HR 1560

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, and for other purposes.

Congress: 114 (2015–2017, Ended)
Chamber: House
Policy Area: Armed Forces and National Security
Introduced: Mar 24, 2015
Current Status: Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
Latest Action: Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Jul 14, 2016)
Official Text: https://www.congress.gov/bill/114th-congress/house-bill/1560

Sponsor

Name: Rep. Nunes, Devin [R-CA-22]
Party: Republican • **State:** CA • **Chamber:** House

Cosponsors (8 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Himes, James A. [D-CT-4]	D · CT		Mar 24, 2015
Rep. Schiff, Adam B. [D-CA-28]	D · CA		Mar 24, 2015
Rep. Westmoreland, Lynn A. [R-GA-3]	R · GA		Mar 24, 2015
Rep. King, Peter T. [R-NY-2]	R · NY		Mar 25, 2015
Rep. LoBiondo, Frank A. [R-NJ-2]	R · NJ		Mar 25, 2015
Rep. Murphy, Patrick [D-FL-18]	D · FL		Mar 25, 2015
Rep. Quigley, Mike [D-IL-5]	D · IL		Mar 25, 2015
Rep. Sewell, Terri A. [D-AL-7]	D · AL		Mar 25, 2015

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Jul 14, 2016
Intelligence (Permanent Select) Committee	House	Reported By	Apr 13, 2015

Subjects & Policy Tags

Policy Area:

Armed Forces and National Security

Related Bills

Bill	Relationship	Last Action
114 S 754	Related bill	**Oct 28, 2015:** Held at the desk.
114 HR 3305	Related bill	**Aug 11, 2015:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
114 HR 1731	Related bill	**Apr 23, 2015:** Pursuant to the provisions of H. Res. 212, H.R. 1731 is laid on the table.
114 HRES 212	Procedurally related	**Apr 22, 2015:** Motion to reconsider laid on the table Agreed to without objection.

Summary (as of Apr 22, 2015)

TITLE I--PROTECTING CYBER NETWORKS ACT

Protecting Cyber Networks Act

(Sec. 102) Amends the National Security Act of 1947 to require the Director of National Intelligence (DNI) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal, or local governments; and (2) the sharing of imminent or ongoing cybersecurity threats with such entities to prevent or mitigate adverse impacts.

Requires the procedures to provide for: (1) notification to entities when the federal government has shared indicators in error or in contravention of law; and (2) the federal government, prior to sharing indicators, to remove personal information of, or information identifying, a specific person not directly related to a cybersecurity threat.

Directs the DNI to submit such procedures to Congress within 90 days after enactment of this title.

(Sec. 103) Permits private entities to monitor or operate defensive measures to prevent or mitigate cybersecurity threats or security vulnerabilities, or to identify the source of a threat, on: (1) their own information systems; and (2) with written authorization, the information systems of other private or government entities. Authorizes entities to conduct such activities on information that is stored on, processed by, or transiting such monitored systems.

Prohibits defensive measures from being used to destroy, render unusable or inaccessible, or substantially harm an information system that is not owned by: (1) the operator of the defensive measure, or (2) an entity that authorizes the operation of defensive measures on its systems.

Allows non-federal entities to share and receive indicators or defensive measures with other non-federal entities or specifically designated federal entities, but does not authorize non-federal entities to share directly with components of the Department of Defense (DOD), including the National Security Agency (NSA). Allows otherwise lawful sharing by non-federal entities of indicators or defensive measures with DOD or the NSA. Requires recipients to comply with lawful restrictions that sharing entities place on the sharing or use of shared indicators or defensive measures.

Requires non-federal entities monitoring, operating, or sharing indicators or defensive measures: (1) to implement security controls to protect against unauthorized access or acquisitions; and (2) prior to sharing an indicator, to take reasonable efforts to remove information that the non-federal entity reasonably believes to be personal information of, or information identifying, a specific person not directly related to a cybersecurity threat.

Permits state, tribal, or local agencies to use shared indicators or defensive measures:

- to protect (including through the use of a defensive measure) an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability or to identify the source of a cybersecurity threat;
- to respond to, prosecute, prevent, or mitigate a threat of death or serious bodily harm or an offense arising out of such a threat; or
- to respond to, prevent, or mitigate a serious threat to a minor, including sexual exploitation and threats to physical safety.

