

PROTECTING CYBER NETWORKS ACT

APRIL 13, 2015.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. NUNES, from the Permanent Select Committee on Intelligence, submitted the following

R E P O R T

[To accompany H.R. 1560]

[Including cost estimate of the Congressional Budget Office]

The Committee on Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 1560) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

- (a) SHORT TITLE.—This Act may be cited as the “Protecting Cyber Networks Act”.
(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

- Sec. 1. Short title; table of contents.
Sec. 2. Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.
Sec. 3. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.
Sec. 4. Sharing of cyber threat indicators and defensive measures with appropriate Federal entities other than the Department of Defense or the National Security Agency.
Sec. 5. Federal Government liability for violations of privacy or civil liberties.
Sec. 6. Protection from liability.
Sec. 7. Oversight of Government activities.
Sec. 8. Report on cybersecurity threats.
Sec. 9. Construction and preemption.
Sec. 10. Conforming amendments.
Sec. 11. Definitions.

SEC. 2. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT WITH NON-FEDERAL ENTITIES.

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 110 (50 U.S.C. 3045) the following new section:

“SEC. 111. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT WITH NON-FEDERAL ENTITIES.

“(a) SHARING BY THE FEDERAL GOVERNMENT.—

“(1) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—

“(A) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with representatives of relevant non-Federal entities with appropriate security clearances;

“(B) the timely sharing with relevant non-Federal entities of cyber threat indicators in the possession of the Federal Government that may be declassified and shared at an unclassified level; and

“(C) the sharing with non-Federal entities, if appropriate, of information in the possession of the Federal Government about imminent or ongoing cybersecurity threats to such entities to prevent or mitigate adverse impacts from such cybersecurity threats.

“(2) DEVELOPMENT OF PROCEDURES.—The procedures developed and promulgated under paragraph (1) shall—

“(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;

“(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector-specific information sharing and analysis centers;

“(C) include procedures for notifying non-Federal entities that have received a cyber threat indicator from a Federal entity in accordance with this Act that is known or determined to be in error or in contravention of the requirements of this section, the Protecting Cyber Networks Act, or the amendments made by such Act or another provision of Federal law or policy of such error or contravention;

“(D) include requirements for Federal entities receiving a cyber threat indicator or defensive measure to implement appropriate security controls to protect against unauthorized access to, or acquisition of, such cyber threat indicator or defensive measure;

“(E) include procedures that require Federal entities, prior to the sharing of a cyber threat indicator, to—

“(i) review such cyber threat indicator to assess whether such cyber threat indicator, in contravention of the requirement under section 3(d)(2) of the Protecting Cyber Networks Act, contains any information that such Federal entity knows at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat and remove such information; or

“(ii) implement a technical capability configured to remove or exclude any personal information of or information identifying a specific person not directly related to a cybersecurity threat; and

“(F) include procedures to promote the efficient granting of security clearances to appropriate representatives of non-Federal entities.

“(b) DEFINITIONS.—In this section, the terms ‘appropriate Federal entities’, ‘cyber threat indicator’, ‘defensive measure’, ‘Federal entity’, and ‘non-Federal entity’ have the meaning given such terms in section 11 of the Protecting Cyber Networks Act.”.

(b) SUBMITTAL TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall submit to Congress the procedures required by section 111(a) of the National Security Act of 1947, as inserted by subsection (a) of this section.

(c) TABLE OF CONTENTS AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting after the item relating to section 110 the following new item:

“Sec. 111. Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.”.

SEC. 3. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR PRIVATE-SECTOR DEFENSIVE MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for a cybersecurity purpose, monitor—

(A) an information system of such private entity;

(B) an information system of a non-Federal entity or a Federal entity, upon the written authorization of such non-Federal entity or such Federal entity; and

- (C) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.
- (2) CONSTRUCTION.—Nothing in this subsection shall be construed to—
- (A) authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this Act;
- (B) authorize the Federal Government to conduct surveillance of any person; or
- (C) limit otherwise lawful activity.
- (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—
- (1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a private entity may, for a cybersecurity purpose, operate a defensive measure that is operated on and is limited to—
- (A) an information system of such private entity to protect the rights or property of the private entity; and
- (B) an information system of a non-Federal entity or a Federal entity upon written authorization of such non-Federal entity or such Federal entity for operation of such defensive measure to protect the rights or property of such private entity, such non-Federal entity, or such Federal entity.
- (2) LIMITATION.—The authority provided in paragraph (1) does not include the intentional or reckless operation of any defensive measure that destroys, renders unusable or inaccessible (in whole or in part), substantially harms, or initiates a new action, process, or procedure on an information system or information stored on, processed by, or transiting such information system not owned by—
- (A) the private entity operating such defensive measure; or
- (B) a non-Federal entity or a Federal entity that has provided written authorization to that private entity for operation of such defensive measure on the information system or information of the entity in accordance with this subsection.
- (3) CONSTRUCTION.—Nothing in this subsection shall be construed—
- (A) to authorize the use of a defensive measure other than as provided in this subsection; or
- (B) to limit otherwise lawful activity.
- (c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—
- (1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the requirement under subsection (d)(2) to remove personal information of or information identifying a specific person not directly related to a cybersecurity threat and the protection of classified information—
- (A) share a lawfully obtained cyber threat indicator or defensive measure with any other non-Federal entity or an appropriate Federal entity (other than the Department of Defense or any component of the Department, including the National Security Agency); and
- (B) receive a cyber threat indicator or defensive measure from any other non-Federal entity or an appropriate Federal entity.
- (2) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity.
- (3) CONSTRUCTION.—Nothing in this subsection shall be construed to—
- (A) authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection;
- (B) authorize the sharing or receiving of classified information by or with any person not authorized to access such classified information;
- (C) prohibit any Federal entity from engaging in formal or informal technical discussion regarding cyber threat indicators or defensive measures with a non-Federal entity or from providing technical assistance to address vulnerabilities or mitigate threats at the request of such an entity;
- (D) limit otherwise lawful activity;
- (E) prohibit a non-Federal entity, if authorized by applicable law or regulation other than this Act, from sharing a cyber threat indicator or defensive measure with the Department of Defense or any component of the Department, including the National Security Agency; or
- (F) authorize the Federal Government to conduct surveillance of any person.
- (d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement an appropriate security control to protect against unauthorized access to, or acquisition of, such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Federal entity sharing a cyber threat indicator pursuant to this Act shall, prior to such sharing, take reasonable efforts to—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the non-Federal entity reasonably believes at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement a technical capability configured to remove any information contained within such indicator that the non-Federal entity reasonably believes at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY NON-FEDERAL ENTITIES.—A non-Federal entity may, for a cybersecurity purpose—

(A) use a cyber threat indicator or defensive measure shared or received under this section to monitor or operate a defensive measure on—

(i) an information system of such non-Federal entity; or

(ii) an information system of another non-Federal entity or a Federal entity upon the written authorization of that other non-Federal entity or that Federal entity; and

(B) otherwise use, retain, and further share such cyber threat indicator or defensive measure subject to—

(i) an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure; or

(ii) an otherwise applicable provision of law.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—A State, tribal, or local government may use a cyber threat indicator shared with such State, tribal, or local government for the purposes described in clauses (i), (ii), and (iii) of section 4(d)(5)(A).

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records, except as otherwise required by applicable State, tribal, or local law requiring disclosure in any criminal prosecution.

(e) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with a non-Federal entity under this Act shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

SEC. 4. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH APPROPRIATE FEDERAL ENTITIES OTHER THAN THE DEPARTMENT OF DEFENSE OR THE NATIONAL SECURITY AGENCY.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) IN GENERAL.—Section 111 of the National Security Act of 1947, as inserted by section 2 of this Act, is amended—

(A) by redesignating subsection (b) as subsection (c); and

(B) by inserting after subsection (a) the following new subsection:

“(b) POLICIES AND PROCEDURES FOR SHARING WITH THE APPROPRIATE FEDERAL ENTITIES OTHER THAN THE DEPARTMENT OF DEFENSE OR THE NATIONAL SECURITY AGENCY.—

“(1) ESTABLISHMENT.—The President shall develop and submit to Congress policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

“(2) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—The policies and procedures required under paragraph (1) shall—

“(A) be developed in accordance with the privacy and civil liberties guidelines required under section 4(b) of the Protecting Cyber Networks Act;

“(B) ensure that—

“(i) a cyber threat indicator shared by a non-Federal entity with an appropriate Federal entity (other than the Department of Defense or any component of the Department, including the National Security

Agency) pursuant to section 3 of such Act is shared in real-time with all of the appropriate Federal entities (including all relevant components thereof);

“(ii) the sharing of such cyber threat indicator with appropriate Federal entities is not subject to any delay, modification, or any other action without good cause that could impede receipt by all of the appropriate Federal entities; and

“(iii) such cyber threat indicator is provided to each other Federal entity to which such cyber threat indicator is relevant; and

“(C) ensure there—

“(i) is an audit capability; and

“(ii) are appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully use a cyber threat indicator or defense measure shared with the Federal Government by a non-Federal entity under the Protecting Cyber Networks Act other than in accordance with this section and such Act.”.

(2) SUBMISSION.—The President shall submit to Congress—

(A) not later than 90 days after the date of the enactment of this Act, interim policies and procedures required under section 111(b)(1) of the National Security Act of 1947, as inserted by paragraph (1) of this section; and

(B) not later than 180 days after such date, final policies and procedures required under such section 111(b)(1).

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—The Attorney General, in consultation with the heads of the other appropriate Federal agencies and with officers designated under section 1062 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee–1), shall develop and periodically review guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in accordance with this Act and the amendments made by this Act.

(2) CONTENT.—The guidelines developed and reviewed under paragraph (1) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act, 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 in accordance with this Act or the amendments made by this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or information identifying specific persons, including by establishing—

(i) a process for the prompt destruction of such information that is known not to be directly related to a use for a cybersecurity purpose;

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained; and

(iii) a process to inform recipients that such indicators may only be used for a cybersecurity purpose;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying non-Federal entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) be consistent with any other applicable provisions of law and the fair information practice principles set forth in appendix A of the document entitled “National Strategy for Trusted Identities in Cyberspace” and published by the President in April, 2011; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified information and other sensitive national security information.

(3) SUBMISSION.—The Attorney General shall submit to Congress—

(A) not later than 90 days after the date of the enactment of this Act, interim guidelines required under paragraph (1); and

(B) not later than 180 days after such date, final guidelines required under such paragraph.

(c) NATIONAL CYBER THREAT INTELLIGENCE INTEGRATION CENTER.—

(1) ESTABLISHMENT.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.), as amended by section 2 of this Act, is further amended—

(A) by redesignating section 119B as section 119C; and

(B) by inserting after section 119A the following new section:

“SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION CENTER.

“(a) ESTABLISHMENT.—There is within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center.

“(b) DIRECTOR.—There is a Director of the Cyber Threat Intelligence Integration Center, who shall be the head of the Cyber Threat Intelligence Integration Center, and who shall be appointed by the Director of National Intelligence.

“(c) PRIMARY MISSIONS.—The Cyber Threat Intelligence Integration Center shall—

“(1) 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;

“(2) ensure that appropriate departments and agencies have full access to and receive all-source intelligence support needed to execute the cyber threat intelligence activities of such agencies and to perform independent, alternative analyses;

“(3) disseminate cyber threat analysis to the President, the appropriate departments and agencies of the Federal Government, and the appropriate committees of Congress;

“(4) coordinate cyber threat intelligence activities of the departments and agencies of the Federal Government; and

“(5) conduct strategic cyber threat intelligence planning for the Federal Government.

