HR 624

Cyber Intelligence Sharing and Protection Act

Congress: 113 (2013–2015, Ended)

Chamber: House

Policy Area: Armed Forces and National Security

Introduced: Feb 13, 2013

Current Status: Received in the Senate and Read twice and referred to the Select Committee on Intelligence.

Latest Action: Received in the Senate and Read twice and referred to the Select Committee on Intelligence. (Apr 22, 2013)

Official Text: https://www.congress.gov/bill/113th-congress/house-bill/624

Sponsor

Name: Rep. Rogers, Mike J. [R-MI-8]

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

Cosponsors (37 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Ruppersberger, C. A. Dutch [D-MD-2]	D · MD		Feb 13, 2013
Rep. Amodei, Mark E. [R-NV-2]	R · NV		Apr 15, 2013
Rep. Camp, Dave [R-MI-4]	R · MI		Apr 15, 2013
Rep. Cole, Tom [R-OK-4]	R · OK		Apr 15, 2013
Rep. Conaway, K. Michael [R-TX-11]	R · TX		Apr 15, 2013
Rep. Costa, Jim [D-CA-16]	D · CA		Apr 15, 2013
Rep. Cuellar, Henry [D-TX-28]	D · TX		Apr 15, 2013
Rep. Enyart, William L. [D-IL-12]	D · IL		Apr 15, 2013
Rep. Griffin, Tim [R-AR-2]	R · AR		Apr 15, 2013
Rep. Guthrie, Brett [R-KY-2]	R · KY		Apr 15, 2013
Rep. Gutierrez, Luis V. [D-IL-4]	D · IL		Apr 15, 2013
Rep. Hastings, Alcee L. [D-FL-20]	D · FL		Apr 15, 2013
Rep. Hastings, Doc [R-WA-4]	R · WA		Apr 15, 2013
Rep. Heck, Joseph J. [R-NV-3]	R · NV		Apr 15, 2013
Rep. Kilmer, Derek [D-WA-6]	D · WA		Apr 15, 2013
Rep. King, Peter T. [R-NY-2]	R · NY		Apr 15, 2013
Rep. Kinzinger, Adam [R-IL-16]	R · IL		Apr 15, 2013
Rep. Kline, John [R-MN-2]	R · MN		Apr 15, 2013
Rep. Lance, Leonard [R-NJ-7]	R · NJ		Apr 15, 2013
Rep. Lipinski, Daniel [D-IL-3]	D · IL		Apr 15, 2013
Rep. LoBiondo, Frank A. [R-NJ-2]	R · NJ		Apr 15, 2013
Rep. McCaul, Michael T. [R-TX-10]	R · TX		Apr 15, 2013
Rep. McHenry, Patrick T. [R-NC-10]	R · NC		Apr 15, 2013
Rep. Miller, Candice S. [R-MI-10]	R · MI		Apr 15, 2013
Rep. Mulvaney, Mick [R-SC-5]	R · SC		Apr 15, 2013
Rep. Nunes, Devin [R-CA-22]	R · CA		Apr 15, 2013
Rep. Peters, Scott H. [D-CA-52]	D · CA		Apr 15, 2013
Rep. Pompeo, Mike [R-KS-4]	R · KS		Apr 15, 2013
Rep. Schock, Aaron [R-IL-18]	R · IL		Apr 15, 2013
Rep. Sewell, Terri A. [D-AL-7]	D · AL		Apr 15, 2013
Rep. Sinema, Kyrsten [D-AZ-9]	D · AZ		Apr 15, 2013
Rep. Stivers, Steve [R-OH-15]	R · OH		Apr 15, 2013
Rep. Thornberry, Mac [R-TX-13]	R · TX		Apr 15, 2013
Rep. Upton, Fred [R-MI-6]	R · MI		Apr 15, 2013
Rep. Vargas, Juan [D-CA-51]	D · CA		Apr 15, 2013
Rep. Walden, Greg [R-OR-2]	R · OR		Apr 15, 2013
Rep. Westmoreland, Lynn A. [R-GA-3]	R · GA		Apr 15, 2013

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security Committee	House	Bills of Interest - Exchange of Letters	Aug 1, 2014
Intelligence (Permanent Select) Committee	House	Reported By	Apr 15, 2013
Intelligence (Select) Committee	Senate	Referred To	Apr 22, 2013

Subjects & Policy Tags

Policy Area:

Armed Forces and National Security

Related Bills

Bill	Relationship	Last Action
113 HRES 164	Procedurally related	**Apr 17, 2013:** Motion to reconsider laid on the table Agreed to without objection.

