HR 3696

National Cybersecurity and Critical Infrastructure Protection Act of 2014

Congress: 113 (2013–2015, Ended)
Chamber: House
Policy Area: Science, Technology, Communications
Introduced: Dec 11, 2013
Current Status: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governm
Latest Action: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Jul 29, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/house-bill/3696

Sponsor

Name: Rep. McCaul, Michael T. [R-TX-10]
Party: Republican • **State:** TX • **Chamber:** House

Cosponsors (3 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Clarke, Yvette D. [D-NY-9]	D · NY		Dec 11, 2013
Rep. Meehan, Patrick [R-PA-7]	R · PA		Dec 11, 2013
Rep. Thompson, Bennie G. [D-MS-2]	D · MS		Dec 11, 2013

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Jul 29, 2014
Homeland Security Committee	House	Reported by	Jan 15, 2014
Oversight and Government Reform Committee	House	Discharged From	Jul 23, 2014
Science, Space, and Technology Committee	House	Referred to	Jan 8, 2014

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

Bill	Relationship	Last Action
113 HR 3107	Related bill	**Jul 29, 2014:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
113 HR 2962	Related bill	**Sep 6, 2013:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

Summary (as of Jul 28, 2014)

National Cybersecurity and Critical Infrastructure Protection Act of 2014 - **Title I: Securing the Nation Against Cyber Attack -** (Sec. 102) Amends the Homeland Security Act of 2002 (HSA) to require the Secretary of Homeland Security to conduct cybersecurity activities, including the provision of shared situational awareness among federal entities to enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

Defines “cyber incident” as an incident, or an attempt to cause an incident, that if successful, would: (1) jeopardize the security, integrity, confidentiality, or availability of an information system or network or any information stored on, processed on, or transiting such a system; (2) violate laws or procedures relating to system security, acceptable use policies, or acts of terrorism against such a system or network; or (3) deny access to or degrade, disrupt, or destruct such a system or network or defeat an operations or technical control of such a system or network.

(Sec. 103) Directs the Secretary to coordinate with federal, state, and local governments, national laboratories, critical infrastructure owners and operators, and other cross-sector coordinating entities to: (1) facilitate a national effort to strengthen and maintain critical infrastructure from cyber threats; (2) ensure that Department of Homeland Security (DHS) policies and procedures enable critical infrastructure owners and operators to receive appropriate and timely cyber threat information; (3) seek industry sector-specific expertise to develop voluntary security and resiliency strategies and to ensure that the allocation of federal resources is cost effective and reduces burdens on critical infrastructure owners and operators; (4) upon request, provide risk management assistance to entities and education to critical infrastructure owners and operators; and (5) coordinate a research and development strategy for cybersecurity technologies.

Directs the Secretary: (1) to manage federal efforts to secure federal civilian information systems (excluding national security, Department of Defense [DOD], military, and intelligence community systems) using a risk-based and performance-based approach and, upon request, to support the efforts of critical infrastructure owners and operators to protect against cyber threats; (2) to direct a DHS entity to serve as a federal civilian entity by and among federal, state, and local governments, private entities, and critical infrastructure sectors to share cyber threat information; (3) to promote national awareness and educate the public regarding information system security; (4) upon request, to facilitate cyber incident response and recovery assistance and provide analysis and warnings related to threats to, and vulnerabilities of, critical information systems, crisis and consequence management support, and other remote or on-site technical assistance to federal, state, and local government entities and private entities for cyber incidents affecting critical infrastructure; and (5) to engage with international partners and conduct outreach to educational institutions.

Requires the Secretary to: (1) designate critical infrastructure sectors; and (2) recognize, for each sector, a previously designated Sector Specific Agency (SSA), a Sector Coordinating Council (SCC), and at least one Information Sharing and Analysis Center (ISAC).

Permits to be included as critical infrastructure sectors:

- chemical;
- commercial facilities;
- communications;
- critical manufacturing;
- dams;
- Defense Industrial Base;

emergency services;
- energy;
- financial services;
- food and agriculture;
- government facilities;
- health care and public health;
- information technology;
- nuclear reactors, materials, and waste;
- transportation systems; and
- water and wastewater systems.

Requires SCCs to: (1) be comprised of small, medium, and large critical infrastructure owners and operators, private entities, and representative trade associations; and (2) serve as a self-governing, self-organized, primary policy, planning, and strategic communications entity for coordinating with DHS, SSAs, and ISACs on security and resilience activities and emergency response and recovery efforts.

Prohibits a government entity with regulating authority from being an SCC member. Bars the Secretary from having any role in the determination of SCC membership.

Directs the Secretary to implement procedures for continuous, collaborative, and effective interactions between DHS and critical infrastructure owners and operators.

