S 754

An act to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Congress: 114 (2015–2017, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Mar 17, 2015
Current Status: Held at the desk.
Latest Action: Held at the desk. (Oct 28, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/senate-bill/754

Sponsor

Name: Sen. Burr, Richard [R-NC]
Party: Republican • **State:** NC • **Chamber:** Senate

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Intelligence (Select) Committee	Senate	Reported Original Measure	Mar 17, 2015

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
114 S 1869	Related bill	**Nov 17, 2016:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 673.
114 HR 1560	Related bill	**Jul 14, 2016:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
114 HR 2029	Related bill	**Dec 18, 2015:** Became Public Law No: 114-113.
114 HR 1584	Related bill	**Dec 2, 2015:** Ordered to be Reported by Voice Vote.
114 HR 3873	Related bill	**Nov 2, 2015:** Referred to the House Committee on Foreign Affairs.
114 S 2007	Related bill	**Aug 6, 2015:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
114 S 1990	Related bill	**Aug 5, 2015:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
114 HR 1731	Related bill	**Apr 23, 2015:** Pursuant to the provisions of H. Res. 212, H.R. 1731 is laid on the table.

Summary (as of Oct 27, 2015)

Highlights:

This bill requires the Director of National Intelligence and the Departments of Homeland Security (DHS), Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threats.

To detect, prevent, or mitigate cybersecurity threats or security vulnerabilities, private entities may monitor and operate defensive measures on: (1) their own information systems; and (2) with written consent, the information systems of other private or government entities.

Liability protections are provided to entities that voluntarily share and receive cyber threat indicators and defensive measures with other entities or the government.

A sharing process must be developed within DHS for the federal government to: (1) receive indicators and defensive measures that are shared by any entity, and (2) ensure that appropriate federal entities receive shared indicators in an automated, real-time manner.

The bill limits the purposes for which the government may use shared information to certain cybersecurity purposes and responses to imminent threats or serious threats to a minor. The crimes that may be prosecuted with such information are restricted to offenses relating to fraud and identity theft, espionage, censorship, trade secrets, or an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or use of a weapon of mass destruction.

DHS must also deploy a system to: (1) detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system, and (2) prevent or modify such traffic to remove cybersecurity risks.

The DHS Secretary may: (1) issue emergency directives to agencies in response to a substantial information security threat, vulnerability, or incident; or (2) authorize intrusion detection and prevention capabilities to secure agency information systems in the case of an imminent threat.

Federal agencies must identify and mitigate skill shortages in federal workforce positions requiring the performance of cybersecurity functions.

The Department of State must develop a diplomacy strategy to obtain agreements on international behavior in cyberspace and consult with countries regarding the prosecution and prevention of cyber or intellectual property crimes.

The National Cybersecurity and Communications Integration Center must establish a process for statewide interoperability coordinators to report risks or incidents involving networks used by emergency response providers.

The Department of Health and Human Services must convene a task force to: (1) plan a single system for the federal government to share intelligence regarding cybersecurity threats to the health care industry, and (2) recommend protections for networked medical devices and electronic health records.

DHS must develop a strategy to ensure that a cyber incident affecting critical infrastructure entities will not result in catastrophic regional or national effects on public health or safety, economic security, or national security.

The bill also allows criminal penalties for fraud involving account access devices to be imposed regardless of whether the

underlying articles, property, or proceeds are held within, or have transferred through, U.S. jurisdiction.

Full Summary:

TITLE I--CYBERSECURITY INFORMATION SHARING

Cybersecurity Information Sharing Act of 2015

(Sec. 103) This title requires the Director of National Intelligence (DNI) and the Departments of Homeland Security (DHS), Defense (DOD), and Justice (DOJ) to develop and promulgate procedures to promote the sharing of: (1) classified and declassified cyber threat indicators in possession of the federal government with private entities, nonfederal government agencies, or state, tribal, or local governments; (2) unclassified indicators with the public; (3) information with entities under cybersecurity threats to prevent or mitigate adverse effects; and (4) cybersecurity best practices with attention to the challenges faced by small businesses.