“(d) LIMITATIONS.—The Cyber Threat Intelligence Integration Center shall—

“(1) have not more than 50 permanent positions;

“(2) in carrying out the primary missions of the Center described in subsection (c), may not augment staffing through detailees, assignees, or core contractor personnel or enter into any personal services contracts to exceed the limitation under paragraph (1); and

“(3) be located in a building owned or operated by an element of the intelligence community as of the date of the enactment of this section.”.

(2) TABLE OF CONTENTS AMENDMENTS.—The table of contents in the first section of the National Security Act of 1947, as amended by section 2 of this Act, is further amended by striking the item relating to section 119B and inserting the following new items:

“Sec. 119B. Cyber Threat Intelligence Integration Center.

“Sec. 119C. National intelligence centers.”.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this Act shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 3(c)(2), a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this Act shall be considered the commercial, financial, and proprietary information of the non-Federal entity that is the originator of such cyber threat indicator or defensive measure when so designated by such non-Federal entity or a non-Federal entity acting in accordance with the written authorization of the non-Federal entity that is the originator of such cyber threat indicator or defensive measure.

(3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure provided to the Federal Government under this Act shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records, except as otherwise required by applicable Federal, State, tribal, or local law requiring disclosure in any criminal prosecution.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this Act shall not be subject to a rule of any Federal department or agency or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) **AUTHORIZED ACTIVITIES.**—A cyber threat indicator or defensive measure provided to the Federal Government under this Act may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any department, agency, component, officer, employee, or agent of the Federal Government solely for—

- (i) a cybersecurity purpose;
- (ii) the purpose of responding to, prosecuting, or otherwise preventing or mitigating a threat of death or serious bodily harm or an offense arising out of such a threat;
- (iii) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or
- (iv) the purpose of preventing, investigating, disrupting, or prosecuting any of the offenses listed in sections 1028, 1029, 1030, and 3559(c)(2)(F) and chapters 37 and 90 of title 18, United States Code.

(B) **PROHIBITED ACTIVITIES.**—A cyber threat indicator or defensive measure provided to the Federal Government under this Act shall not be disclosed to, retained by, or used by any Federal department or agency for any use not permitted under subparagraph (A).

(C) **PRIVACY AND CIVIL LIBERTIES.**—A cyber threat indicator or defensive measure provided to the Federal Government under this Act shall be retained, used, and disseminated by the Federal Government in accordance with—

- (i) the policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government required by subsection (b) of section 111 of the National Security Act of 1947, as added by subsection (a) of this section; and
- (ii) the privacy and civil liberties guidelines required by subsection (b).

SEC. 5. FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF PRIVACY OR CIVIL LIBERTIES.

(a) **IN GENERAL.**—If a department or agency of the Federal Government intentionally or willfully violates the privacy and civil liberties guidelines issued by the Attorney General under section 4(b), the United States shall be liable to a person injured by such violation in an amount equal to the sum of—

- (1) the actual damages sustained by the person as a result of the violation or \$1,000, whichever is greater; and
- (2) reasonable attorney fees as determined by the court and other litigation costs reasonably incurred in any case under this subsection in which the complainant has substantially prevailed.

(b) **VENUE.**—An action to enforce liability created under this section may be brought in the district court of the United States in—

- (1) the district in which the complainant resides;
- (2) the district in which the principal place of business of the complainant is located;
- (3) the district in which the department or agency of the Federal Government that violated such privacy and civil liberties guidelines is located; or
- (4) the District of Columbia.

(c) **STATUTE OF LIMITATIONS.**—No action shall lie under this subsection unless such action is commenced not later than two years after the date of the violation of the privacy and civil liberties guidelines issued by the Attorney General under section 4(b) that is the basis for the action.

(d) **EXCLUSIVE CAUSE OF ACTION.**—A cause of action under this subsection shall be the exclusive means available to a complainant seeking a remedy for a violation by a department or agency of the Federal Government under this Act.

SEC. 6. PROTECTION FROM LIABILITY.

(a) **MONITORING OF INFORMATION SYSTEMS.**—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 3(a) that is conducted in good faith in accordance with this Act and the amendments made by this Act.

(b) **SHARING OR RECEIPT OF CYBER THREAT INDICATORS.**—No cause of action shall lie or be maintained in any court against any non-Federal entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 3(c), or a good faith failure to act based on such sharing or receipt, if such sharing or receipt is conducted in good faith in accordance with this Act and the amendments made by this Act.

(c) **WILLFUL MISCONDUCT.**—

(1) **RULE OF CONSTRUCTION.**—Nothing in this section shall be construed—

(A) to require dismissal of a cause of action against a non-Federal entity (including a private entity) that has engaged in willful misconduct in the course of conducting activities authorized by this Act or the amendments made by this Act; or

(B) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(2) **PROOF OF WILLFUL MISCONDUCT.**—In any action claiming that subsection (a) or (b) does not apply due to willful misconduct described in paragraph (1), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each non-Federal entity subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

(3) **WILLFUL MISCONDUCT DEFINED.**—In this subsection, the term “willful misconduct” means an act or omission that is taken—

(A) intentionally to achieve a wrongful purpose;

(B) knowingly without legal or factual justification; and

(C) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) **BIENNIAL REPORT ON IMPLEMENTATION.**—

(1) **IN GENERAL.**—Section 111 of the National Security Act of 1947, as added by section 2(a) and amended by section 4(a) of this Act, is further amended—

(A) by redesignating subsection (c) (as redesignated by such section 4(a)) as subsection (d); and

(B) by inserting after subsection (b) (as inserted by such section 4(a)) the following new subsection:

“(c) **BIENNIAL REPORT ON IMPLEMENTATION.**—

“(1) **IN GENERAL.**—Not less frequently than once every two years, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall submit to Congress a report concerning the implementation of this section and the Protecting Cyber Networks Act.

“(2) **CONTENTS.**—Each report submitted under paragraph (1) shall include the following:

“(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by this section and section 4 of the Protecting Cyber Networks Act in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

“(B) An assessment of whether the procedures developed under section 3 of such Act comply with the goals described in subparagraphs (A), (B), and (C) of subsection (a)(1).

“(C) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this section and such Act.

“(D) A review of the type of cyber threat indicators shared with the Federal Government under this section and such Act, including the following:

“(i) The degree to which such information may impact the privacy and civil liberties of specific persons.

“(ii) A quantitative and qualitative assessment of the impact of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons.

“(iii) The adequacy of any steps taken by the Federal Government to reduce such impact.

“(E) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this section or such Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under this section or section 4 of such Act.

“(F) A description of any significant violations of the requirements of this section or such Act by the Federal Government—

“(i) an assessment of all reports of officers, employees, and agents of the Federal Government misusing information provided to the Federal Government under the Protecting Cyber Networks Act or this section, without regard to whether the misuse was knowing or wilful; and

“(ii) an assessment of all disciplinary actions taken against such officers, employees, and agents.

“(G) A summary of the number and type of non-Federal entities that received classified cyber threat indicators from the Federal Government

under this section or such Act and an evaluation of the risks and benefits of sharing such cyber threat indicators.

“(H) An assessment of any personal information of or information identifying a specific person not directly related to a cybersecurity threat that—

“(i) was shared by a non-Federal entity with the Federal Government under this Act in contravention of section 3(d)(2); or

“(ii) was shared within the Federal Government under this Act in contravention of the guidelines required by section 4(b).

“(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities and processes under this section or such Act.

“(4) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

“(5) PUBLIC AVAILABILITY OF REPORTS.—The Director of National Intelligence shall make publicly available the unclassified portion of each report required by paragraph (1).”

(2) INITIAL REPORT.—The first report required under subsection (c) of section 111 of the National Security Act of 1947, as inserted by paragraph (1) of this subsection, shall be submitted not later than one year after the date of the enactment of this Act.

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—

(A) IN GENERAL.—Section 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(e)) is amended by adding at the end the following new paragraph:

“(3) BIENNIAL REPORT ON CERTAIN CYBER ACTIVITIES.—

“(A) REPORT REQUIRED.—The Privacy and Civil Liberties Oversight Board shall biennially submit to Congress and the President a report containing—

“(i) an assessment of the privacy and civil liberties impact of the activities carried out under the Protecting Cyber Networks Act and the amendments made by such Act; and

“(ii) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 4 of the Protecting Cyber Networks Act and the amendments made by such section 4 in addressing privacy and civil liberties concerns.

“(B) RECOMMENDATIONS.—Each report submitted under this paragraph may include such recommendations as the Privacy and Civil Liberties Oversight Board may have for improvements or modifications to the authorities under the Protecting Cyber Networks Act or the amendments made by such Act.

“(C) FORM.—Each report required under this paragraph shall be submitted in unclassified form, but may include a classified annex.

“(D) PUBLIC AVAILABILITY OF REPORTS.—The Privacy and Civil Liberties Oversight Board shall make publicly available the unclassified portion of each report required by subparagraph (A).”

(B) INITIAL REPORT.—The first report required under paragraph (3) of section 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(e)), as added by subparagraph (A) of this paragraph, shall be submitted not later than 2 years after the date of the enactment of this Act.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, and the Inspector General of the Department of Defense, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this Act and the amendments made by this Act.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(C) RECOMMENDATIONS.—Each report submitted under this paragraph may include such recommendations as the Inspectors General referred to in subparagraph (A) may have for improvements or modifications to the authorities under this Act or the amendments made by this Act.

(D) FORM.—Each report required under this paragraph shall be submitted in unclassified form, but may include a classified annex.

(E) PUBLIC AVAILABILITY OF REPORTS.—The Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, and the Inspector General of the Department of Defense shall make publicly available the unclassified portion of each report required under subparagraph (A).

SEC. 8. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) An assessment of—

(A) the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats (including cyber attacks, theft, and data breaches) directed against the United States that threaten the United States national security interests, economy, and intellectual property; and

(B) the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and non-state actors that are the primary threats of carrying out a cybersecurity threat (including a cyber attack, theft, or data breach) against the United States and that threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats (including cyber attacks, theft, or data breaches) directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats (including cyber attacks, theft, and data breaches).

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) PUBLIC AVAILABILITY OF REPORT.—The Director of National Intelligence shall make publicly available the unclassified portion of the report required by subsection (a).

(e) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term “intelligence community” has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 9. CONSTRUCTION AND PREEMPTION.

(a) PROHIBITION OF SURVEILLANCE.—Nothing in this Act or the amendments made by this Act shall be construed to authorize the Department of Defense or the National Security Agency or any other element of the intelligence community to target a person for surveillance.

(b) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this Act or the amendments made by this Act shall be construed to limit or prohibit—

(1) otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government; or

(2) any otherwise lawful use of such disclosures by any entity of the Federal government, without regard to whether such otherwise lawful disclosures duplicate or replicate disclosures made under this Act.

(c) WHISTLE BLOWER PROTECTIONS.—Nothing in this Act or the amendments made by this Act shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), or any similar provision of Federal or State law.

(d) PROTECTION OF SOURCES AND METHODS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any department or agency thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of the President or a department or agency of the Federal Government to protect and control the dissemination of classified information, intelligence sources and methods, and the national security of the United States.

(e) RELATIONSHIP TO OTHER LAWS.—Nothing in this Act or the amendments made by this Act shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to limit or modify an existing information-sharing relationship;

(2) to prohibit a new information-sharing relationship; or

(3) to require a new information-sharing relationship between any non-Federal entity and the Federal Government.

