HR 1731

National Cybersecurity Protection Advancement Act of 2015

Congress: 114 (2015–2017, Ended)
Chamber: House
Policy Area: Government Operations and Politics
Introduced: Apr 13, 2015
Current Status: Pursuant to the provisions of H. Res. 212, H.R. 1731 is laid on the table.
Latest Action: Pursuant to the provisions of H. Res. 212, H.R. 1731 is laid on the table. (Apr 23, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/house-bill/1731

Sponsor

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

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Ratcliffe, John [R-TX-4]	R · TX		Apr 13, 2015

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security Committee	House	Reported By	Apr 17, 2015

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
114 HR 1560	Related bill	**Jul 14, 2016:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
114 S 754	Related bill	**Oct 28, 2015:** Held at the desk.
114 HRES 212	Procedurally related	**Apr 22, 2015:** Motion to reconsider laid on the table Agreed to without objection.

Summary (as of Apr 23, 2015)

National Cybersecurity Protection Advancement Act of 2015

(Sec. 2) Amends the Homeland Security Act of 2002 to allow the Department of Homeland Security's (DHS's) national cybersecurity and communications integration center (NCCIC) to include tribal governments, information sharing and analysis centers, and private entities among its non-federal representatives. Expands the composition of the NCCIC to include:

- a collaborator with state and local governments on cybersecurity risks and incidents;
- a U.S. Computer Emergency Readiness Team that coordinates and shares information in a timely manner and provides technical assistance, upon request, to information system owners and operators;
- the Industrial Control System Cyber Emergency Response Team that coordinates with owners and operators of industrial control systems, provides requested training, and remains current on industry adoption of new technologies;
- a National Coordinating Center for Communications that coordinates the protection, response, and recovery of emergency communications; and
- a coordinator of small and medium-sized businesses.

(Sec. 3) Requires the NCCIC to be the lead federal civilian interface for multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, and cybersecurity risks for federal and non-federal entities. Expands the NCCIC's functions to include:

- global cybersecurity with international partners;
- information sharing across critical infrastructure sectors, with state and major urban area fusion centers and with small and medium-sized businesses;
- notification to Congress regarding any significant violations of information retention or disclosure policies;
- notification to non-federal entities of indicators or defensive measures shared in error or in contravention of specified requirements; and
- participation in exercises run by DHS's National Exercise Program.

Excludes from the definition of "cybersecurity risk" violations of consumer terms of service or licensing agreements.

Requires the NCCIC to designate an agency contact for non-federal entities.

Directs the NCCIC to: (1) safeguard cybersecurity information against unauthorized disclosure, and (2) work with the Chief Privacy Officer to follow appropriate privacy procedures.

Requires the Under Secretary for Cybersecurity and Infrastructure Protection (the Under Secretary) to develop capabilities that make use of existing industry standards to advance implementation of automated mechanisms for the timely sharing of indicators and defensive measures to and from the NCCIC and with federal agencies designated as sector specific agencies for critical infrastructure sectors.

Directs the Under Secretary, every six months, to provide Congress with progress reports regarding the development of such capabilities.

Authorizes the NCCIC to enter voluntary information sharing relationships with consenting non-federal entities.

Directs the Under Secretary to develop procedures for coordinating vulnerability disclosures consistent with international standards.

Allows non-federal entities, for cybersecurity purposes, to share with other non-federal entities or the NCCIC any indicators or defensive measures obtained from: (1) their own information systems; or (2) the information systems of other federal or non-federal entities, with written consent. Authorizes non-federal entities (excluding state, local, or tribal governments) to conduct network awareness to scan, identify, acquire, monitor, log, or analyze information, or to operate defensive measures, on the information systems of entities that provide consent.

Requires entities, prior to sharing, to take reasonable efforts to: (1) exclude information that can be used to identify specific persons and that is unrelated to cybersecurity risks or incidents, and (2) safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition.

Directs the Under Secretary to establish and annually review privacy and civil liberties policies governing the receipt, retention, use, and disclosure of cybersecurity information shared with the NCCIC. Provides for such policies to apply only to DHS. Allows the Under Secretary to consult with the National Institute of Standards and Technology on such policies.