The procedures must incorporate sector specific information sharing and analysis centers and other existing processes of federal and nonfederal entities for information sharing by the federal government. The procedures must also include a process for timely notifications to: (1) recipients of threat indicators from federal entities when the federal government has shared indicators in error or in contravention of law, and (2) U.S. persons whose personal information has been shared by the federal government in violation of this Act. The DNI must submit such procedures to Congress within 60 days after enactment of this Act.

(Sec. 104) To detect, prevent, or mitigate cybersecurity threats or security vulnerabilities, private entities may monitor and operate defensive measures on: (1) their own information systems; and (2) with authorization and written consent, the information systems of other private or government entities.

A "defensive measure" is an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on or processed by, or that is transiting, an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. Defensive measures do not include measures that destroy, render unusable, provide unauthorized access to, or substantially harm an information system or data not belonging to: (1) the private entity operating the measure, or (2) another entity that is authorized to provide, and has provided, consent to that private entity for operation of such measure.

The term "private entity" includes state, tribal, or local governments performing electric or other utility services but excludes foreign powers under the Foreign Intelligence Surveillance Act of 1978.

Entities may share and receive indicators and defensive measures with other entities or the federal government for a cybersecurity purpose. Recipients must comply with lawful restrictions that sharing entities place on the sharing or use of shared indicators or defensive measures.

The federal government and entities monitoring, operating, or sharing indicators or defensive measures must: (1) utilize security controls to protect against unauthorized access or acquisitions, and (2) remove personal information, or information that identifies a specific person not directly related to a cybersecurity threat, prior to sharing an indicator.

State, tribal, or local agencies may use shared indicators (with the consent of the entity sharing the indicators) to prevent, investigate, or prosecute offenses relating to: (1) an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or use of a weapon of mass destruction; or (2) crimes involving fraud and identity theft,

espionage and censorship, or trade secrets.

This title exempts from antitrust laws private entities that, for cybersecurity purposes, exchange or provide: (1) cyber threat indicators; or (2) assistance relating to the prevention, investigation, or mitigation of cybersecurity threats. The exemption is inapplicable to price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(Sec. 105) DOJ and DHS must promulgate procedures relating to the receipt of indicators and defensive measures by the federal government. The procedures must include automated real-time sharing procedures, an audit capability, and appropriate sanctions for federal officers, employees, or agents who conduct unauthorized activities.

DOJ and DHS must also develop, and make publicly available, guidelines to assist entities in sharing indicators with the federal government, including guidance for identifying and protecting personal information.

DOJ must promulgate, and review at least every two years, privacy and civil liberties guidelines to limit receipt, retention, use, and dissemination of personal or identifying information. The guidelines must include steps to make dissemination of cyber threat indicators consistent with the protection of classified and other sensitive national security information.

DHS must develop a process within DHS for the federal government to: (1) accept cyber threat indicators and defensive measures from any entity in real time, and (2) ensure that appropriate federal entities receive the shared indicators in an automated manner through that real-time process. Before the process is implemented, DHS must certify to Congress that the DHS sharing capability is fully operational.

This title requires the DHS capability to be the process by which the federal government receives indicators and defensive measures under this title that are shared by a private entity with the federal government through electronic mail or media, an interactive Internet website form, or a real-time, automated process between information systems, except: (1) communications between a federal entity and a private entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such indicator, and (2) communications by a regulated entity with such entity's federal regulatory authority regarding a cybersecurity threat.

DHS's process is prohibited from limiting lawful disclosures of communications, records, or other information to: (1) report known or suspected criminal activity, (2) participate in a federal investigation voluntarily or upon being legally compelled, or (3) provide indicators or defensive measures as part of a statutory or authorized contractual requirement.

DHS must ensure that there is public notice of, and access to, the DHS sharing procedures.

DHS must report to Congress regarding implementation of the sharing process within DHS.