Summary   (as of Apr 18, 2013)

Cyber Intelligence Sharing and Protection Act - (Sec. 2) Directs the federal government to conduct cybersecurity activities to provide shared situational awareness enabling integrated operational actions to protect, prevent, mitigate, respond to, and recover from cyber incidents.

Defines "shared situational awareness" as an environment where cyber threat information is shared in real time between all designated federal cyber operations centers to provide actionable information about all known cyber threats.

Directs the President, with respect to information shared by a cybersecurity provider (a non-federal entity that provides goods or services intended to be used for cybersecurity purposes) or self-protected entity (an entity that provides goods or services for cybersecurity purposes to itself), to designate: (1) an entity within the Department of Homeland Security (DHS) as the civilian federal entity to receive cyber threat information under prescribed procedures and subject to specified exceptions, and (2) an entity within the Department of Justice (DOJ) as the civilian federal entity to receive information related to cybersecurity crimes.

Requires federal agencies receiving shared cyber threat information to establish procedures to: (1) ensure that specified information is also shared in real time with appropriate federal agencies with a national security mission; (2) ensure real-time information distribution to other federal agencies; and (3) facilitate information sharing, interaction, and collaboration among and between federal, state, local, tribal, and territorial governments, cybersecurity providers, and self-protected entities.

Directs the DHS, Attorney General, Director of National Intelligence (DNI), and Department of Defense (DOD) to jointly establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the federal government. Requires such procedures, consistent with the need to protect against and mitigate cyber threats in a timely manner, to: (1) minimize the impact on privacy and civil liberties; (2) reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is unnecessary to protect against or mitigate cyber threats in a timely manner; (3) include requirements to safeguard non-publicly available cyber threat information that may be used to identify specific persons from unauthorized access or acquisition; (4) protect the confidentiality of cyber threat information associated with specific persons; and (5) not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

Instructs: (1) the DHS, Attorney General, DNI, and DOD to submit such procedures to Congress and establish a program to monitor and oversee the compliance of federal agencies; and (2) federal agencies to implement such procedures and notify such officials and Congress of any significant violations.

Prohibits such procedures from being construed to prohibit any federal agency from engaging in technical discussions regarding cyber threat information with a cybersecurity provider or self-protected entity or from providing technical assistance to address vulnerabilities or mitigate threats at their request. Requires any such activity to be coordinated with DHS and other agencies.

Directs the President's designated DHS entity to share with all appropriate federal agencies all significant information resulting from: (1) technical discussions with a cybersecurity provider or self-protected entity about cyber threat information, or (2) any technical assistance it provides to such cybersecurity provider or such self-protected entity to address vulnerabilities or mitigate threats.

Directs the DHS Inspector General to submit annually to Congress a review of the use of such information shared with

the federal government, as well as recommendations for improvements and modifications to address privacy and civil liberties concerns.

Requires the DHS Officer for Civil Rights and Civil Liberties to submit to Congress an annual report assessing the privacy and civil liberties impact of the federal government's cyber threat information sharing activities.

(Sec. 3) Amends the National Security Act of 1947 to add provisions concerning cyber threat intelligence and information sharing. Defines "cyber threat intelligence" as intelligence in the possession of an element of the intelligence community directly pertaining to: (1) a vulnerability of a system or network of a government or private entity or utility; (2) a threat to the integrity, confidentiality, or availability of such a system or network or any information stored on, processed on, or transiting such a system or network; (3) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or (4) efforts to gain unauthorized access to such a system or network, including for the purpose of exfiltrating information. Excludes intelligence pertaining to efforts to gain unauthorized access to such a system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Requires the DNI to: (1) establish procedures to allow intelligence community elements to share cyber threat intelligence with private-sector entities and utilities, and (2) encourage the sharing of such intelligence.

