that is awarded financial assistance under this title. Directs such centers to make loans, on a short-term basis, of items of advanced protective cybersecurity measures to small businesses with less than 100 employees.

Authorizes the Secretary to provide, subject to exception, up to 50% of a center's annual operating and maintenance costs for a period not to exceed six years.

Permits any nonprofit institution, or consortia of nonprofit institutions, with certain specified assurances, to apply for financial support.

Sets forth awards criteria, with competitive, merit-based review, including geographic diversity, extent of service area, and the percentage of funding and amount of in-kind commitment for the applicant from other sources.

Requires each center receiving such financial assistance to be evaluated during its third year by an evaluation panel composed of private experts and federal officials. Prohibits funding for the fourth through the sixth years unless the center receives a positive evaluation and authorizes declining levels of funding through the sixth year if such evaluation is positive. Allows additional financial support to a center after the sixth year if it has received a positive evaluation though an independent review. Requires an additional independent review at least every two years after the sixth year. Limits funding for a fiscal year after the sixth year to an amount not to exceed one-third of annual operating and maintenance costs.

Applies federal patent law related to the patent rights in inventions made with federal assistance to the promotion of technology from research by centers under this title, except for contracts for such specific technology extension or transfer services as specified by statute or by the President.

(Sec. 403) Directs the President to: (1) review and assess existing information sharing models used by federal agencies; and (2) establish or designate a facility to serve as the central cybersecurity threat and vulnerability information clearinghouse for the federal government and U.S. critical infrastructure information systems incorporating the best practices and concepts of operations of existing information sharing models to promote the sharing of public-private cybersecurity threat and vulnerability information.

Sets forth requirements for promulgating information sharing rules and procedures that: (1) expand the federal government's sharing of cybersecurity threat and vulnerability information with critical infrastructure information systems owners and operators; (2) ensure confidentiality and privacy protections for individuals and personally identifiable information, and for private sector-owned intellectual property and proprietary information; (3) establish criteria under which critical infrastructure information systems owners or operators share actionable cybersecurity threat and vulnerability information and relevant data with the federal government; (4) protect against, or mitigate, civil and criminal liability implicated by shared information; and (5) otherwise enhance sharing of cybersecurity threat and vulnerability information between critical infrastructure information systems owners or operators and the federal government.

(Sec. 404) Requires the President to report to Congress on the feasibility of creating a market for cybersecurity risk management.

Actions Timeline

- **Dec 22, 2010:** By Senator Rockefeller from Committee on Commerce, Science, and Transportation filed written report. Report No. 111-384.
- **Dec 17, 2010:** Committee on Commerce, Science, and Transportation. Reported by Senator Rockefeller with an amendment in the nature of a substitute. Without written report.
- **Dec 17, 2010:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 707.
- **Mar 24, 2010:** Committee on Commerce, Science, and Transportation. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Apr 1, 2009:** Introduced in Senate
- **Apr 1, 2009:** Read twice and referred to the Committee on Commerce, Science, and Transportation.