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity;

or

(2) to abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this Act or the amendments made by this Act shall be construed to permit the Federal Government—

(1) to require a non-Federal entity to provide information to the Federal Government;

(2) to condition the sharing of a cyber threat indicator with a non-Federal entity on such non-Federal entity's provision of a cyber threat indicator to the Federal Government; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this Act or the amendments made by this Act shall be construed to subject any non-Federal entity to liability for choosing not to engage in a voluntary activity authorized in this Act and the amendments made by this Act.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this Act or the amendments made by this Act shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this Act or the amendments made by this Act for any use other than permitted in this Act or the amendments made by this Act.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This Act and the amendments made by this Act supersede any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this Act or the amendments made by this Act.

(2) STATE LAW ENFORCEMENT.—Nothing in this Act or the amendments made by this Act shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized by this Act or the amendments made by this Act;

(2) to establish any regulatory authority not specifically established under this Act or the amendments made by this Act; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

SEC. 10. CONFORMING AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

- (1) in paragraph (8), by striking “or” at the end;
- (2) in paragraph (9), by striking “wells.” and inserting “wells; or”; and
- (3) by inserting after paragraph (9) the following:
“(10) information shared with or provided to the Federal Government pursuant to the Protecting Cyber Networks Act or the amendments made by such Act.”.

SEC. 11. DEFINITIONS.

In this Act:

(1) **AGENCY.**—The term “agency” has the meaning given the term in section 3502 of title 44, United States Code.

(2) **APPROPRIATE FEDERAL ENTITIES.**—The term “appropriate Federal entities” means the following:

- (A) The Department of Commerce.
- (B) The Department of Defense.
- (C) The Department of Energy.
- (D) The Department of Homeland Security.
- (E) The Department of Justice.
- (F) The Department of the Treasury.
- (G) The Office of the Director of National Intelligence.

(3) **CYBERSECURITY PURPOSE.**—The term “cybersecurity purpose” means the purpose of protecting (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 identifying the source of a cybersecurity threat.

(4) **CYBERSECURITY THREAT.**—

(A) **IN GENERAL.**—Except as provided in subparagraph (B), the term “cybersecurity threat” means an action, not protected by the first amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, confidentiality, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system.

(B) **EXCLUSION.**—The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(5) **CYBER THREAT INDICATOR.**—The term “cyber threat indicator” means information or a physical object that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law.

(6) **DEFENSIVE MEASURE.**—The term “defensive measure” means an action, device, procedure, technique, or other measure executed on an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability.

(7) **FEDERAL ENTITY.**—The term “Federal entity” means a department or agency of the United States or any component of such department or agency.

(8) **INFORMATION SYSTEM.**—The term “information system”—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(9) LOCAL GOVERNMENT.—The term “local government” means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(10) MALICIOUS CYBER COMMAND AND CONTROL.—The term “malicious cyber command and control” means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(11) MALICIOUS RECONNAISSANCE.—The term “malicious reconnaissance” means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(12) MONITOR.—The term “monitor” means to acquire, identify, scan, or otherwise possess information that is stored on, processed by, or transiting an information system.

(13) NON-FEDERAL ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term “non-Federal entity” means any private entity, non-Federal government department or agency, or State, tribal, or local government (including a political subdivision, department, officer, employee, or agent thereof).

(B) INCLUSIONS.—The term “non-Federal entity” includes a government department or agency (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term “non-Federal entity” does not include a foreign power or known agent of a foreign power, as both terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(14) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term “private entity” means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term “private entity” includes a component of a State, tribal, or local government performing electric utility services.

(C) EXCLUSION.—The term “private entity” does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(15) REAL TIME; REAL-TIME.—The terms “real time” and “real-time” mean a process by which an automated, machine-to-machine system processes cyber threat indicators such that the time in which the occurrence of an event and the reporting or recording of it are as simultaneous as technologically and operationally practicable.

(16) SECURITY CONTROL.—The term “security control” means the management, operational, and technical controls used to protect against an unauthorized effort to adversely impact the security, confidentiality, integrity, and availability of an information system or its information.

(17) SECURITY VULNERABILITY.—The term “security vulnerability” means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) TRIBAL.—The term “tribal” has the meaning given the term “Indian tribe” in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

PURPOSE

The purpose of H.R. 1560 is to improve cybersecurity in the United States by enhancing the sharing of information about cybersecurity threats.

BACKGROUND AND NEED FOR LEGISLATION

Four years ago, when this Committee first considered cybersecurity legislation, few Americans understood the threat our Nation faced from cyberattacks by foreign militaries, intelligence services, and criminal organizations. Even fewer understood that, as citizens and consumers, those same attacks could endanger their health records, financial data, and other sensitive personal information.

Today, hardly a day goes by without news of a cyberattack on an American business or government agency. High-profile attacks are commonplace. Both in the boardroom and around the kitchen table, Americans suffer the impact of cyberattacks. Whether carried out by foreign governments or criminals, these attacks steal Americans' identities, credit card information, tax refunds, and countless other kinds of private information. In just the past year, attackers have shown they can adeptly carry out criminal activity, including theft and espionage, on computer networks inside the United States. These attacks violate Americans' privacy on a massive scale and cost thousands of American jobs.

Some cyberattacks are sponsored by foreign governments. China, Russia, North Korea, and Iran have created highly skilled cyberwarfare units that directly target American businesses for their most valuable intellectual property. Corporate research and development forms the lifeblood of the American economy, and China, in particular, engages in daily assaults that pillage American innovation. In May 2014, for instance, federal prosecutors charged five military officers from Unit 61398 of the Third Department of the Chinese People's Liberation Army with computer hacking and economic espionage against the U.S. nuclear power, metals, and solar products industries. They were not the first and will not be the last foreign military officers who launch cyberattacks on American industry. The sheer number of attacks against American companies—at least thousands each day—harms our economy and thus our national security.

Other attacks are carried out by criminal organizations. A recent Washington Post report suggested that more than 3,000 companies were alerted to cyberattacks by federal agents in 2013. And that number represents only the number of cases in which the federal government learned that an attack occurred. We cannot expect the private sector to defend itself against unrelenting assaults of foreign governments without federal assistance.

There is no silver bullet to end cyberattacks. Thousands of attacks occur each day and will continue after this bill becomes law. Companies must defend their networks around the clock on all fronts, but an attacker only needs to succeed once to cause tremendous amounts of damage. No piece of legislation can wholly prevent this devastating hacking. However, the ability to share cyber threat information and solutions will significantly help security officials throughout both the private sector and the government defend their networks, and thereby defend Americans' most private information and most valuable intellectual property.

The government already provides significant support and assistance to private companies to address cyberattacks, but more can—and should—be done. Real and perceived legal barriers to cybersecurity monitoring and information sharing constrain companies

with even the best of intentions. After hundreds of conversations with companies in virtually every sector of the economy, the executive branch, and privacy and civil liberties advocates, it is clear to the Committee that American businesses need positive legal authority to monitor their networks and to share and receive cyber threat indicators and defensive measures. Voluntary information sharing between companies helps businesses defend themselves against cyberattacks, and voluntary, two-way information sharing with the federal government can help the government disseminate cyber threat information with greater speed and accuracy. The positive authorization contained in this bill is important to encourage this sharing and to help businesses improve their defenses against cyberattacks. As a result, this bill helps protect Americans' privacy.

In each of the past two Congresses, the Committee adopted cybersecurity information sharing legislation that passed the House with bipartisan support. Then-Chairman Rogers and Ranking Member Ruppertsberger made great strides in educating the American people about the cybersecurity threat and the need for information sharing legislation. Even so, in both of the past two Congresses, the Senate failed to act.

Building on those past efforts, Chairman Nunes and Ranking Member Schiff led a bipartisan effort to advance cyber legislation in the 114th Congress. The result of their efforts, the Protecting Cyber Networks Act, enables private companies to monitor their networks and to voluntarily share cyber threat indicators with one another and with the federal government, all while providing strong protections for privacy and civil liberties.

SCOPE OF COMMITTEE REVIEW

On March 19, 2015, the Committee held an open hearing, *The Growing Cyber Threat and Its Impact on American Business*. At that hearing, the Committee heard testimony from Governor Tim Pawlenty, the former governor of Minnesota and current Chief Executive Officer of the Financial Services Roundtable; Mr. Andrew Tannenbaum, cybersecurity counsel for IBM; Mr. John Latimer, Chief Risk and Compliance Officer for Total Systems Services, Inc.; and Mr. Richard Bejtlich, Chief Security Strategist for FireEye, Inc. The hearing focused on the state of cybersecurity information sharing between the federal government and the private sector, as well as information sharing within the private sector.

Before and after the open hearing, Committee staff met with representatives from the White House, the Department of Justice, the Department of Defense, the Federal Bureau of Investigation, the Department of Treasury, the Department of Homeland Security, and the National Security Agency in the course of developing this legislation. Committee staff also held numerous meetings with private sector companies and trade groups in the telecommunications, technology, financial services, utilities, retail, defense, and internet security industries, and several meetings with representatives of privacy groups including, among others, the Center for Democracy and Technology, the American Civil Liberties Union, and the Open Technology Institute.

Lastly, as part of its regular oversight responsibilities, the Committee held numerous classified briefings and meetings about

cyberattacks and the serious threat they pose to our national security.

COMMITTEE STATEMENT AND VIEWS

The Protecting Cyber Networks Act tears down legal barriers to improved cybersecurity. The bill authorizes companies to monitor their own networks and the networks of other consenting private parties for cybersecurity threats. It also authorizes companies to use and share defensive measures—techniques that prevent or mitigate cybersecurity threats—on their own networks and on the networks of other consenting private parties. And most importantly, notwithstanding any other federal or state law, the bill authorizes and provides liability protection for the sharing and receipt of cyber threat indicators and defensive measures. The bill encourages sharing of cyber threat indicators and defensive measures along three axes: between private companies; from private companies to the federal government; and from the federal government to private companies. Because of the real and perceived legal barriers to information sharing, the bill provides strong liability protection for sharing through its procedures. Any company that shares cyber threat indicators or defensive measures in good faith compliance with the bill—including the requirement to strip out private information unrelated to the cyber threat—will receive immunity from lawsuits. This immunity includes, among other things, immunity from liability under the antitrust laws. The bill also prohibits the federal government from penalizing companies for sharing cyber threat information pursuant to the Act. As Section 9(l) makes clear, nothing in the bill allows the government to establish regulations or regulatory authority based on the cybersecurity information companies share.

The bill also provides companies with the flexibility that will encourage information sharing. Compared to previous legislative efforts, the bill gives companies the flexibility to choose to share cyber threat indicators or defensive measures with a number of different government agencies. Companies receive authorization and liability protection for sharing with the Department of Justice (including the Federal Bureau of Investigation), the Department of Commerce, the Department of the Treasury, the Office of the Director of National Intelligence, the Department of Homeland Security, and the Department of Energy. Some companies may be more comfortable sharing different kinds of cyber threat indicators with different agencies that possess different expertise. Under this bill, banks can share cyber threat information with the Department of the Treasury; power plants can share with the Department of Energy; and victims of crime can share with federal law enforcement agencies. After any federal agency receives a cyber threat indicator or defensive measure from the private sector, it must share that indicator or defensive measure in real-time, that is, by an automated machine-to-machine process, with all other appropriate federal agencies, including the Department of Defense and the National Security Agency.

Although the bill does not grant any new authorization or liability protection for companies to share cyber threat indicators or defensive measures with the Department of Defense or the National Security Agency, companies may choose to share cyber threat indi-

cators or defensive measures with the Department of Defense or the National Security Agency outside of the bill. The Committee understands the critical importance of cybersecurity to the Department of Defense's missions, many of which rely on private sector partnerships with the Defense Industrial Base. The bill's lack of authorization for companies to share with the Department of Defense or the National Security Agency is not a prohibition on sharing with those agencies if doing so is otherwise lawful. Section 3(c)(3)(E) expressly states that nothing in the bill should be construed to prohibit private companies from sharing cyber threat indicators with the Department of Defense or the National Security Agency when that sharing is authorized by another law or regulation, and Section 9(f) makes clear that nothing in the bill limits or modifies any existing information sharing relationship or prohibits a new information sharing relationship outside of the Act. The bill also does not supersede any private contract, including any contractual obligation for a company to report a cyber intrusion to the Department of Defense or to any other federal agency.