(Sec. 104) Establishes the National Cybersecurity and Communications Integration Center (NCCIC) as a federal civilian information sharing interface to: (1) provide shared situational awareness to enable real-time, integrated, and operational actions across the federal government; and (2) share cyber threat information among federal, state, and local government entities, ISACs, private entities, and critical infrastructure owners and operators that have information sharing relationships.

Requires the NCCIC to include: (1) at least one ISAC, (2) the Multi-State Information Sharing and Analysis Center to collaborate with state and local governments, (3) the U.S. Computer Emergency Readiness Team, (4) the Industrial Control System Cyber Emergency Response Team, and (5) the National Coordinating Center for Telecommunications.

Requires the NCCIC to: (1) promote ongoing multi-directional sharing among entities and provide technical assistance as well as crisis management support; (2) identify requirements for data and information formats and accessibility, system interoperability, redundant systems, and alternative capabilities in the event of a disruption in NCCIC's primary information sharing mechanisms; (3) cooperate with international partners to share information and respond to cyber incidents; (4) safeguard sensitive cyber threat information from unauthorized disclosure; and (5) participate in appropriate exercises run by the National Exercise Program.

Directs the NCCIC to require other federal civilian agencies to provide NCCIC with: (1) reports and information about cyber incidents, threats, and vulnerabilities affecting federal civilian information systems and critical infrastructure systems; (2) cyber incident detection, analysis, mitigation, and response information; and (3) cyber threat information received by such agencies. Requires the NCCIC, in the event a private vendor product or service of such an agency is implicated, to first notify such private vendor of a vulnerability before further disclosing such information.

Directs the NCCIC to require federal civilian agencies with data breaches involving unauthorized acquisition or access of personally identifiable information to notify: (1) the NCCIC without unreasonable delay after discovery of the breach; and

(2) potential victims without unreasonable delay, based on the risk of harm and consistent with the needs of law enforcement.

Requires the NCCIC to: (1) collaborate with SCCs, ISACs, SSAs, and relevant critical infrastructure sectors on the development of prioritized federal response efforts to support the defense and recovery of critical infrastructure from cyber incidents; and (2) facilitate continuous improvements to the security and resiliency of public safety communications networks.

Directs the Secretary to report annually to Congress and the Comptroller General (GAO) regarding: (1) major cyber incidents involving federal civilian agency information systems, including aggregate statistics on the number of breaches, the extent of any personally identifiable information involved, the volume of data exfiltrated, the consequential impact, and the estimated cost of remedies; (2) the capacity of the NCCIC to carry out its cybersecurity mission; (3) DHS's interactions with critical infrastructure sectors, SCCs, and SSAs; and (4) the volume and range of voluntary technical assistance sought and provided by DHS to critical infrastructure owners and operators.

Requires a Comptroller General report on the effectiveness of NCCIC.

(Sec. 105) Requires the Secretary to establish Cyber Incident Response Teams to provide technical assistance and recommendations to federal, state, and local government entities, private entities, and critical infrastructure owners and operators.

Directs the Secretary, in coordination with SCCs, ISACs, and federal, state, and local governments, to develop, regularly update, and exercise a National Cybersecurity Incident Response Plan that: (1) includes emergency response plans associated with cyber threats to critical infrastructure, information systems, or networks; (2) adapts to a changing cyber threat environment; (3) incorporates best practices from exercises, training, and after-action reports; and (4) facilitates coordination between DHS and each critical infrastructure sector.

(Sec. 106) Redesignates the National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection Directorate.

Requires the President, with the advice and consent of the Senate, to appoint: (1) the Under Secretary for Cybersecurity and Infrastructure Protection, (2) the Deputy Under Secretary for Cybersecurity, and (3) the Deputy Under Secretary for Infrastructure Protection.

Requires the Secretary to report to Congress with recommendations for: (1) making the Cybersecurity and Communications Office an operational component of DHS; and (2) restructuring the SAFETY Act Office (the office implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002) within DHS to provide incentives for the development and deployment of anti-terrorism technologies, including the use of third-party registrars to improve the certification process.

Directs the Secretary to report to Congress regarding the effectiveness of DHS's acquisition processes for cybersecurity technologies.

Title II: Public-Private Collaboration on Cybersecurity - (Sec. 201) Directs the National Institute of Standards and Technology (NIST) to facilitate and support the development of a voluntary, industry-led set of standards and processes to reduce cyber risks to critical infrastructure. Prohibits NIST from requiring the use of specific solutions, products, services, or manufacturing or design techniques.

Requires the Secretary to: (1) meet biannually with each SCC, and (2) submit annual reports to Congress on the state of cybersecurity in each sector.