Cyber threat indicators and defensive measures shared with the federal government and threat indicators shared with state, tribal, or local governments are: (1) deemed voluntarily shared information, and (2) exempt from disclosure and withheld from the public under any laws of such jurisdictions requiring disclosure of information or records.

Consistent with otherwise applicable federal law, indicators and defensive measures may be disclosed to, retained by, and used by any federal agency or federal government agent 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;

identifying a cybersecurity threat, including the source, or a security vulnerability;
- identifying the use of an information system by a foreign adversary or terrorist;
- responding to, or otherwise preventing or mitigating, a serious threat to a minor or an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction; or
- preventing, investigating, disrupting, or prosecuting an offense arising out of an imminent threat of death, serious bodily harm, or serious economic harm, as well as offenses relating to fraud and identity theft, espionage and censorship, or trade secrets.

Indicators and defensive measures provided to the government may not be used by government agencies to regulate the lawful activities of an entity.

(Sec. 106) Liability protections are provided to entities acting in accordance with this title that: (1) monitor information systems; or (2) share or receive indicators or defensive measures, provided that the manner in which an entity shares such indicators or measures with the federal government is consistent with specified procedures and exceptions set forth under the DHS sharing process.

(Sec. 107) The appropriate federal entities and inspectors general must report to Congress at least every two years concerning the implementation of this title. The reports must include:

- whether cyber threat indicators have been properly classified;
- an accounting of the number of security clearances authorized for purposes of this title;
- the type of indicators shared with appropriate federal entities, the number of indicators received through the DHS sharing process, and the number of times shared information was used by a federal entity to prosecute an offense consistent with purposes for which the federal government is authorized to disclose, retain, and use indicators and defensive measures under this title;
- the effect on privacy and civil liberties of specific persons, including the number of notices that were issued for a failure to remove personal information or information that identified a specific person not directly related to a cybersecurity threat;
- actions taken by the federal government based on shared cyber threat indicators, including the appropriateness of any federal entity's subsequent use or dissemination of such cyber threat indicators;
- any significant violations by the federal government; and
- the types of entities that received classified cyber threat indicators from the federal government.

This title also requires reports to Congress, at least every two years, by: (1) the Privacy and Civil Liberties Oversight Board; and (2) inspectors general of DHS, the Intelligence Community, DOJ, DOD, and the Department of Energy regarding shared indicators and defensive measures.

(Sec. 108) Nothing in this title shall be construed to permit a federal entity to require an entity to provide information to a federal entity or another entity.

(Sec. 109) The DNI must report to Congress regarding cybersecurity threats, including cyber attacks, theft, and data breaches. The report must include: (1) an assessment of current U.S. intelligence sharing and cooperation relationships with other countries regarding cybersecurity threats to the U.S. national security interests, economy, and intellectual property; (2) a list of countries and nonstate actors that are primary threats; (3) a description of the U.S. government's response and prevention capabilities; and (4) an assessment of additional technologies that would enhance U.S.

capabilities, including private sector technologies that could be rapidly fielded to assist the intelligence community.

(Sec. 110) The National Defense Authorization Act for Fiscal Year 2013 is amended to authorize DOD to share with other federal entities information reported by a cleared defense contractor regarding a penetration of network or information systems.

TITLE II--FEDERAL CYBERSECURITY ENHANCEMENT

Federal Cybersecurity Enhancement Act of 2015

(Sec. 203) This title amends the Homeland Security Act of 2002 to require DHS, in coordination with the Office of Management and Budget (OMB), to implement an intrusion assessment plan to identify and remove intruders in federal agency information systems.

DHS must deploy, operate, and maintain, for use by other agencies, capabilities to: (1) detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system, and (2) prevent or modify such traffic to remove cybersecurity risks. The DHS Secretary may access, and agency heads may disclose to the Secretary, information transiting agency systems, regardless of the location from which the information is accessed, notwithstanding any laws that would otherwise restrict or prevent such disclosures.

Agencies must utilize such capabilities and adopt subsequent improvements.

DHS must establish a pilot to test and deploy advanced technologies to improve detection and prevention.