Requires the Small Business Administration (SBA) to provide assistance to small businesses and financial institutions to monitor information systems, operate defensive measures, and share and receive indicators and defensive measures. Directs the SBA to submit to the President a report regarding the degree to which small businesses and financial institutions are able to engage in such sharing. Requires the federal government to conduct outreach to encourage such businesses and institutions to engage in those activities.

(Sec. 104) Directs the President to report on procedures for the receipt of cyber threat indicators and defensive measures by the federal government. Requires the procedures to ensure that: (1) cyber threat indicators shared by a non-federal entity with the Department of Commerce, the Department of Energy, the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Department of the Treasury, and the DNI (but not DOD, including the NSA) are shared in real time with all appropriate federal entities; (2) such indicators are provided to other relevant federal entities; (3) there is an audit capability; and (4) there are appropriate sanctions for federal officers, employees, or agents who use shared indicators or defensive measures in an unauthorized manner.

Requires DOJ to develop and periodically review privacy and civil liberties guidelines to govern the receipt, retention, use, and dissemination of cyber threat indicators by federal entities, including guidelines to ensure that personal information of, or information identifying, specific persons is properly removed from information received, retained, used, or disseminated by a federal entity.

Establishes within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center (CTIIC) to serve as the primary organization within the federal government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to cyber threats. Requires the CTIIC to: (1) ensure that appropriate agencies receive all-source intelligence support to execute cyber threat intelligence activities and perform independent, alternative analyses; (2) disseminate threat analysis to the President, federal agencies, and Congress; and (3) coordinate federal cyber threat intelligence activities and conduct strategic planning.

Requires the head of the CTIIC to be appointed by the DNI.

Authorizes indicators or defensive measures to be disclosed to, retained by, and used by, consistent with otherwise applicable federal law, any agency or agent of the federal government solely for:

- protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability or identifying the source of a cybersecurity threat;
- responding to, investigating, prosecuting, or otherwise preventing or mitigating a threat of death or serious bodily harm or an offense arising out of such a threat;
- responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety; or
- preventing, investigating, disrupting, or prosecuting specified criminal offenses relating to fraud and identity theft, serious violent felonies, espionage and censorship, or trade secrets.

(Sec. 105) Allows a person to bring a private cause of action against the federal government if an agency intentionally or willfully violates DOJ's privacy and civil liberties guidelines.

(Sec. 106) Provides liability protections to: (1) private entities that monitor information systems; or (2) non-federal entities that share, receive, or fail, in good faith, to act upon shared indicators or defensive measures.

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

(Sec. 107) Requires reports to Congress, at least biennially, by: (1) the DNI regarding the implementation of the federal government's information sharing procedures, including assessments of any misuse of information or disciplinary actions taken; and (2) inspectors general of specified agencies regarding the receipt, use, and dissemination of indicators and defensive measures that have been shared with federal entities.

Directs the Privacy and Civil Liberties Oversight Board, every two years, to report to Congress and the President regarding the sufficiency of procedures to address privacy and civil liberties concerns.

(Sec. 108) Directs the DNI, in a report to Congress regarding cyber threats, attacks, theft, and data breaches, to: (1) assess current U.S. intelligence sharing and cooperation relationships with other countries regarding cybersecurity threats to U.S. national security interests, the economy, and intellectual property; (2) list countries and non-state actors that are primary threats; (3) describe U.S. response and prevention capabilities; and (4) assess additional technologies that would enhance U.S. capabilities, including private sector technologies that could be rapidly fielded to assist the intelligence community.

Requires unclassified portions of reports under this title to be made publicly available.

(Sec. 109) Prohibits this title from being construed to: (1) authorize the federal government to conduct surveillance of a person or allow the intelligence community to target a person for surveillance; (2) limit lawful disclosures of communications or records, including reporting of known or suspected criminal activity, by a non-federal entity to another non-federal entity or the federal government; or (3) permit the federal government to require a non-federal entity to provide information to the federal government.

(Sec. 111) Requires the Government Accountability Office (GAO) to report on federal actions to remove personal information from shared cyber threat indicators.