(Sec. 202) Expands liability protections for technology providers under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 to include designated cybersecurity technologies deployed in defense of qualifying cyber incidents, which include: (1) unlawful or unauthorized access incidents; (2) disruption of the integrity, operation, confidentiality, or availability of programmable electronic devices or communication networks; (3) misappropriation, corruption, or disruption of data, assets, information, or intellectual property; and (4) harm inside or outside the United States that results in damages, disruptions, or casualties severely affecting the U.S. population, infrastructure, economy, national morale, or federal, state, local, or tribal government functions.

(Sec. 203) Prohibits this Act from being construed to create or authorize any new regulations or additional federal government regulatory authority.

(Sec. 204) Declares that no additional funds are authorized to be appropriated to carry out this Act.

(Sec. 205) Prohibits this Act from permitting DHS to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

(Sec. 206) Directs the Secretary to determine the feasibility and potential benefit of developing a visiting security researchers program from academia, including cybersecurity scholars at DHS's Centers of Excellence.

(Sec. 207) Directs the Secretary to enter into an agreement with the National Research Council (NRC) to research the future resilience and reliability of the nation's electric power transmission and distribution system. Names such research the "Saving More American Resources Today Study" or "SMART Study."

Requires the NRC to report to the Secretary and Congress regarding its findings.

Title III: Homeland Security Cybersecurity Workforce - (Sec. 301) Amends the HSA to add provisions entitled the Homeland Security Cybersecurity Boots-on-the-Ground Act, which require the Secretary to: (1) develop occupation categories for individuals performing activities in furtherance of DHS's cybersecurity mission, (2) ensure that such categories may be used throughout DHS and are made available to other federal agencies, and (3) conduct an annual assessment of the readiness and capacity of the DHS workforce to meet its cybersecurity mission.

Directs the Secretary to include in such readiness assessment information on which cybersecurity positions are performed by: (1) permanent full time departmental employees (together with demographic information about such employees' race, ethnicity, gender, disability status, and veterans status); (2) individuals employed by independent contractors; and (3) individuals employed by other federal agencies, including the National Security Agency (NSA). Requires the assessment to address vacancies within the supervisory workforce, job training, and recruiting costs.

Directs the Secretary to develop: (1) a workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the DHS cybersecurity workforce, including a multi-phased recruitment plan, a 5-year implementation plan, and a 10-year projection of DHS workforce needs; and (2) a process to verify that employees of independent contractors who serve in DHS cybersecurity positions receive initial and recurrent information security and role-based security training commensurate with assigned responsibilities.

Requires the Secretary to provide Congress with annual updates regarding such strategies, assessments, and training. Requires the Comptroller General to study and report to the Secretary and Congress with respect to such assessments

and strategies.

Directs the Secretary to report to Congress regarding the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for DHS for an agreed-upon period of time.

(Sec. 302) Authorizes the Secretary to exercise personnel authorities (in the same manner as the DOD Secretary exercises authority with respect to civilian intelligence personnel and scholarship programs) to establish positions in the excepted service, appoint individuals, fix pay, and pay retention bonuses if needed to retain essential DHS employees who perform functions relating to the security of federal civilian information systems, critical infrastructure information systems, or related networks. Requires the Secretary to provide an explanation to Congress before announcing a bonus.

Requires the Secretary to provide an annual report to Congress for a specified period regarding the processes used in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by a qualified employee.

Actions Timeline

- **Jul 29, 2014:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
- **Jul 28, 2014:** Mr. McCaul moved to suspend the rules and pass the bill, as amended.
- **Jul 28, 2014:** Considered under suspension of the rules. (consideration: CR H6908-6922)
- **Jul 28, 2014:** DEBATE - The House proceeded with forty minutes of debate on H.R. 3696.
- **Jul 28, 2014:** Passed/agreed to in House: On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote.(text: CR H6909-6915)
- **Jul 28, 2014:** On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote. (text: CR H6909-6915)
- **Jul 28, 2014:** Motion to reconsider laid on the table Agreed to without objection.
- **Jul 23, 2014:** Reported (Amended) by the Committee on Homeland Security. H. Rept. 113-550, Part I.
- **Jul 23, 2014:** Committee on Science, Space, and Technology discharged.
- **Jul 23, 2014:** Committee on Oversight and Government discharged.
- **Jul 23, 2014:** Placed on the Union Calendar, Calendar No. 411.
- **Feb 5, 2014:** Committee Consideration and Mark-up Session Held.
- **Feb 5, 2014:** Ordered to be Reported (Amended) by Voice Vote.
- **Jan 15, 2014:** Subcommittee Consideration and Mark-up Session Held.
- **Jan 15, 2014:** Forwarded by Subcommittee to Full Committee (Amended) by Voice Vote .
- **Jan 8, 2014:** Referred to the Subcommittee on Research and Technology.
- **Jan 7, 2014:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
- **Dec 11, 2013:** Introduced in House
- **Dec 11, 2013:** Referred to the Committee on Homeland Security, and in addition to the Committees on Science, Space, and Technology, and Oversight and Government Reform, 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.