DHS must also ensure that: (1) the activities are reasonably necessary to protect agency information and systems from a cybersecurity risk, (2) information accessed by DHS will be retained no longer than reasonably necessary for such purposes, and (3) notice is provided to users of agency information systems concerning access to their communications.

This title provides liability protections to private entities authorized to assist the Secretary with such capabilities. It prohibits the liability protections from being construed to authorize an Internet service provider to break a user agreement with customers without their consent.

DOJ must review the intrusion detection and prevention system for consistency with laws governing acquisition, interception, retention, use, and disclosure of communications.

The authority for such capabilities expires seven years after enactment of this Act.

DOD, national security systems, and the intelligence community are excluded from procedures of this title.

(Sec. 204) DHS must include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity to detect and mitigate intrusions and anomalous activity. The OMB must implement a plan to ensure that agencies utilize such advanced tools.

DHS must collaborate with the OMB to update government information security metrics to include measures of intrusion and incident detection and response times. The OMB must display additional agency metrics on federal government performance websites.

Upon an agency's request, DHS is authorized to operate and maintain technology that is deployed to agencies to diagnose and mitigate against cyber threats and vulnerabilities.

(Sec. 205) DHS must issue binding operational directives to assist the OMB in ensuring timely agency adoption of and compliance with standards for securing agency information systems.

Agencies must: (1) encrypt sensitive and mission critical data or otherwise render such data indecipherable to unauthorized users; (2) implement single sign-on trusted identity platforms for public websites; and (3) implement identity management, including multifactor authentication standards, for remote access to agency systems and user accounts with elevated privileges. Agency information systems are exempted from such cybersecurity requirements if the agency certifies to the OMB and Congress that the agency has taken all steps necessary to secure the agency's systems and that the requirements would be excessively burdensome and unnecessary.

(Sec. 206) The Government Accountability Office (GAO), within three years after enactment of this Act, must report on the effectiveness of the federal government's approach to securing agency information systems.

DHS must report annually to Congress on the implementation status of the intrusion detection and prevention capabilities.

The OMB must submit to Congress: (1) an annual analysis of agency application of the intrusion detection and prevention capabilities; (2) updated intrusion assessment plans; and (3) annual updates on implementation, assessment findings, agency compliance, utilization of advanced security tools, and security metrics.

(Sec. 207) When authority expires for DHS's federal intrusion detection and prevention capabilities, the reporting requirements concerning such capabilities shall also expire.

(Sec. 208) The DNI and the OMB must submit to Congress an assessment of: (1) the risks that would result from the breach of unclassified information systems that provide access to information that may enable an adversary to derive information that would otherwise be considered classified, and (2) the cost and impact on the mission carried out by each agency if such systems were subsequently designated as national security systems.

(Sec. 209) The DHS Secretary may issue an emergency directive to an agency to take any lawful action with respect to the operation of the agency's information system in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to information security. DHS must report annually to Congress regarding the specific actions taken pursuant to such directive.

The Secretary may also authorize intrusion detection and prevention capabilities to ensure the security of agency information systems if the Secretary: (1) determines that there is an imminent threat to such systems, that operational or emergency directives are unlikely to be timely, and that the risk outweighs any adverse consequences; (2) provides prior notice to the OMB and the chief information officers of the affected agencies and notice to Congress within seven days of taking an action; and (3) authorizes the use of protective capabilities under procedures established in coordination with the OMB.

The Secretary may direct or authorize such lawful action or protective capability only: (1) to protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or (2) to require the remediation of, or to protect against, identified information security risks for information collected or maintained by or on behalf of an agency or that portion of an information system used or operated by an agency or by a contractor or other organization on behalf of an agency.

The OMB must report to Congress annually regarding specific actions it has taken to enforce agency compliance and

accountability.