At the same time, the bill contains strong privacy protections, far in excess of previous legislative efforts. First, the bill only authorizes the sharing of cyber threat indicators. The bill contains a narrow definition of cyber threat indicator that does not include personal information unrelated to cybersecurity. Thus, the sharing of personal information that is not directly related to a cybersecurity threat is not authorized by the bill. Companies will not receive any liability protection for such sharing.

Second, even if personal information constitutes a cyber threat indicator, companies may only share the information for a cybersecurity purpose. This restriction ensures that companies do not improperly share personal information for reasons outside the scope of the bill.

Third, the liability protections of the bill are only available if a company sharing information takes reasonable efforts to remove irrelevant personally identifiable information before sharing. If a company fails to take such efforts, it will not receive the liability protections of the bill. The bill's description of personally identifiable information is intended to match the description contained in the Cybersecurity Information Sharing Act, S. 754, as reported favorably by the Senate Select Committee on Intelligence on March 17, 2015.

Fourth, if the federal government receives cyber threat indicators, the bill obligates the government to search for and remove or exclude any residual, irrelevant personally identifiable information that it may have received. This dual privacy scrub will drastically minimize the sharing or dissemination of any personally identifiable information, protecting privacy while also ensuring that companies are able to take needed actions to address cyber threats.

Fifth, the bill imposes strict limitations on the use and retention of any data voluntarily shared by the private sector with the government. The government may use the information it receives for cybersecurity purposes because it must be able to protect itself from cybersecurity threats that exist in the private sector, as well as provide the information to others to fulfill its duties to protect the Nation from cybersecurity threats. The government may also use the information to respond to specific dangerous crimes. These

include the sexual abuse of minors, threats of death and serious bodily harm, and other violent felonies. Companies cannot share cyber threat information with the government for the purpose of stopping crimes, but when companies share these cyber threat indicators for a cybersecurity purpose, and that information also contains information related to these kinds of crimes, the government should not sit on its hands and ignore violent felonies and child sex offenses.

Sixth, the bill provides for strong public and congressional oversight by requiring a detailed biennial Inspectors General report of appropriate federal entities of the government's receipt, use, and dissemination of cyber threat indicators. Additionally, the Privacy and Civil Liberties Oversight Board must produce a biennial report on the privacy and civil liberties impact of the Act.

Finally, the bill expressly states that it provides no authority for the U.S. government to conduct any surveillance. The bill authorizes the sharing of cyber threat indicators and defensive measures, not surveillance.

COMMITTEE CONSIDERATION AND ROLL CALL VOTES

On March 26, 2015, the Committee met in open session to consider H.R. 1560, the Protecting Cyber Networks Act. The section-by-section analysis details the contents of H.R. 1560.

Chairman Nunes and Ranking Member Schiff offered an amendment to clarify that the bill does not impact any existing information sharing relationships between the private sector and the Department of Defense, including the National Security Agency. The amendment made several other technical changes and incorporated privacy-enhancing proposals by Ms. Speier, Mr. Carson, and Mr. Swalwell. The amendment was agreed to by a voice vote.

Mr. Swalwell offered an amendment to the bill's liability provision, which he subsequently withdrew.

The Committee then adopted a motion by Chairman Nunes to favorably report the bill H.R. 1560 to the House, as amended. The motion was agreed to by a voice vote.

SECTION-BY-SECTION ANALYSIS

Section 1: Short title; Table of contents

The short title of the Act is the Protecting Cyber Networks Act.

Section 2: Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government with Non-Federal Entities

This section of the Act amends Title I of the National Security Act by adding a new section, Section 111. Under this new section, the Director of National Intelligence, in consultation with the heads of the Departments of Homeland Security, Treasury, Justice, Commerce, and Defense (hereinafter the "appropriate Federal entities"), should create procedures to facilitate and promote the timely sharing of cyber threat indicators with the private sector. The procedures would promote the sharing of: classified cyber threat indicators with representatives of the private sector with appropriate security clearances; classified cyber threat indicators that may be declassified and shared at an unclassified level; and any information in the possession of the Federal Government about imminent

or ongoing cyber threats that may allow private companies to prevent or mitigate those threats.

The procedures must also ensure the Federal Government creates and maintains the capability to share cyber threat indicators in real time with the private sector, consistent with the protection of classified information.

Additionally, the procedures drafted by the Director of National Intelligence will require federal agencies to perform a review of cyber threat indicators they receive from the private sector before the agencies share those indicators within the Federal Government. In that review, the receiving agencies will assess whether—despite the private sector’s own requirement to conduct a similar review—the cyber threat indicators contain any personal information or information identifying a specific person that does not directly relate to a cyber threat. If so, the Federal Government must remove that information. The Federal Government must implement a technical capability configured to remove or exclude the information.

Section 3: Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats

Subsection (a)

Subsection (a) of this section authorizes private entities to engage in defensive monitoring of their own networks and the networks of non-Federal entities that have consented to monitoring. Subsection (a) does not authorize the Federal Government to conduct surveillance of any person.

Subsection (b)

Subsection (b) of this section authorizes private entities to operate defensive measures on their own networks and the networks of non-Federal entities that have consented to the operation of defensive measures. Subsection (b) does not authorize non-Federal entities to intentionally or recklessly operate any defensive measure that destroys, render unusable or inaccessible (in whole or in part), substantially harms, or initiates a new action, process, or procedure on any network that does not belong to them or to a non-Federal entity that has not consented to the operation of those defensive measures. As a result, subsection (b) does not authorize “hacking back” or any other form of cyber operation that takes place on computers or networks without the consent of the owner of those computers or networks.

Subsection (c)

Subsection (c) of this section authorizes non-Federal entities, notwithstanding any other provision of law, to share or receive cyber threat indicators or defensive measures for cybersecurity purposes with other non-Federal entities. This subsection also authorizes non-Federal entities to share or receive cyber threat indicators or defensive measures with appropriate Federal entities other than the Department of Defense and the National Security Agency. Even so, subsection (c) expressly states that companies may share cyber threat information or defensive measures with the Department of

Defense and the National Security Agency if they are authorized to do so by another applicable law or regulation.

Subsection (d)

Before sharing, non-Federal entities must, under the requirements of subsection (d), take reasonable efforts to review cyber threat indicators and defensive measures for any personal information or information identifying a specific person that does not directly relate to a cyber threat. If cyber threat indicators or defensive measures contain that kind of information, non-Federal entities must take reasonable efforts to remove the information before sharing. Subsection (d) also permits non-Federal entities to use cyber threat indicators and defensive measures to monitor or operate defensive measures on their own networks and the networks of other non-Federal entities that have consented to the operation of the defensive measures.

In addition, subsection (d) permits state and local governments to use cyber threat indicators for certain law enforcement purposes; the subsection also exempts those shared cyber threat indicators from state and local disclosure laws.

Section 4: Sharing of cyber threat indicators and defensive measures with appropriate Federal entities other than the Department of Defense or the National Security Agency

Subsection (a)

Subsection (a) of this section amends Title I of the National Security Act of 1947, as amended by Section 2 of the Act, to add a subsection (b) to the newly created Section 111. The new subsection requires the President to develop and submit to Congress policies and procedures for the receipt of cyber threat indicators and defensive measures by the Federal Government. Those policies and procedures must ensure that, when an appropriate Federal entity other than the Department of Defense or the National Security Agency receives a cyber threat indicator under Section 3 of the Act, that Federal entity shares the cyber threat indicator in real time with all other appropriate Federal entities, including all relevant components of those other appropriate Federal entities. Among other things, the procedures must also ensure that additional Federal entities beyond the appropriate Federal entities receive cyber threat indicators when those indicators are relevant.

Subsection (b)

Subsection (b) of this section requires the Attorney General, in consultation with the heads of other appropriate Federal entities, to develop and periodically review privacy and civil liberties guidelines. The Attorney General guidelines will govern the receipt, retention, use, and dissemination of cyber threat indicators obtained by the Federal Government under the Act. The guidelines must also establish, among other things: a process for the prompt destruction of any personal information or information identifying a specific person that does not directly relate to a cyber threat; specific limitations on the length of time for which a cyber threat indicator can be retained; and a process to inform recipients of cyber threat indicators that the indicators may only be used for cyberse-

curity purposes. The Attorney General must submit an interim version of the guidelines to Congress within 90 days of the enactment of the Act and a final version within 180 days.

Subsection (c)

Subsection (c) of this section further amends Title I of the National Security Act of 1947 by inserting a new Section 119B. That new section establishes the Cyber Threat Intelligence Integration Center (CTIIC) within the Office of the Director of National Intelligence. Section 119B also lays out the missions of the CTIIC and imposes certain limitations regarding the center's personnel and location.

Subsection (d)

Subsection (d) of this section states that the act of sharing a cyber threat indicator with the Federal Government does not constitute a waiver of any applicable privilege or protection provided by law. The subsection also establishes that cyber threat indicators shared with the Federal Government remain the proprietary information of the sharing non-Federal entity, are exempt from federal disclosure laws, and do not constitute ex parte communications in a judicial or regulatory proceeding.

Additionally, subsection (d) lays out the purposes for which the Federal Government may use a cyber threat indicator it receives from a non-Federal entity under the Act. The Federal Government may use shared cyber threat indicators solely for: a cybersecurity purpose; preventing or prosecuting a threat of death or seriously bodily harm or an offense arising out of such a threat; preventing or prosecuting a serious threat to a minor, including sexual exploitation; or preventing or prosecuting espionage, economic espionage, serious violent felonies, and violations of the Computer Fraud and Abuse Act.

Section 5: Federal Government liability for violations of privacy and civil liberties

Section 5 creates a private cause of action against the Federal Government if a department or agency intentionally or willfully violates the privacy and civil liberties guidelines issued by the Attorney General under Section 4(b) of the Act. The section also establishes statutory damages for a violation of the Attorney General guidelines, provides for reasonable attorney fees for injured persons, specifies the possible venues for an action, and creates a statute of limitations for the new cause of action. Lastly, Section 5 clarifies that this cause of action is the exclusive means available to a complainant seeking a remedy for a violation of the Act by a department or agency of the Federal Government.

Section 6: Protection from liability

This section states that no cause of action shall lie or be maintained in any court against any private entity acting in good faith for the monitoring of an information system or information under Section 3(a) of the Act or for the sharing or receipt of cyber threat indicators or defensive measures under Section 3(c) of the Act. Section 6 nonetheless states that nothing shall be construed to require the dismissal of a cause of action against a non-Federal entity that

has engaged in willful misconduct in the course of conducting activities authorized by the Act. Section 6 also defines the term “willful misconduct” for the purposes of the section and establishes the standard by which a plaintiff may prove willful misconduct.

Section 7: Oversight of Government activities

Subsection (a) of this section further amends Section 111 of the National Security Act of 1947, as created by the Act, to require a biennial report by the Director of National Intelligence, in consultation with the heads of other appropriate Federal entities, on the implementation of the Act.

Subsection (b) of this section requires two reports on privacy liberties. First, subsection (b) requires the Privacy and Civil Liberties Oversight Board to submit to Congress a biennial report on the privacy and civil liberties impact of the Act. Second, subsection (b) requires the Inspectors General of certain appropriate Federal entities, in consultation with the Council of Inspectors General on Financial Oversight, to jointly submit a biennial report to Congress on the receipt, use, and dissemination of cyber threat indicators shared with the Federal Government under the Act.