Requires the Chief Privacy Officer to:

- monitor implementation of such privacy and civil liberties policies;
- update privacy impact assessments on a regular basis to ensure that all relevant privacy protections are followed;
- work with the Under Secretary to carry out certain notifications to Congress and non-federal entities;
- submit an annual report to Congress regarding the effectiveness of DHS's privacy and civil liberties policies; and
- ensure appropriate sanctions for DHS officers, employees, or agents who intentionally or willfully conduct activities in an unauthorized manner.

Directs the DHS Inspector General to periodically report to Congress with a review of the use of cybersecurity risk information shared with the NCCIC.

Requires the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer to biennially submit a report to Congress that: (1) assesses the privacy and civil liberties impact of DHS's retention, use, and disclosure policies; and (2) recommends methods to minimize or mitigate the impact of sharing indicators and defensive measures.

Prohibits federal entities from using shared indicators or defensive measures to engage in surveillance or other collection activities for the purpose of tracking an individual's personally identifiable information, except for purposes authorized under this section. Bars the federal government from using such information for regulatory purposes.

Provides liability protections to non-federal entities (excluding state, local, or tribal governments) acting in accordance with this section that: (1) conduct network awareness, or (2) share indicators or defensive measures or that fail, in good faith, to act based on such sharing.

Prohibits such liability protections from being construed to apply to willful misconduct.

Establishes a private cause of action that a person may bring against the federal government if a federal agency intentionally or willfully violates restrictions on the use and protection of voluntarily shared indicators or defensive measures.

Exempts from antitrust laws non-federal entities that, for cybersecurity purposes, share: (1) cyber threat indicators or defensive measures; or (2) assistance relating to the prevention, investigation, or mitigation of cybersecurity risks or incidents. Makes such exemption inapplicable to price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

Prohibits this section from being construed to permit the federal government to require a non-federal entity to provide information to a federal entity.

Requires the Secretary of Homeland Security to: (1) develop procedures for the NCCIC Director to report directly to the Secretary regarding significant cybersecurity risks and incidents, and (2) promote a national awareness effort to educate the general public on the importance of securing information systems.

Directs DHS to report to Congress on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners.

(Sec. 4) Expands the purpose of information sharing and analysis organizations to include responsibilities for disseminating information about cybersecurity risks and incidents.

(Sec. 5) Redesignates DHS's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection. Requires the President to appoint: (1) the Under Secretary, with the advice and consent of the Senate; and (2) the Deputy Under Secretaries for Cybersecurity and for Infrastructure Protection, without the advice and consent of the Senate. Requires the Under Secretary to report to Congress regarding the feasibility of becoming an operational component.

(Sec. 6) Requires the Secretary to regularly update, maintain, and exercise the Cyber Incident Annex to DHS's National Response Framework.

(Sec. 7) Requires the NCCIC to facilitate improvements to the security and resiliency of public safety communications.

Directs the Under Secretary to implement a cybersecurity awareness campaign to disseminate: (1) public service announcements targeted at state, local, and tribal governments, the private sector, academia, and stakeholders in specific audiences, including the elderly, students, small businesses, members of the Armed Forces, and veterans; and (2) vendor and technology-neutral voluntary best practices.

Requires DHS to establish a National Cybersecurity Preparedness Consortium to:

- train state and local first responders and officials to prepare for and respond to cyber attacks,
- develop a curriculum utilizing the DHS-sponsored Community Cyber Security Maturity Model,
- provide technical assistance,
- conduct cybersecurity training and simulation exercises,
- coordinate with the NCCIC to help states and communities develop information sharing programs, and
- coordinate with the National Domestic Preparedness Consortium to incorporate cybersecurity emergency responses into existing state and local emergency management functions.

(Sec. 8) Directs the Under Secretary for Science and Technology to biennially provide to Congress an updated strategic plan to guide the overall direction of federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure. Requires the plan to:

identify critical infrastructure security risks and any associated security technology gaps;
- prioritize technology needs based on gaps, risks, evolving threats, and technology advancements;
- include research, development, and acquisition roadmaps with clearly defined objectives, goals, and measures;
- identify laboratories, facilities, modeling, and simulation capabilities required to support new technologies; and
- identify programmatic initiatives for the rapid advancement and deployment of security technologies for critical infrastructure protection, including public-private partnerships, intragovernment collaboration, university centers of excellence, and national laboratory technology transfers.