(Sec. 112) Terminates the provisions of this title seven years after its enactment.

TITLE II--NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT

National Cybersecurity Protection Advancement Act of 2015

(Sec. 202) Amends the Homeland Security Act of 2002 to allow 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. 203) 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. 204) Expands the purpose of information sharing and analysis organizations to include responsibilities for disseminating information about cybersecurity risks and incidents.

(Sec. 205) 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. 206) Requires the Secretary to regularly update, maintain, and exercise the Cyber Incident Annex to DHS's National Response Framework.

(Sec. 207) 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. 208) 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. 209) 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. 210) Directs the GAO to report on DHS's implementation of this title, including any findings regarding increases in sharing at the NCCIC and throughout the United States.

(Sec. 211) 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. 212) 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. 213) Prohibits this title 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 title.

(Sec. 214) Terminates reporting requirements under this title seven years after enactment of this title.

(Sec. 216) 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. 217) Terminates the provisions of this title seven years after its enactment.

(Sec. 218) 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. 219) 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. 220) Directs the GAO to assess the impact on privacy and civil liberties limited to the work of the NCCIC.

Actions Timeline

- **Jul 14, 2016:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
- **Apr 27, 2015:** Received in the Senate.
- **Apr 22, 2015:** Considered under the provisions of rule H. Res. 212. (consideration: CR H2381-2398)
- **Apr 22, 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 22, 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 22, 2015:** The Speaker designated the Honorable Kenny Marchant to act as Chairman of the Committee.
- **Apr 22, 2015:** GENERAL DEBATE - The Committee of the Whole proceeded with one hour of general debate on H.R. 1560.
- **Apr 22, 2015:** DEBATE - Pursuant to the provisions of H.Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Nunes part A amendment No. 1.
- **Apr 22, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Cardenas part A amendment No. 2.
- **Apr 22, 2015:** DEBATE - Pursuant to the provisions of H. Res. 212, the Committee of the Whole proceeded with 10 minutes of debate on the Carson(IN) part A amendment No. 3.
- **Apr 22, 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 A amendment No. 4.
- **Apr 22, 2015:** POSTPONED PROCEEDINGS - At the conclusion of debate on the Mulvaney part A amendment No. 4, the Chair put the question on adoption of the amendment and by voice vote, announced that the noes had prevailed. Mr. Mulvaney 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 22, 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 A amendment No. 5.
- **Apr 22, 2015:** The House rose from the Committee of the Whole House on the state of the Union to report H.R. 1560.
- **Apr 22, 2015:** The previous question was ordered pursuant to the rule. (consideration: CR H2396)
- **Apr 22, 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 substitute: CR H2386-2390)
- **Apr 22, 2015:** Miss Rice (NY) moved to recommit with instructions to the Committee on Intelligence (Permanent). (consideration: CR H2396-2397; text: CR H2396)
- **Apr 22, 2015:** DEBATE - The House proceeded with 10 minutes of debate on the 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 prioritize the sharing of cyber threat indicators within the Cyber Threat Intelligence Integration Center.
- **Apr 22, 2015:** The previous question on the motion to recommit with instructions was ordered without objection. (consideration: CR H2397)
- **Apr 22, 2015:** On motion to recommit with instructions Failed by recorded vote: 183 - 239 (Roll no. 169).
- **Apr 22, 2015:** Passed/agreed to in House: On passage Passed by recorded vote: 307 - 116 (Roll no. 170).
- **Apr 22, 2015:** On passage Passed by recorded vote: 307 - 116 (Roll no. 170).
- **Apr 22, 2015:** Motion to reconsider laid on the table Agreed to without objection.
- **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 13, 2015:** Reported (Amended) by the Committee on Intelligence. H. Rept. 114-63.
- **Apr 13, 2015:** Placed on the Union Calendar, Calendar No. 44.
- **Mar 26, 2015:** Committee Consideration and Mark-up Session Held.
- **Mar 26, 2015:** Ordered to be Reported (Amended) by Voice Vote.
- **Mar 24, 2015:** Introduced in House
- **Mar 24, 2015:** Referred to the House Committee on Intelligence (Permanent Select).