Both these reports would be made publicly available.

Section 8: Report on cybersecurity threats

This section requires the Director of National Intelligence, in consultation with the heads of appropriate elements of the Intelligence Community, to submit a report to the congressional intelligence committees on cybersecurity threats, including cyberattacks, theft, and data breaches. The report shall be submitted in unclassified form, and must be made publicly available, but may contain a classified annex.

Section 9: Construction and preemption

Section 9 contains a variety of construction and preemption provisions to clarify the scope of the Act. Among other things, these provisions make clear that nothing in the Act authorizes the Department of Defense or any element of the Intelligence Community, including the National Security Agency, to target a person for surveillance. The provisions also state that nothing in the Act shall be construed to limit or modify any existing information-sharing relationships outside of the Act or prohibit any new information-sharing relationships outside of the Act.

The preemption provision of Section 9 expressly supersedes any provision of state or local law that may restrict or otherwise expressly regulate an activity authorized under the Act. The intent of this provision is to preempt state and local laws or regulations that may restrict the sharing of cyber threat indicators as authorized by the Act. The provision is not intended to preempt state and local laws that may encourage or require sharing outside of the Act, including state and local regulations and rules protecting critical infrastructure information or risk assessments concerning critical infrastructure.

Section 10: Conforming amendments

This section contains conforming amendments to Section 552(b) of title 5, United States Code.

Section 11: Definitions

Section 11 provides definitions for a number of key terms used in the Act. These definitions—in particular, the definitions of the terms “cybersecurity purpose,” “cyber threat,” “cyber threat indicator,” and “defensive measure”—narrowly cabin the scope and breadth of the Act.

OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held multiple closed hearings and briefings on the classified intelligence programs affected by H.R. 1560. The Committee also held an open hearing on March 19, 2015, “The Growing Cyber Threat and its Impact on American Business.”

In previous Congresses, the Committee also held numerous closed hearings and briefings on cyber threats. In addition, the Committee held several open hearings on cyber threats in past Congresses, including, “Cybersecurity Threats: The Way Forward,” on November 20, 2014, and “Advanced Cyber Threats Facing Our Nation,” on February 14, 2013.

The bill, as reported by the Committee, reflects conclusions reached by the Committee in light of this oversight activity.

GENERAL PERFORMANCE GOALS AND OBJECTIVES

The goal and objective of H.R. 1560 is to improve cybersecurity in the United States by providing clear legal authority for the sharing of information about cybersecurity threats between and among non-Federal entities and the Federal Government.

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandates Reform Act, P.L. 104–4) requires a statement of whether the provisions of the reported bill include unfunded mandates. In compliance with this requirement, the Committee has received a letter from the Congressional Budget Office included herein.

STATEMENT ON CONGRESSIONAL EARMARKS

Pursuant to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee states that the bill as reported contains no congressional earmarks, limited tax benefits, or limited tariff benefits.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

With respect to clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 1560 from the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 13, 2015.

Hon. DEVIN NUNES,
*Chairman, Permanent Select Committee on Intelligence,
House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1560, the Protecting Cyber Networks Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 1560—Protecting Cyber Networks Act

Summary: H.R. 1560 would establish within the Office of the Director of National Intelligence (ODNI) a center that would be responsible for analyzing and integrating information from the intelligence community related to cyber threats. In addition, the bill would require the government to establish procedures for sharing information and data on cyber threats between the federal government and nonfederal entities. CBO estimates that implementing the bill would cost \$186 million over the 2016–2020 period, assuming appropriation of the estimated amounts.

In addition, the bill would allow information shared with the government to be used in certain criminal prosecutions, which could increase federal revenues from fines as well as direct spending from the Crime Victims Fund. However, CBO anticipates that the number of cases that could be affected would be small and that any additional revenues and spending would be insignificant. Finally, section 5 of H.R. 1560 would make the government liable if an agency or department were to violate the privacy and civil liberty guidelines required by the bill. While such liability could result in additional direct spending, CBO does not have sufficient basis to estimate the type or frequency of violations or budgetary impact that might occur if the legislation was enacted. Because the bill would affect direct spending and revenues, pay-as-you-go procedure apply.

H.R. 1560 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use cyber threat information. Doing so would prevent public and private entities from seeking compensation for damages from those protected entities if they share or use cybersecurity information. The bill also would impose additional intergovernmental mandates on state and local governments by preempting disclosure and liability laws and by preempting any laws that restrict activities authorized by the bill.

Because of uncertainty about the number of cases that would be limited and any foregone compensation that would result from compensatory damages that might otherwise go to private-sector enti-

ties, CBO cannot determine whether the costs of the mandate would exceed the annual thresholds established in UMRA for private-sector mandates (\$154 million in 2015, adjusted annually for inflation). The amount of cybersecurity information shared by state, local, and tribal governments is much smaller than that shared by the private sector, and public entities are much less likely to bring lawsuits as plaintiffs in such cases. Consequently, CBO estimates that the aggregate costs of the mandates on public entities would fall below the threshold for intergovernmental mandates (\$77 million in 2015, adjusted annually for inflation).

Estimated cost to the Federal Government: The estimated budgetary effect of H.R. 1560 is shown in the following table. The costs of this legislation fall within budget function 050 (national defense).

	By fiscal year, in millions of dollars—					
	2016	2017	2018	2019	2020	2016–2020
National Cyber Threat Intelligence and Integration Center:						
Estimated Authorization Level	35	36	37	38	39	185
Estimated Outlays	23	33	35	37	38	166
Oversight, Administration, and Reporting:						
Estimated Authorization Level	4	4	4	4	4	20
Estimated Outlays	4	4	4	4	4	20
Total Changes:						
Estimated Authorization Level	39	40	41	42	43	205
Estimated Outlays	27	37	39	41	42	186

Basis of estimate: For this estimate, CBO assumes that the legislation will be enacted near the end of fiscal year 2015, and that outlays will be similar to historical spending patterns for similar activities.

National Cyber Threat Intelligence and Integration Center

The bill would establish a National Cyber Threat Intelligence Integration Center (CTIIC) that would be responsible for analyzing, integrating, and disseminating intelligence on cyber threats within the federal government. In February, based on authority in current law to establish intelligence centers, the President announced his intention to establish a CTIIC within the ODNI; however, the process for establishing and creating an operational center has not been completed. H.R. 1560 would require such a center to have a maximum of 50 permanent positions. CBO estimates, based on publicly available information regarding the planned center, the personnel ceiling in H.R. 1560, and budget data from the Office of Management and Budget (OMB), that implementing this provision would cost approximately \$166 million over the 2016–2020 period, assuming appropriation of the estimated amounts.

Oversight, administration, and reporting

H.R. 1560 also would require the government to establish procedures to be followed when information on cyber threats is shared between the government and nonfederal entities, such as requiring personal data to be expunged from shared information. The bill also would require the government to audit the process for sharing information with nonfederal entities and would require additional reports to the Congress on cyber intelligence sharing. CBO antici-

pates that approximately 20 additional personnel would be needed to administer the program, prepare the required reports, and manage the exchange of information between the government and non-federal entities (such as state, local, and tribal governments and private companies). Based on information from the Department of Homeland Security, OMB, and other cybersecurity experts, CBO estimates that the requirements imposed by H.R. 1560 would cost approximately \$20 million over the 2016–2020 period, assuming appropriation of the estimated amounts.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. Enacting H.R. 1560 would affect direct spending and revenues because the bill would allow information shared with the government to be used in investigating and prosecuting certain violent crimes. Any additional convictions that result could increase the collection of fines. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent. CBO expects that additional revenues and direct spending would not be significant because of the small number of cases likely to be effected.

In addition, section 5 of H.R. 1560 would allow a person to collect damages and attorney’s fees if a federal agency or department violates the privacy and civil liberty guidelines required to be issued under the bill. Any costs to the federal government for such cases would constitute direct spending. However, because the types of violations and the frequency with which they might occur would depend on guidelines that have not yet been established, CBO does not have a sufficient basis to estimate the effect of this provision.

Intergovernmental and private-sector impact: H.R. 1560 would impose intergovernmental and private-sector mandates as defined in UMRA, by extending civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use cyber threat information. Doing so would prevent public and private entities from seeking compensation for damages from those protected entities for sharing or using cybersecurity information. The bill also would impose additional intergovernmental mandates on state and local governments by preempting disclosure and liability laws and by preempting any laws that restrict the cybersecurity monitoring, sharing, and countermeasure activities authorized by the bill.

Because of uncertainty about the number of cases that would be limited and any foregone compensation that would result from compensatory damages that might otherwise go to private-sector entities, CBO cannot determine whether the costs of the mandate would exceed the annual thresholds established in UMRA for private-sector mandates (\$154 million in 2015, adjusted annually for inflation). The amount of cybersecurity information shared by state, local, and tribal governments is much smaller than that shared by the private sector, and public entities are much less likely to bring lawsuits as plaintiffs in such cases. Consequently, CBO estimates that the aggregate costs of the mandates on public entities would fall below the threshold for intergovernmental mandates (\$77 million in 2015, adjusted annually for inflation).

Estimate prepared by: Federal costs: Jason Wheelock; Impact on state, local, and tribal governments: Jon Sperl; Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Theresa Gullo, Assistant Director for Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in *italics*, and existing law in which no change is proposed is shown in roman):

NATIONAL SECURITY ACT OF 1947

SHORT TITLE

That this Act may be cited as the “National Security Act of 1947”.

TABLE OF CONTENTS

*	*	*	*	*	*	*
TITLE I—COORDINATION FOR NATIONAL SECURITY						
*	*	*	*	*	*	*
Sec. 111. <i>Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.</i>						
*	*	*	*	*	*	*
[Sec. 119B. National intelligence centers.]						
Sec. 119B. <i>Cyber Threat Intelligence Integration Center.</i>						
Sec. 119C. <i>National intelligence centers.</i>						
*	*	*	*	*	*	*

TITLE I—COORDINATION FOR NATIONAL SECURITY

*	*	*	*	*	*	*
---	---	---	---	---	---	---

SEC. 111. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT WITH NON-FEDERAL ENTITIES.