Requires the procedures established to ensure that such intelligence is only: (1) shared with certified entities or a person with an appropriate security clearance; (2) shared consistent with the need to protect U.S. national security; (3) used in a manner that protects such intelligence from unauthorized disclosure; and (4) used, retained, or further disclosed by a certified entity for cybersecurity purposes. Provides guidelines for the granting of security clearance approvals to certified entities or officers, employees, or independent contractors of such entities. Prohibits a certified entity receiving such intelligence from further disclosing the information to any entity other than another certified entity or a federal agency authorized to receive such intelligence.

Authorizes a cybersecurity provider, with the express consent of a protected entity (an entity that contracts with a cybersecurity provider), to: (1) use cybersecurity systems to identify and obtain cyber threat information in order to protect the rights and property of the protected entity; and (2) share cyber threat information with any other entity designated by the protected entity, including, if specifically designated, the DHS and DOJ entities designated by the President. Provides cybersecurity system use and threat information sharing authority to self-protected entities.

Sets forth requirements with respect to the use and protection of shared information, including anonymization or minimization of such information and prohibiting the use of such information to gain a competitive advantage and, if shared with the federal government, exempts such information from public disclosure and prohibits the use of such information for regulatory purposes. Specifies that a non-federal recipient may only use such information for a cybersecurity purpose.

Prohibits a civil or criminal cause of action against a protected entity, a self-protected entity, or a cybersecurity provider acting in good faith under the above circumstances.

Prohibits such shared information requirements from being construed to provide new authority to: (1) a cybersecurity provider to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, or (2) a self-protected entity to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by such self-protected

entity.

Allows the federal government to use shared cyber threat information for: (1) cybersecurity purposes to ensure the integrity, confidentiality, availability, or safeguarding of a system or network; (2) the investigation of cybersecurity crimes; or (3) the protection of individuals from the danger of death or serious bodily harm and the prosecution of crimes involving such dangers (including the protection of minors from child pornography, sexual exploitation, kidnapping, and trafficking). Prohibits the federal government from affirmatively searching such information for any other purpose.

Prohibits the federal government from using certain personally identifiable information shared from sensitive personal documents such as library records, firearms sales records, educational records, tax returns, and medical records. Requires a federal agency receiving information that is not cyber threat information to so notify the entity or provider of such information. Prohibits federal agencies from retaining shared information for any unauthorized use.

Outlines federal government liability for violations of restrictions on the disclosure, use, and protection of voluntarily shared information.

Preempts any state statute that restricts or otherwise regulates specified activity authorized by this Act.

States that nothing in this section shall be construed to: (1) provide additional authority to, or modify existing authority of, any element of the intelligence community to control or direct the cybersecurity efforts of a private-sector entity or a component of the federal government or a state, local, or tribal government; (2) limit or affect existing information sharing relationships of the federal government; (3) preclude the federal government from requiring an entity to report significant cyber incidents under another provision of law; or (4) provide additional authority to, or modify existing authority of, any entity to use a cybersecurity system owned or controlled by the federal government on a private-sector system or network to protect the latter system or network.

Prohibits this section from being construed to authorize the DOD, National Security Agency (NSA), or any other intelligence community element to target a U.S. person for surveillance.

(Sec. 4) Repeals amendments made by this Act five years after enactment of this Act.

(Sec. 5) Expresses the sense of Congress that international cooperation with regard to cybersecurity should be encouraged wherever possible.

(Sec. 6) Prohibits this Act from being construed to provide new or alter any existing authority for an entity to sell personal information of a consumer to another entity for marketing purposes.

(Sec. 7) Prohibits this Act from being construed to authorize a federal agency to require a federally contracted cybersecurity provider to provide information about cybersecurity incidents that do not pose a threat to the federal government's information.