(Sec. 9) Requires DHS to report to Congress regarding the feasibility of DHS reducing cybersecurity risks in DHS data centers, including by increasing compartmentalization between systems and providing a mix of security controls between such compartments.

(Sec. 10) Directs the Government Accountability Office (GAO) to report on DHS's implementation of this Act, including any findings regarding increases in sharing at the NCCIC and throughout the United States.

(Sec. 11) Requires the Under Secretary to produce a report on the feasibility of creating a risk-informed prioritization plan should multiple critical infrastructures experience cyber incidents simultaneously.

(Sec. 12) Directs the DHS Inspector General to review operations of the U.S. Computer Emergency Readiness Team and the Industrial Control Systems Cyber Emergency Response Team to assess the capacity to provide technical assistance to non-federal entities and to adequately respond to potential increases in requests for technical assistance.

(Sec. 13) Prohibits this Act from being construed to grant DHS any authority to promulgate regulations or set standards relating to the cybersecurity of non-federal entities (excluding state, local, and tribal governments) that were not in effect on the day before the enactment of this Act.

(Sec. 14) Terminates reporting requirements under this Act seven years after enactment of this Act.

(Sec. 16) Requires DHS to deploy and operate (to make available for use by any federal agency, with or without reimbursement) capabilities to protect federal agency information and information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks involving such systems. Authorizes the DHS Secretary to access, and allows federal agency heads to disclose to the Secretary, information traveling to or from or stored on a federal agency information system, regardless of from where the Secretary accesses such information, notwithstanding any law that would otherwise restrict or prevent federal agency heads from disclosing such information to the Secretary.

Allows a private entity to assist the Secretary in carrying out such activities.

Authorizes the Secretary to retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect federal agency information and information systems from cybersecurity risks, or, with DOJ approval and if disclosure of such information is not otherwise prohibited by law, to law enforcement only to investigate, prosecute, disrupt, or otherwise respond to:

- criminal computer fraud;
- an imminent threat of death or serious bodily harm;
- a serious threat to a minor, including sexual exploitation or threats to physical safety; or
- an attempt or conspiracy to commit any of such offenses.

Provides liability protections to private entities that provide assistance to the Secretary for such purposes.

(Sec. 17) Terminates the provisions of this Act seven years after its enactment.

(Sec. 18) Requires DHS to report to Congress with recommendations to mitigate cybersecurity vulnerabilities for the 10 U.S. ports that are at greatest risk of a cybersecurity incident.

(Sec. 19) Authorizes DHS to consult with sector specific agencies, businesses, and stakeholders to submit to Congress a report on how to align federally funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties while assuring security and resilience of the nation's critical infrastructure.

(Sec. 20) Directs the GAO to assess the impact on privacy and civil liberties limited to the work of the NCCIC.