(a) **SHARING BY THE FEDERAL GOVERNMENT.**—

(1) **IN GENERAL.**—*Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—*

(A) *the timely sharing of classified cyber threat indicators in the possession of the Federal Government with representatives of relevant non-Federal entities with appropriate security clearances;*

(B) *the timely sharing with relevant non-Federal entities of cyber threat indicators or information in the possession of the Federal Government that may be declassified and shared at an unclassified level; and*

(C) *the sharing with non-Federal entities, if appropriate, of information in the possession of the Federal Government about imminent or ongoing cybersecurity threats to such entities to prevent or mitigate adverse impacts from such cybersecurity threats.*

(2) **DEVELOPMENT OF PROCEDURES.**—*The procedures developed and promulgated under paragraph (1) shall—*

(A) *ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;*

(B) *incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector-specific information sharing and analysis centers;*

(C) *include procedures for notifying non-Federal entities that have received a cyber threat indicator from a Federal entity in accordance with this Act that is known or determined to be in error or in contravention of the requirements of this section, the Protecting Cyber Networks Act, or the amendments made by such Act or another provision of Federal law or policy of such error or contravention;*

(D) *include requirements for Federal entities receiving a cyber threat indicator or defensive measure to implement appropriate security controls to protect against unauthorized access to, or acquisition of, such cyber threat indicator or defensive measure;*

(E) *include procedures that require Federal entities, prior to the sharing of a cyber threat indicator, to—*

(i) *review such cyber threat indicator to assess whether such cyber threat indicator, in contravention of the requirement under section 3(d)(2) of the Protecting Cyber Networks Act, contains any information that such Federal entity knows at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat and remove such information; or*

(ii) *implement a technical capability configured to remove or exclude any personal information of or information identifying a specific person not directly related to a cybersecurity threat; and*

(F) *include procedures to promote the efficient granting of security clearances to appropriate representatives of non-Federal entities.*

(b) **POLICIES AND PROCEDURES FOR SHARING WITH THE APPROPRIATE FEDERAL ENTITIES OTHER THAN THE DEPARTMENT OF DEFENSE OR THE NATIONAL SECURITY AGENCY.**—

(1) **ESTABLISHMENT.**—*The President shall develop and submit to Congress policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.*

(2) **REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.**—*The policies and procedures required under paragraph (1) shall—*

(A) be developed in accordance with the privacy and civil liberties guidelines required under section 4(b) of the Protecting Cyber Networks Act;

(B) ensure that—

(i) a cyber threat indicator shared by a non-Federal entity with an appropriate Federal entity (other than the Department of Defense or any component of the Department, including the National Security Agency) pursuant to section 3 of such Act is shared in real-time with all of the appropriate Federal entities (including all relevant components thereof);

(ii) the sharing of such cyber threat indicator with appropriate Federal entities is not subject to any delay, modification, or any other action without good cause that could impede receipt by all of the appropriate Federal entities; and

(iii) such cyber threat indicator is provided to each other Federal entity to which such cyber threat indicator is relevant; and

(C) ensure there—

(i) is an audit capability; and

(ii) are appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully use a cyber threat indicator or defense measure shared with the Federal Government by a non-Federal entity under the Protecting Cyber Networks Act other than in accordance with this section and such Act.

(c) BIENNIAL REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Not less frequently than once every two years, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall submit to Congress a report concerning the implementation of this section and the Protecting Cyber Networks Act.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by this section and section 4 of the Protecting Cyber Networks Act in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

(B) An assessment of whether the procedures developed under section 3 of such Act comply with the goals described in subparagraphs (A), (B), and (C) of subsection (a)(1).

(C) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this section and such Act.

(D) A review of the type of cyber threat indicators shared with the Federal Government under this section and such Act, including the following:

(i) The degree to which such information may impact the privacy and civil liberties of specific persons.

(ii) A quantitative and qualitative assessment of the impact of the sharing of such cyber threat indicators

with the Federal Government on privacy and civil liberties of specific persons.

(iii) The adequacy of any steps taken by the Federal Government to reduce such impact.

(E) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this section or such Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under this section or section 4 of such Act.

(F) A description of any significant violations of the requirements of this section or such Act by the Federal Government—

(i) an assessment of all reports of officers, employees, and agents of the Federal Government misusing information provided to the Federal Government under the Protecting Cyber Networks Act or this section, without regard to whether the misuse was knowing or wilful; and

(ii) an assessment of all disciplinary actions taken against such officers, employees, and agents.

(G) A summary of the number and type of non-Federal entities that received classified cyber threat indicators from the Federal Government under this section or such Act and an evaluation of the risks and benefits of sharing such cyber threat indicators.

(H) An assessment of any personal information of or information identifying a specific person not directly related to a cybersecurity threat that—

(i) was shared by a non-Federal entity with the Federal Government under this Act in contravention of section 3(d)(2); or

(ii) was shared within the Federal Government under this Act in contravention of the guidelines required by section 4(b).

(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities and processes under this section or such Act.

(4) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(5) PUBLIC AVAILABILITY OF REPORTS.—The Director of National Intelligence shall make publicly available the unclassified portion of each report required by paragraph (1).

(d) DEFINITIONS.—In this section, the terms “appropriate Federal entities”, “cyber threat indicator”, “defensive measure”, “Federal entity”, and “non-Federal entity” have the meaning given such terms in section 11 of the Protecting Cyber Networks Act.

* * * * *

SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION CENTER.

(a) ESTABLISHMENT.—There is within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center.

(b) *DIRECTOR.*—There is a Director of the Cyber Threat Intelligence Integration Center, who shall be the head of the Cyber Threat Intelligence Integration Center, and who shall be appointed by the Director of National Intelligence.

(c) *PRIMARY MISSIONS.*—The Cyber Threat Intelligence Integration Center shall—

(1) 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;

(2) ensure that appropriate departments and agencies have full access to and receive all-source intelligence support needed to execute the cyber threat intelligence activities of such agencies and to perform independent, alternative analyses;

(3) disseminate cyber threat analysis to the President, the appropriate departments and agencies of the Federal Government, and the appropriate committees of Congress;

(4) coordinate cyber threat intelligence activities of the departments and agencies of the Federal Government; and

(5) conduct strategic cyber threat intelligence planning for the Federal Government.

(d) *LIMITATIONS.*—The Cyber Threat Intelligence Integration Center shall—

(1) have not more than 50 permanent positions;

(2) in carrying out the primary missions of the Center described in subsection (c), may not augment staffing through detailees, assignees, or core contractor personnel or enter into any personal services contracts to exceed the limitation under paragraph (1); and

(3) be located in a building owned or operated by an element of the intelligence community as of the date of the enactment of this section.

NATIONAL INTELLIGENCE CENTERS

SEC. [119B.] 119C. (a) *AUTHORITY TO ESTABLISH.*—The Director of National Intelligence may establish one or more national intelligence centers to address intelligence priorities, including, but not limited to, regional issues.

(b) *RESOURCES OF DIRECTORS OF CENTERS.*—(1) The Director of National Intelligence shall ensure that the head of each national intelligence center under subsection (a) has appropriate authority, direction, and control of such center, and of the personnel assigned to such center, to carry out the assigned mission of such center.

(2) The Director of National Intelligence shall ensure that each national intelligence center has appropriate personnel to accomplish effectively the mission of such center.

(c) *INFORMATION SHARING.*—The Director of National Intelligence shall, to the extent appropriate and practicable, ensure that each national intelligence center under subsection (a) and the other elements of the intelligence community share information in order to facilitate the mission of such center.

(d) *MISSION OF CENTERS.*—Pursuant to the direction of the Director of National Intelligence, each national intelligence center under subsection (a) may, in the area of intelligence responsibility assigned to such center—

(1) have primary responsibility for providing all-source analysis of intelligence based upon intelligence gathered both domestically and abroad;

(2) have primary responsibility for identifying and proposing to the Director of National Intelligence intelligence collection and analysis and production requirements; and

(3) perform such other duties as the Director of National Intelligence shall specify.

(e) REVIEW AND MODIFICATION OF CENTERS.—The Director of National Intelligence shall determine on a regular basis whether—

(1) the area of intelligence responsibility assigned to each national intelligence center under subsection (a) continues to meet appropriate intelligence priorities; and

(2) the staffing and management of such center remains appropriate for the accomplishment of the mission of such center.

(f) TERMINATION.—The Director of National Intelligence may terminate any national intelligence center under subsection (a).

(g) SEPARATE BUDGET ACCOUNT.—The Director of National Intelligence shall, as appropriate, include in the National Intelligence Program budget a separate line item for each national intelligence center under subsection (a).

* * * * *

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

* * * * *

TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY

* * * * *

Subtitle F—Privacy and Civil Liberties

SEC. 1061. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.

(a) IN GENERAL.—There is established as an independent agency within the executive branch a Privacy and Civil Liberties Oversight Board (referred to in this section as the “Board”).

(b) FINDINGS.—Consistent with the report of the National Commission on Terrorist Attacks Upon the United States, Congress makes the following findings:

(1) In conducting the war on terrorism, the Government may need additional powers and may need to enhance the use of its existing powers.

(2) This shift of power and authority to the Government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life and to ensure that the Government uses its powers for the purposes for which the powers were given.

(3) The National Commission on Terrorist Attacks Upon the United States correctly concluded that “The choice between se-

curity and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.”.

(c) PURPOSE.—The Board shall—

(1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and

(2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.

(d) FUNCTIONS.—

(1) ADVICE AND COUNSEL ON POLICY DEVELOPMENT AND IMPLEMENTATION.—The Board shall—

(A) review proposed legislation, regulations, and policies related to efforts to protect the Nation from terrorism, including the development and adoption of information sharing guidelines under subsections (d) and (f) of section 1016;

(B) review the implementation of new and existing legislation, regulations, and policies related to efforts to protect the Nation from terrorism, including the implementation of information sharing guidelines under subsections (d) and (f) of section 1016;

(C) advise the President and the departments, agencies, and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of such legislation, regulations, policies, and guidelines; and

(D) in providing advice on proposals to retain or enhance a particular governmental power, consider whether the department, agency, or element of the executive branch has established—

(i) that the need for the power is balanced with the need to protect privacy and civil liberties;

(ii) that there is adequate supervision of the use by the executive branch of the power to ensure protection of privacy and civil liberties; and

(iii) that there are adequate guidelines and oversight to properly confine its use.

(2) OVERSIGHT.—The Board shall continually review—

(A) the regulations, policies, and procedures, and the implementation of the regulations, policies, and procedures, of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected;

(B) the information sharing practices of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to determine whether they appropriately protect privacy and civil liberties and adhere to the information sharing guidelines issued or developed under subsections (d) and (f) of

section 1016 and to other governing laws, regulations, and policies regarding privacy and civil liberties; and

(C) other actions by the executive branch relating to efforts to protect the Nation from terrorism to determine whether such actions—

(i) appropriately protect privacy and civil liberties; and

(ii) are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.

(3) RELATIONSHIP WITH PRIVACY AND CIVIL LIBERTIES OFFICERS.—The Board shall—

(A) receive and review reports and other information from privacy officers and civil liberties officers under section 1062;

(B) when appropriate, make recommendations to such privacy officers and civil liberties officers regarding their activities; and

(C) when appropriate, coordinate the activities of such privacy officers and civil liberties officers on relevant inter-agency matters.

(4) TESTIMONY.—The members of the Board shall appear and testify before Congress upon request.

(e) REPORTS.—

(1) IN GENERAL.—The Board shall—

(A) receive and review reports from privacy officers and civil liberties officers under section 1062; and

(B) periodically submit, not less than semiannually, reports—

(i)(I) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives; and

(II) to the President; and

(ii) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) CONTENTS.—Not less than 2 reports submitted each year under paragraph (1)(B) shall include—

(A) a description of the major activities of the Board during the preceding period;

(B) information on the findings, conclusions, and recommendations of the Board resulting from its advice and oversight functions under subsection (d);

(C) the minority views on any findings, conclusions, and recommendations of the Board resulting from its advice and oversight functions under subsection (d);

(D) each proposal reviewed by the Board under subsection (d)(1) that—

- (i) the Board advised against implementation; and
 - (ii) notwithstanding such advice, actions were taken to implement; and
- (E) for the preceding period, any requests submitted under subsection (g)(1)(D) for the issuance of subpoenas that were modified or denied by the Attorney General.
- (3) *BIENNIAL REPORT ON CERTAIN CYBER ACTIVITIES.*—
- (A) *REPORT REQUIRED.*—*The Privacy and Civil Liberties Oversight Board shall biennially submit to Congress and the President a report containing—*
- (i) *an assessment of the privacy and civil liberties impact of the activities carried out under the Protecting Cyber Networks Act and the amendments made by such Act; and*
 - (ii) *an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 4 of the Protecting Cyber Networks Act and the amendments made by such section 4 in addressing privacy and civil liberties concerns.*
- (B) *RECOMMENDATIONS.*—*Each report submitted under this paragraph may include such recommendations as the Privacy and Civil Liberties Oversight Board may have for improvements or modifications to the authorities under the Protecting Cyber Networks Act or the amendments made by such Act.*
- (C) *FORM.*—*Each report required under this paragraph shall be submitted in unclassified form, but may include a classified annex.*
- (D) *PUBLIC AVAILABILITY OF REPORTS.*—*The Privacy and Civil Liberties Oversight Board shall make publicly available the unclassified portion of each report required by subparagraph (A).*
- (f) *INFORMING THE PUBLIC.*—*The Board shall—*
- (1) *make its reports, including its reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and*
 - (2) *hold public hearings and otherwise inform the public of its activities, as appropriate and in a manner consistent with the protection of classified information and applicable law.*
- (g) *ACCESS TO INFORMATION.*—
- (1) *AUTHORIZATION.*—*If determined by the Board to be necessary to carry out its responsibilities under this section, the Board is authorized to—*
 - (A) *have access from any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element, to all relevant records, reports, audits, reviews, documents, papers, recommendations, or other relevant material, including classified information consistent with applicable law;*
 - (B) *interview, take statements from, or take public testimony from personnel of any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element;*
 - (C) *request information or assistance from any State, tribal, or local government; and*

(D) at the direction of a majority of the members of the Board, submit a written request to the Attorney General of the United States that the Attorney General require, by subpoena, persons (other than departments, agencies, and elements of the executive branch) to produce any relevant information, documents, reports, answers, records, accounts, papers, and other documentary or testimonial evidence.