Actions Timeline

- **Apr 22, 2013:** Received in the Senate and Read twice and referred to the Select Committee on Intelligence.
- **Apr 18, 2013:** ORDER OF PROCEDURE - Mr. Sessions asked unanimous consent that, during further consideration of H.R. 624 in the Committee of the Whole and pursuant to the provisions of H.Res. 164, amendment numbered 13 offered by Mr. McCaul of Texas be modified in the form that was placed at the desk. Agreed to without objection.
- **Apr 18, 2013:** Considered as unfinished business. (consideration: CR H2130-2139)
- **Apr 18, 2013:** DEBATE - Pursuant to the provisions of H.Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Sinema amendment No. 7.
- **Apr 18, 2013:** POSTPONED PROCEEDINGS - At the conclusion of debate on the Sinema amendment, the Chair put the question on adoption of the amendment and by voice vote announced that the ayes had prevailed. Ms. Sinema demanded a recorded vote and the Chair postponed further proceedings on the question of adoption of the amendment until later in the legislative day.
- **Apr 18, 2013:** DEBATE - Pursuant to the provisions of H.Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Loretta Sanchez amendment No. 8.
- **Apr 18, 2013:** DEBATE - Pursuant to the provisions of H.Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the LaMalfa amendment No. 9.
- **Apr 18, 2013:** POSTPONED PROCEEDINGS - At the conclusion of debate on the LaMalfa amendment, the Chair put the question on adoption of the amendment and by voice vote announced that the ayes had prevailed. Mr. Rogers (MI) demanded a recorded vote and the Chair postponed further proceedings on the question of adoption of the amendment until later in the legislative day.
- **Apr 18, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Paulsen amendment No. 10.
- **Apr 18, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Barton amendment No. 11.
- **Apr 18, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Jackson Lee amendment No. 12.
- **Apr 18, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the McCaul amendment No. 13.
- **Apr 18, 2013:** POSTPONED PROCEEDINGS - At the conclusion of debate on the McCaul amendment, 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 later in the legislative day.
- **Apr 18, 2013:** Mr. Rogers (MI) moved that the Committee rise.
- **Apr 18, 2013:** On motion that the Committee rise Agreed to by voice vote.
- **Apr 18, 2013:** Committee of the Whole House on the state of the Union rises leaving H.R. 624 as unfinished business.
- **Apr 18, 2013:** Considered as unfinished business. (consideration: CR H2140-2145)
- **Apr 18, 2013:** The House resolved into Committee of the Whole House on the state of the Union for further consideration.
- **Apr 18, 2013:** UNFINISHED BUSINESS - The Chair announced that the unfinished business was on the adoption of amendments which had been debated earlier and on which further proceedings had been postponed.
- **Apr 18, 2013:** The House rose from the Committee of the Whole House on the state of the Union to report H.R. 624.
- **Apr 18, 2013:** The previous question was ordered pursuant to the rule. (consideration: CR H2142)
- **Apr 18, 2013:** 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.
- **Apr 18, 2013:** Mr. Perlmutter moved to recommit with instructions to Intelligence (Permanent). (consideration: CR H2142; text: CR H2142)
- **Apr 18, 2013:** DEBATE - The House proceeded with 10 minutes of debate on the Perlmutter motion to recommit with instructions. The instructions contained in the motion seek to require the bill to be reported back to the House with an amendment to prohibit employers, prospective employers, or the Federal Government from requiring the disclosure of social networking or personal account passwords by an employee or job applicant without a court order. The Motion would also prohibit the Federal Government from establishing a mechanism by which it could control citizen's access to the Internet with a national firewall similar to the "Great Internet Firewall of China." Lastly, the Motion would make changes to the McCaul amendment, adding a section that requires reporting of information on the number of Americans who have been forced to disclose passwords and had information released to the Federal government or