TITLE III--FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

Federal Cybersecurity Workforce Assessment Act of 2015

(Sec. 303) This title requires federal agencies to: (1) identify all personnel positions that require the performance of cybersecurity or other cyber-related functions, and (2) assign a corresponding employment code to such positions using a coding structure that the National Institute of Standards and Technology (NIST) must include in the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework.
To implement the coding structure: (1) the Office of Personnel Management (OPM) must coordinate with NIST and the DNI to establish procedures to identify such federal civilian positions, and (2) DOD must establish procedures to identify such federal noncivilian positions.

Federal agencies must submit to Congress a report identifying: (1) the percentage of personnel with such job functions who currently hold industry-recognized certifications, (2) the preparedness of other civilian and noncivilian cyber personnel without existing credentials to take certification exams, and (3) a strategy for mitigating any identified gaps with training and certification for existing personnel.

The agencies must establish procedures to identify all encumbered and vacant positions with such functions and assign the appropriate employment code to each position.

(Sec. 304) Annually through 2022, the agencies must submit a report to the OPM that identifies cyber-related roles designated as critical needs in the agency's workforce. The OPM must provide agencies with guidance for identifying roles with acute and emerging skill shortages.

The OPM, within two years after enactment of this Act, must identify critical needs for the cyber workforce across all federal agencies and report to Congress regarding the implementation of this Act.

(Sec. 305) The GAO must report on the status of the implementation of this title within three years after enactment of this Act.

TITLE IV--OTHER CYBER MATTERS

(Sec. 401) DHS must report to Congress on threats relating to the security of the mobile devices of the federal government, including a plan for accelerated adoption of secure mobile device technology by DHS.

(Sec. 402) The Department of State shall produce a comprehensive strategy relating to U.S. international cyberspace policy. The strategy must include:

- a review of activities undertaken to support the goal of the President's International Strategy for Cyberspace;
- a plan to guide the diplomacy of the State Department to obtain agreements on the norms of responsible international behavior in cyberspace;
- a review of alternative concepts with regard to international norms in cyberspace offered by other foreign countries, including China, Russia, Brazil, and India;
- a description of cyberspace threats to U.S. national security from foreign countries, state-sponsored actors, and private actors to federal and private sector infrastructure, U.S. intellectual property, and U.S. citizens;
- a review of deterrent policy tools available to the President; and

a review of resources required by the State Department, including the Office of the Coordinator for Cyber Issues, to build international cyber behavior norms.

The State Department must brief congressional committees on such issues and make the strategy available to the public.

(Sec. 403) The State Department must consult with countries in which international cyber criminals are physically present, and from which extradition is unlikely, to determine what actions those governments have taken to prosecute and prevent cyber or intellectual property crimes against U.S. interests or citizens.

The State Department must also report annually to Congress regarding: (1) the number of such criminals located in other countries, including an indication of countries from which extradition is unlikely; (2) its discussions with officials of other countries; and (3) each international cyber criminal extradited to the United States.

(Sec. 404) The National Cybersecurity and Communications Integration Center must: (1) establish a process for statewide interoperability coordinators to report cybersecurity risks or incidents involving information systems or networks used by emergency response providers within their states, and (2) develop security and resilience recommendations for such networks. NIST must support, and report to Congress regarding, the development of methods for reducing cybersecurity risks to such emergency response providers.

(Sec. 405) The Department of Health and Human Services (HHS) must report to Congress regarding the preparedness of the health care industry in responding to cybersecurity threats. The report must identify the HHS official responsible for coordinating HHS cyber threat efforts and include plans on how HHS divisions will communicate with each other regarding such threats.

HHS must convene a one-year task force of health care industry stakeholders, cybersecurity experts, and federal agencies to plan a single system for the federal government to share intelligence regarding cybersecurity threats to the health care industry in near real time without charging a fee to the recipients. The task force must report to Congress regarding the plan and recommendations for securing private entities against cyber attacks and protecting networked medical devices and other software or systems that connect to an electronic health record. The task force must also provide HHS with cybersecurity preparedness information to disseminate to the health care industry.

HHS must collaborate with DHS, health care industry stakeholders, NIST, and other entities to establish a single, voluntary, national, health-specific cybersecurity framework with a common set of standards and security practices as a resource for cost-effectively reducing cybersecurity risks for health care organizations.