(2) REVIEW OF SUBPOENA REQUEST.—

(A) IN GENERAL.—Not later than 30 days after the date of receipt of a request by the Board under paragraph (1)(D), the Attorney General shall—

(i) issue the subpoena as requested; or

(ii) provide the Board, in writing, with an explanation of the grounds on which the subpoena request has been modified or denied.

(B) NOTIFICATION.—If a subpoena request is modified or denied under subparagraph (A)(ii), the Attorney General shall, not later than 30 days after the date of that modification or denial, notify the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(3) ENFORCEMENT OF SUBPOENA.—In the case of contumacy or failure to obey a subpoena issued pursuant to paragraph (1)(D), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found may issue an order requiring such person to produce the evidence required by such subpoena.

(4) AGENCY COOPERATION.—Whenever information or assistance requested under subparagraph (A) or (B) of paragraph (1) is, in the judgment of the Board, unreasonably refused or not provided, the Board shall report the circumstances to the head of the department, agency, or element concerned without delay. The head of the department, agency, or element concerned shall ensure that the Board is given access to the information, assistance, material, or personnel the Board determines to be necessary to carry out its functions.

(h) MEMBERSHIP.—

(1) MEMBERS.—The Board shall be composed of a full-time chairman and 4 additional members, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) QUALIFICATIONS.—Members of the Board shall be selected solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience, and without regard to political affiliation, but in no event shall more than 3 members of the Board be members of the same political party. The President shall, before appointing an individual who is not a member of the same political party as the President, consult with the leadership of that party, if any, in the Senate and House of Representatives.

(3) INCOMPATIBLE OFFICE.—An individual appointed to the Board may not, while serving on the Board, be an elected offi-

cial, officer, or employee of the Federal Government, other than in the capacity as a member of the Board.

(4) TERM.—Each member of the Board shall serve a term of 6 years, except that—

(A) a member appointed to a term of office after the commencement of such term may serve under such appointment only for the remainder of such term; and

(B) upon the expiration of the term of office of a member, the member shall continue to serve until the member's successor has been appointed and qualified, except that no member may serve under this subparagraph—

(i) for more than 60 days when Congress is in session unless a nomination to fill the vacancy shall have been submitted to the Senate; or

(ii) after the adjournment sine die of the session of the Senate in which such nomination is submitted.

(5) QUORUM AND MEETINGS.—The Board shall meet upon the call of the chairman or a majority of its members. Three members of the Board shall constitute a quorum.

(i) COMPENSATION AND TRAVEL EXPENSES.—

(1) COMPENSATION.—

(A) CHAIRMAN.—The chairman of the Board shall be compensated at the rate of pay payable for a position at level III of the Executive Schedule under section 5314 of title 5, United States Code.

(B) MEMBERS.—Each member of the Board shall be compensated at a rate of pay payable for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Board.

(2) TRAVEL EXPENSES.—Members of the Board shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for persons employed intermittently by the Government under section 5703(b) of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Board.

(j) STAFF.—

(1) APPOINTMENT AND COMPENSATION.—The chairman of the Board, in accordance with rules agreed upon by the Board, shall appoint and fix the compensation of a full-time executive director and such other personnel as may be necessary to enable the Board to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(2) DETAILEES.—Any Federal employee may be detailed to the Board without reimbursement from the Board, and such detailee shall retain the rights, status, and privileges of the detailee's regular employment without interruption.

(3) CONSULTANT SERVICES.—The Board may procure the temporary or intermittent services of experts and consultants in accordance with section 3109 of title 5, United States Code, at rates that do not exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of such title.

(k) SECURITY CLEARANCES.—

(1) IN GENERAL.—The appropriate departments, agencies, and elements of the executive branch shall cooperate with the Board to expeditiously provide the Board members and staff with appropriate security clearances to the extent possible under existing procedures and requirements.

(2) RULES AND PROCEDURES.—After consultation with the Secretary of Defense, the Attorney General, and the Director of National Intelligence, the Board shall adopt rules and procedures of the Board for physical, communications, computer, document, personnel, and other security relating to carrying out the functions of the Board.

(l) TREATMENT AS AGENCY, NOT AS ADVISORY COMMITTEE.—The Board—

(1) is an agency (as defined in section 551(1) of title 5, United States Code); and

(2) is not an advisory committee (as defined in section 3(2) of the Federal Advisory Committee Act (5 U.S.C. App.)).

(m) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section amounts as follows:

(1) For fiscal year 2008, \$5,000,000.

(2) For fiscal year 2009, \$6,650,000.

(3) For fiscal year 2010, \$8,300,000.

(4) For fiscal year 2011, \$10,000,000.

(5) For fiscal year 2012 and each subsequent fiscal year, such sums as may be necessary.

* * * * *

TITLE 5, UNITED STATES CODE

* * * * *

PART I—THE AGENCIES GENERALLY

* * * * *

CHAPTER 5—ADMINISTRATIVE PROCEDURE

* * * * *

Subchapter II—ADMINISTRATIVE PROCEDURE

* * * * *

§ 552. Public information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public—

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submissions or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection and copying—

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register;

(C) administrative staff manuals and instructions to staff that affect a member of the public;

(D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and

(E) a general index of the records referred to under subparagraph (D);

unless the materials are promptly published and copies offered for sale. For records created on or after November 1, 1996, within one year after such date, each agency shall make such records available, including by computer telecommunications or, if computer telecommunications means have not been established by the agency, by other electronic means. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, staff manual, instruction, or copies of records referred to in subparagraph (D). However, in each case the justification for the deletion shall be explained fully in writing, and the extent of such deletion shall be indicated

on the portion of the record which is made available or published, unless including that indication would harm an interest protected by the exemption in subsection (b) under which the deletion is made. If technically feasible, the extent of the deletion shall be indicated at the place in the record where the deletion was made. Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of such index on request at a cost not to exceed the direct cost of duplication. Each agency shall make the index referred to in subparagraph (E) available by computer telecommunications by December 31, 1999. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if—

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

(3)(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(B) In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.

(C) In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.

(D) For purposes of this paragraph, the term "search" means to review, manually or by automated means, agency records for the purpose of locating those records which are responsive to a request.

(E) An agency, or part of an agency, that is an element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) shall not make any record available under this paragraph to—

(i) any government entity, other than a State, territory, commonwealth, or district of the United States, or any subdivision thereof; or

(ii) a representative of a government entity described in clause (i).

(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(ii) Such agency regulations shall provide that—

(I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;

(II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or non-commercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media; and

(III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.

In this clause, the term “a representative of the news media” means any person or entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. In this clause, the term “news” means information that is about current events or that would be of current interest to the public. Examples of news-media entities are television or radio stations broadcasting to the public at large and publishers of periodicals (but only if such entities qualify as disseminators of “news”) who make their products available for purchase by or subscription by or free distribution to the general public. These examples are not all-inclusive. Moreover, as methods of news delivery evolve (for example, the adoption of the electronic dissemination of newspapers through telecommunications services), such alternative media shall be considered to be news-media entities. A freelance journalist shall be regarded as working for a news-media entity if the journalist can demonstrate a solid basis for expecting publication through that entity, whether or not the journalist is actually employed by the entity. A publication contract would present a solid basis for such an expectation; the Government may also consider the past publication record of the requester in making such a determination.

(iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a

document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section—

(I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or

(II) for any request described in clause (ii) (II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.

(v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed \$250.

(vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

(vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo: Provided, That the court's review of the matter shall be limited to the record before the agency.

(viii) An agency shall not assess search fees (or in the case of a requester described under clause (ii)(II), duplication fees) under this subparagraph if the agency fails to comply with any time limit under paragraph (6), if no unusual or exceptional circumstances (as those terms are defined for purposes of paragraphs (6)(B) and (C), respectively) apply to the processing of the request.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action. In addition to any other matters to which a court accords substantial weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency's determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service upon the defendant of the pleading in which such complaint is made, unless the court otherwise directs for good cause shown.

(E)(i) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(ii) For purposes of this subparagraph, a complainant has substantially prevailed if the complainant has obtained relief through either—

(I) a judicial order, or an enforceable written agreement or consent decree; or

(II) a voluntary or unilateral change in position by the agency, if the complainant's claim is not insubstantial.

(F)(i) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Special Counsel recommends.

(ii) The Attorney General shall—

(I) notify the Special Counsel of each civil action described under the first sentence of clause (i); and

(II) annually submit a report to Congress on the number of such civil actions in the preceding year.

(iii) The Special Counsel shall annually submit a report to Congress on the actions taken by the Special Counsel under clause (i).

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall—

(i) determine within 20 days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.

The 20-day period under clause (i) shall commence on the date on which the request is first received by the appropriate component of the agency, but in any event not later than ten days after the request is first received by any component of the agency that is des-

ignated in the agency's regulations under this section to receive requests under this section. The 20-day period shall not be tolled by the agency except—

(I) that the agency may make one request to the requester for information and toll the 20-day period while it is awaiting such information that it has reasonably requested from the requester under this section; or

(II) if necessary to clarify with the requester issues regarding fee assessment. In either case, the agency's receipt of the requester's response to the agency's request for information or clarification ends the tolling period.

(B)(i) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the unusual circumstances for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days, except as provided in clause (ii) of this subparagraph.

(ii) With respect to a request for which a written notice under clause (i) extends the time limits prescribed under clause (i) of subparagraph (A), the agency shall notify the person making the request if the request cannot be processed within the time limit specified in that clause and shall provide the person an opportunity to limit the scope of the request so that it may be processed within that time limit or an opportunity to arrange with the agency an alternative time frame for processing the request or a modified request. Refusal by the person to reasonably modify the request or arrange such an alternative time frame shall be considered as a factor in determining whether exceptional circumstances exist for purposes of subparagraph (C). To aid the requester, each agency shall make available its FOIA Public Liaison, who shall assist in the resolution of any disputes between the requester and the agency.

(iii) As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular requests—

(I) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;

(II) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or

(III) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject-matter interest therein.

(iv) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for the aggregation of certain requests by the same requestor, or by a group of requestors acting in concert, if the agency reasonably believes that such requests actually constitute a single request, which would otherwise satisfy the unusual circumstances specified in this subparagraph,

and the requests involve clearly related matters. Multiple requests involving unrelated matters shall not be aggregated.