Actions Timeline

- **Apr 23, 2015:** Considered under the provisions of rule H. Res. 212. (consideration: CR H2423-2426, H2426-2446)
- **Apr 23, 2015:** Previous question shall be considered as ordered except motion to recommit with or without instructions. Debate for both bills shall not exceed one hour. After general debate, both bills shall be considered for amendment under the five-minute rule. All points of order against the bills and amendments are waived. Only amendments printed in the report from the committee on rules are in order.
- **Apr 23, 2015:** House resolved itself into the Committee of the Whole House on the state of the Union pursuant to H. Res. 212 and Rule XVIII.
- **Apr 23, 2015:** The Speaker designated the Honorable Rob Woodall to act as Chairman of the Committee.
- **Apr 23, 2015:** GENERAL DEBATE - The Committee of the Whole proceeded with one hour of general debate on H.R. 1731.
- **Apr 23, 2015:** The Committee of the Whole rose informally to receive a message from the Senate.
- **Apr 23, 2015:** Subsequently, the Committee resumed it's sitting.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the McCaul part B amendment No. 1.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Ratcliffe part B amendment No. 2.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Langevin part B amendment No. 3.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Jackson Lee part B amendment no. 4.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Castro(TX) part B amendment no. 5.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Castro(TX) part B amendment no. 6.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Hurd part B amendment no. 7.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Mulvaney(SC) part B amendment No. 8.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Hahn part B amendment No. 9.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Jackson Lee part B amendment No. 10.
- **Apr 23, 2015:** POSTPONED PROCEEDINGS - At the conclusion of debate on the Jackson Lee part B amendment No. 10, the Chair put the question on adoption of the amendment and by voice vote, announced that the ayes had prevailed. Mr. McCaul demanded a recorded vote and the Chair postponed further proceedings on the question of adoption of the amendment until a time to be announced.
- **Apr 23, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Jackson Lee part B amendment No. 11.
- **Apr 23, 2015:** The House rose from the Committee of the Whole House on the state of the Union to report H.R. 1731.
- **Apr 23, 2015:** The previous question was ordered pursuant to the rule. (consideration: CR H2443)
- **Apr 23, 2015:** The House adopted the amendment in the nature of a substitute as agreed to by the Committee of the Whole House on the state of the Union. (text of amendment in the nature of a substitue: CR H2428-2433)
- **Apr 23, 2015:** Mr. Israel moved to recommit with instructions to the Committee on Homeland Security. (consideration: CR H2443-2445; text: CR H2443-2444)
- **Apr 23, 2015:** DEBATE - The House proceeded with 10 minutes of debate on the Israel motion to recommit H.R. 1731 with instructions, pending reservation of a point of order. The instructions contained in the motion seek to require the bill to be reported back to the House with an amendment to require the Secretary of Homeland Security to prioritize the sharing of cyber threat indicators and defensive measures in the following areas: (1) the security of critical infrastructure, including the electrical grid, nuclear power plants, oil and gas pipelines, financial services, and transportation systems; (2) the protection of intellectual property of U.S. corporations, including small and medium sized businesses; and (3) the privacy and property rights of at-risk Americans, including medical records. Subsequently, the reservation of a point of order was withdrawn.
- **Apr 23, 2015:** The previous question on the motion to recommit with instructions was ordered without objection.

(consideration: CR H2444)

- **Apr 23, 2015:** On motion to recommit with instructions Failed by recorded vote: 180 - 238 (Roll no. 172).
- **Apr 23, 2015:** Passed/agreed to in House: On passage Passed by recorded vote: 355 - 63 (Roll no. 173).
- **Apr 23, 2015:** On passage Passed by recorded vote: 355 - 63 (Roll no. 173).
- **Apr 23, 2015:** Motion to reconsider laid on the table Agreed to without objection.
- **Apr 23, 2015:** ENGROSSMENT INSTRUCTION - Pursuant to the provisions of H. Res. 212, in the engrossment of H.R. 1560, the text of H.R. 1731 as passed by the House is appended to the end of H.R. 1560 as new matter.
- **Apr 23, 2015:** Pursuant to the provisions of H. Res. 212, H.R. 1731 is laid on the table.
- **Apr 22, 2015:** Rule H. Res. 212 passed House.
- **Apr 21, 2015:** Rules Committee Resolution H. Res. 212 Reported to House. Previous question shall be considered as ordered except motion to recommit with or without instructions. Debate for both bills shall not exceed one hour. After general debate, both bills shall be considered for amendment under the five-minute rule. All points of order against the bills and amendments are waived. Only amendments printed in the report from the committee on rules are in order.
- **Apr 17, 2015:** Reported (Amended) by the Committee on Homeland Security. H. Rept. 114-83.
- **Apr 17, 2015:** Placed on the Union Calendar, Calendar No. 61.
- **Apr 14, 2015:** Committee Consideration and Mark-up Session Held.
- **Apr 14, 2015:** Ordered to be Reported (Amended) by Voice Vote.
- **Apr 13, 2015:** Introduced in House
- **Apr 13, 2015:** Referred to the House Committee on Homeland Security.