(Sec. 406) Inspectors general of agencies operating national security systems or federal computer systems that provide access to personally identifiable information must report to Congress regarding their agencies': (1) logical access standards for granting or denying requests to obtain and use information and processing services; (2) use of multi-factor logical access controls that require at least two of specified controls (information known to the user, an access device provided to the user, or a unique biometric characteristic of the user) to gain access to information; (3) procedures to detect exfiltration and inventory software and licenses; and (4) policies to ensure that contractors and other entities providing services to the agency implement appropriate data security management practices.

(Sec. 407) DHS, in conjunction with appropriate sector-specific agencies or federal entities that regulate critical infrastructure, must: (1) assess entities identified under Executive Order 13636, which provides for the identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security; (2) report to Congress regarding the extent to which such

entities report significant intrusions of information systems essential to the operation of critical infrastructure to DHS or appropriate agency heads in a timely manner; and (3) develop a strategy to ensure that a cybersecurity incident affecting such entities would no longer reasonably result in such catastrophic regional or national effects.

(Sec. 408) This section amends the federal criminal code to extend extraterritorially the application of penalties for fraud offenses involving an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States or any U.S. state or territory. (An access device is any card, code, electronic serial number, telecommunications service, or other means of account access that can be used to initiate a transfer of funds or to obtain money, goods, or services.) This section also removes a condition under current law that subjects a person to such penalties only if the underlying articles, property, or proceeds are held within or have transferred through U.S. jurisdiction.

(Sec. 409) This Act shall be in effect for ten years beginning on the date of its enactment.

Actions Timeline

- **Oct 28, 2015:** Received in the House.
- **Oct 28, 2015:** Message on Senate action sent to the House.
- **Oct 28, 2015:** Held at the desk.
- **Oct 27, 2015:** Considered by Senate. (consideration: CR S7498-7510, S7510-7522)
- **Oct 27, 2015:** Cloture motion on the measure withdrawn by unanimous consent in Senate. (consideration: CR S7520)
- **Oct 27, 2015:** Passed/agreed to in Senate: Passed Senate with an amendment by Yea-Nay Vote. 74 - 21. Record Vote Number: 291.(text: CR S7522-7534)
- **Oct 27, 2015:** Passed Senate with an amendment by Yea-Nay Vote. 74 - 21. Record Vote Number: 291. (text: CR S7522-7534)
- **Oct 22, 2015:** Considered by Senate. (consideration: CR S7430-7439, S7441-7445)
- **Oct 21, 2015:** Considered by Senate. (consideration: CR S7374-7406, S7407-7408)
- **Oct 20, 2015:** Measure laid before Senate by unanimous consent. (consideration: CR S7332-7342)
- **Oct 20, 2015:** Cloture motion on the measure presented in Senate. (consideration: CR S7342; text: CR S7342)
- **Aug 5, 2015:** Motion to proceed to measure considered in Senate. (consideration: CR S6329-6348, S6350-6351; text: CR S5329)
- **Aug 5, 2015:** Cloture motion on the motion to proceed to the measure withdrawn by unanimous consent in Senate. (consideration: CR S6342)
- **Aug 4, 2015:** Motion to proceed to measure considered in Senate. (consideration: CR S6256, S6257-6262, S6263-6264, S6266-6267, S6271-6272, S6279)
- **Aug 3, 2015:** Motion to proceed to consideration of measure made in Senate. (consideration: CR S6228)
- **Aug 3, 2015:** Cloture motion on the motion to proceed to consideration of the measure presented in Senate. (consideration: CR S6228; text: CR S6228)
- **Apr 15, 2015:** By Senator Burr from Select Committee on Intelligence filed written report. Report No. 114-32. Additional views filed.
- **Mar 17, 2015:** Introduced in Senate
- **Mar 17, 2015:** Select Committee on Intelligence. Original measure reported to Senate by Senator Burr. Without written report.
- **Mar 17, 2015:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 28.