obtained in connection

- **Apr 18, 2013:** The previous question on the motion to recommit with instructions was ordered without objection. (consideration: CR H2143)
- **Apr 18, 2013:** On motion to recommit with instructions Failed by recorded vote: 189 - 224 (Roll no. 116). (consideration: CR H2143-2144)
- **Apr 18, 2013:** Passed/agreed to in House: On passage Passed by the Yeas and Nays: 288 - 127 (Roll no. 117).
- **Apr 18, 2013:** On passage Passed by the Yeas and Nays: 288 - 127 (Roll no. 117).
- **Apr 18, 2013:** Motion to reconsider laid on the table Agreed to without objection.
- **Apr 18, 2013:** The Clerk was authorized to correct section numbers, punctuation, and cross references, and to make other necessary technical and conforming corrections in the engrossment of H.R. 624.
- **Apr 17, 2013:** Rule H. Res. 164 passed House.
- **Apr 17, 2013:** Considered under the provisions of rule H. Res. 164. (consideration: CR H2088-2103; text of amendment in the nature of a substitute: CR H2097-2100)
- **Apr 17, 2013:** Rule provides for consideration of H.R. 624 with 1 hour of general debate. Previous question shall be considered as ordered without intervening motions except motion to recommit with or without instructions. Measure will be considered read. Specified amendments are in order.
- **Apr 17, 2013:** House resolved itself into the Committee of the Whole House on the state of the Union pursuant to H. Res. 164 and Rule XVIII.
- **Apr 17, 2013:** The Speaker designated the Honorable Ileana Ros-Lehtinen to act as Chairwoman of the Committee.
- **Apr 17, 2013:** GENERAL DEBATE - The Committee of the Whole proceeded with one hour of general debate on H.R. 624.
- **Apr 17, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Rogers (MI) amendment No. 1.
- **Apr 17, 2013:** POSTPONED PROCEEDINGS - At the conclusion of debate on the Rogers (MI) amendment, the Chair put the question on adoption of the amendment and by voice vote announced that the ayes had prevailed. Mr. Rogers (MI) demanded a recorded vote and the Chair postponed further proceedings on the question of adoption of the amendment until later in the legislative day.
- **Apr 17, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Connolly amendment No. 2.
- **Apr 17, 2013:** POSTPONED PROCEEDINGS - At the conclusion of debate on the Connolly amendment, the Chair put the question on adoption of the amendment and by voice vote announced that the ayes had prevailed. Mr. Rogers (MI) demanded a recorded vote and the Chair postponed further proceedings on the question of adoption of the amendment until later in the legislative day.
- **Apr 17, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Schneider amendment No. 3.
- **Apr 17, 2013:** DEBATE - Pursuant to the provisions of H. Res. 164, the Committee of the Whole proceeded with 10 minutes of debate on the Langevin amendment No. 4.
- **Apr 17, 2013:** POSTPONED PROCEEDINGS - At the conclusion of debate on the Langevin amendment, the Chair put the question on adoption of the amendment and by voice vote announced that the ayes had prevailed. Mr. Rogers (MI) demanded a recorded vote and the Chair postponed further proceedings on the question of adoption of the amendment until later in the legislative day.
- **Apr 17, 2013:** Mr. Rogers (MI) moved that the Committee rise.
- **Apr 17, 2013:** Considered as unfinished business. (consideration: CR H2103-2105)
- **Apr 17, 2013:** The House resolved into Committee of the Whole House on the state of the Union for further consideration.
- **Apr 17, 2013:** UNFINISHED BUSINESS - The Chair announced that the unfinished business was on adoption of amendments which had been debated and on which further proceedings had been postponed.
- **Apr 17, 2013:** Mr. Sessions moved that the Committee rise.
- **Apr 17, 2013:** On motion that the Committee rise Agreed to by voice vote.
- **Apr 17, 2013:** Committee of the Whole House on the state of the Union rises leaving H.R. 624 as unfinished business.
- **Apr 16, 2013:** Rules Committee Resolution H. Res. 164 Reported to House. Rule provides for consideration of H.R. 624 with 1 hour of general debate. Previous question shall be considered as ordered without intervening motions except motion to recommit with or without instructions. Measure will be considered read. Specified amendments are in order.
- **Apr 15, 2013:** Reported (Amended) by the Committee on Intelligence. H. Rept. 113-39.

Apr 15, 2013: Placed on the Union Calendar, Calendar No. 25.

- **Feb 13, 2013:** Introduced in House
- **Feb 13, 2013:** Referred to the House Committee on Intelligence (Permanent Select).