(C)(i) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(ii) For purposes of this subparagraph, the term “exceptional circumstances” does not include a delay that results from a predictable agency workload of requests under this section, unless the agency demonstrates reasonable progress in reducing its backlog of pending requests.

(iii) Refusal by a person to reasonably modify the scope of a request or arrange an alternative time frame for processing a request (or a modified request) under clause (ii) after being given an opportunity to do so by the agency to whom the person made the request shall be considered as a factor in determining whether exceptional circumstances exist for purposes of this subparagraph.

(D)(i) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for multitrack processing of requests for records based on the amount of work or time (or both) involved in processing requests.

(ii) Regulations under this subparagraph may provide a person making a request that does not qualify for the fastest multitrack processing an opportunity to limit the scope of the request in order to qualify for faster processing.

(iii) This subparagraph shall not be considered to affect the requirement under subparagraph (C) to exercise due diligence.

(E)(i) Each agency shall promulgate regulations, pursuant to notice and receipt of public comment, providing for expedited processing of requests for records—

(I) in cases in which the person requesting the records demonstrates a compelling need; and

(II) in other cases determined by the agency.

(ii) Notwithstanding clause (i), regulations under this subparagraph must ensure—

(I) that a determination of whether to provide expedited processing shall be made, and notice of the determination shall be provided to the person making the request, within 10 days after the date of the request; and

(II) expeditious consideration of administrative appeals of such determinations of whether to provide expedited processing.

(iii) An agency shall process as soon as practicable any request for records to which the agency has granted expedited processing under this subparagraph. Agency action to deny or affirm denial of

a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review under paragraph (4), except that the judicial review shall be based on the record before the agency at the time of the determination.

(iv) A district court of the United States shall not have jurisdiction to review an agency denial of expedited processing of a request for records after the agency has provided a complete response to the request.

(v) For purposes of this subparagraph, the term “compelling need” means—

(I) that a failure to obtain requested records on an expedited basis under this paragraph could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(II) with respect to a request made by a person primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged Federal Government activity.

(vi) A demonstration of a compelling need by a person making a request for expedited processing shall be made by a statement certified by such person to be true and correct to the best of such person’s knowledge and belief.

(F) In denying a request for records, in whole or in part, an agency shall make a reasonable effort to estimate the volume of any requested matter the provision of which is denied, and shall provide any such estimate to the person making the request, unless providing such estimate would harm an interest protected by the exemption in subsection (b) pursuant to which the denial is made.

(7) Each agency shall—

(A) establish a system to assign an individualized tracking number for each request received that will take longer than ten days to process and provide to each person making a request the tracking number assigned to the request; and

(B) establish a telephone line or Internet service that provides information about the status of a request to the person making the request using the assigned tracking number, including—

(i) the date on which the agency originally received the request; and

(ii) an estimated date on which the agency will complete action on the request.

(b) This section does not apply to matters that are—

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute—

(A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or

(ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and

(B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; **[or]**

(9) geological and geophysical information and data, including maps, concerning **[wells.] wells; or**

(10) *information shared with or provided to the Federal Government pursuant to the Protecting Cyber Networks Act or the amendments made by such Act.*

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted, and the exemption under which the deletion is made, shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted, and the exemption under which the deletion is made, shall be indicated at the place in the record where such deletion is made.

(c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and—

(A) the investigation or proceeding involves a possible violation of criminal law; and

(B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) dis-

closure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.

(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.

(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

(d) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

(e)(1) On or before February 1 of each year, each agency shall submit to the Attorney General of the United States a report which shall cover the preceding fiscal year and which shall include—

(A) the number of determinations made by the agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;

(B)(i) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information; and

(ii) a complete list of all statutes that the agency relies upon to authorize the agency to withhold information under subsection (b)(3), the number of occasions on which each statute was relied upon, a description of whether a court has upheld the decision of the agency to withhold information under each such statute, and a concise description of the scope of any information withheld;

(C) the number of requests for records pending before the agency as of September 30 of the preceding year, and the median and average number of days that such requests had been pending before the agency as of that date;

(D) the number of requests for records received by the agency and the number of requests which the agency processed;

(E) the median number of days taken by the agency to process different types of requests, based on the date on which the requests were received by the agency;

(F) the average number of days for the agency to respond to a request beginning on the date on which the request was received by the agency, the median number of days for the agency to respond to such requests, and the range in number of days for the agency to respond to such requests;

(G) based on the number of business days that have elapsed since each request was originally received by the agency—

- (i) the number of requests for records to which the agency has responded with a determination within a period up to and including 20 days, and in 20-day increments up to and including 200 days;
 - (ii) the number of requests for records to which the agency has responded with a determination within a period greater than 200 days and less than 301 days;
 - (iii) the number of requests for records to which the agency has responded with a determination within a period greater than 300 days and less than 401 days; and
 - (iv) the number of requests for records to which the agency has responded with a determination within a period greater than 400 days;
- (H) the average number of days for the agency to provide the granted information beginning on the date on which the request was originally filed, the median number of days for the agency to provide the granted information, and the range in number of days for the agency to provide the granted information;
- (I) the median and average number of days for the agency to respond to administrative appeals based on the date on which the appeals originally were received by the agency, the highest number of business days taken by the agency to respond to an administrative appeal, and the lowest number of business days taken by the agency to respond to an administrative appeal;
- (J) data on the 10 active requests with the earliest filing dates pending at each agency, including the amount of time that has elapsed since each request was originally received by the agency;
- (K) data on the 10 active administrative appeals with the earliest filing dates pending before the agency as of September 30 of the preceding year, including the number of business days that have elapsed since the requests were originally received by the agency;
- (L) the number of expedited review requests that are granted and denied, the average and median number of days for adjudicating expedited review requests, and the number adjudicated within the required 10 days;
- (M) the number of fee waiver requests that are granted and denied, and the average and median number of days for adjudicating fee waiver determinations;
- (N) the total amount of fees collected by the agency for processing requests; and
- (O) the number of full-time staff of the agency devoted to processing requests for records under this section, and the total amount expended by the agency for processing such requests.
- (2) Information in each report submitted under paragraph (1) shall be expressed in terms of each principal component of the agency and for the agency overall.
- (3) Each agency shall make each such report available to the public including by computer telecommunications, or if computer telecommunications means have not been established by the agency, by other electronic means. In addition, each agency shall make

the raw statistical data used in its reports available electronically to the public upon request.

(4) The Attorney General of the United States shall make each report which has been made available by electronic means available at a single electronic access point. The Attorney General of the United States shall notify the Chairman and ranking minority member of the Committee on Government Reform and Oversight of the House of Representatives and the Chairman and ranking minority member of the Committees on Governmental Affairs and the Judiciary of the Senate, no later than April 1 of the year in which each such report is issued, that such reports are available by electronic means.

(5) The Attorney General of the United States, in consultation with the Director of the Office of Management and Budget, shall develop reporting and performance guidelines in connection with reports required by this subsection by October 1, 1997, and may establish additional requirements for such reports as the Attorney General determines may be useful.

(6) The Attorney General of the United States shall submit an annual report on or before April 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subparagraphs (E), (F), and (G) of subsection (a)(4). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.

(f) For purposes of this section, the term—

(1) “agency” as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

(2) “record” and any other term used in this section in reference to information includes—

(A) any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format; and

(B) any information described under subparagraph (A) that is maintained for an agency by an entity under Government contract, for the purposes of records management.

(g) The head of each agency shall prepare and make publicly available upon request, reference material or a guide for requesting records or information from the agency, subject to the exemptions in subsection (b), including—

(1) an index of all major information systems of the agency;

(2) a description of major information and record locator systems maintained by the agency; and

(3) a handbook for obtaining various types and categories of public information from the agency pursuant to chapter 35 of title 44, and under this section.

(h)(1) There is established the Office of Government Information Services within the National Archives and Records Administration.

(2) The Office of Government Information Services shall—

(A) review policies and procedures of administrative agencies under this section;

(B) review compliance with this section by administrative agencies; and

(C) recommend policy changes to Congress and the President to improve the administration of this section.

(3) The Office of Government Information Services shall offer mediation services to resolve disputes between persons making requests under this section and administrative agencies as a non-exclusive alternative to litigation and, at the discretion of the Office, may issue advisory opinions if mediation has not resolved the dispute.

(i) The Government Accountability Office shall conduct audits of administrative agencies on the implementation of this section and issue reports detailing the results of such audits.

(j) Each agency shall designate a Chief FOIA Officer who shall be a senior official of such agency (at the Assistant Secretary or equivalent level).

(k) The Chief FOIA Officer of each agency shall, subject to the authority of the head of the agency—

(1) have agency-wide responsibility for efficient and appropriate compliance with this section;

(2) monitor implementation of this section throughout the agency and keep the head of the agency, the chief legal officer of the agency, and the Attorney General appropriately informed of the agency's performance in implementing this section;

(3) recommend to the head of the agency such adjustments to agency practices, policies, personnel, and funding as may be necessary to improve its implementation of this section;

(4) review and report to the Attorney General, through the head of the agency, at such times and in such formats as the Attorney General may direct, on the agency's performance in implementing this section;

(5) facilitate public understanding of the purposes of the statutory exemptions of this section by including concise descriptions of the exemptions in both the agency's handbook issued under subsection (g), and the agency's annual report on this section, and by providing an overview, where appropriate, of certain general categories of agency records to which those exemptions apply; and

(6) designate one or more FOIA Public Liaisons.

(l) FOIA Public Liaisons shall report to the agency Chief FOIA Officer and shall serve as supervisory officials to whom a requester under this section can raise concerns about the service the requester has received from the FOIA Requester Center, following an initial response from the FOIA Requester Center Staff. FOIA Public Liaisons shall be responsible for assisting in reducing delays, increasing transparency and understanding of the status of requests, and assisting in the resolution of disputes.

* * * * *

DISCLOSURE OF DIRECTED RULE MAKING

H.R. 1560 does not specifically direct any rule makings within the meaning of 5 U.S.C. 551.

DUPLICATION OF FEDERAL PROGRAMS

H.R. 1560 does not duplicate or reauthorize an established program of the Federal Government that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111-139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

BOB GOODLATTE, Virginia
CHAIRMAN

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR G. SMITH, Texas
STEVE CHABOT, Ohio
DARRILL E. ISSA, California
J. RALPH ABRAHAM, Virginia
STEVE KING, Iowa
THOMAS PRINCE, Arizona
LOUIE GOMBERG, Texas
JIM JOHNSON, Ohio
ERIC LITZ, Texas
JASON CHAFFETZ, Utah
TED CRUZ, Texas
TERRY GOWDY, South Carolina
PAUL B. LABRADOR, Idaho
OLIVER PEARSON, Texas
DOUG COLLINS, Georgia
RONDANIEL FORTIS, Florida
MIKE WALTERS, California
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
DAVE TROTT, Michigan
MARK BURNETT, Michigan

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBLURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-3951
<http://www.house.gov/judiciary>

April 7, 2015

JOHN CONYERS, JR., Michigan
RANKING MEMBER

JERROLD RAOULERS, New York
ZOE LORING, California
SHELIA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "BOB" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
RODNY CHIR, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
GEORGE J. RICHMOND, Louisiana
SUZANNE R. RUBINE, Washington
HAKEEM S. JEFFRIES, New York
DAVID COULSON, Illinois
SCOTT PETERS, California

The Honorable Devin Nunes
Chairman
House Permanent Select Committee on Intelligence
HVC-304
Washington, DC 20515

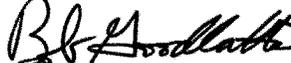
Dear Mr. Chairman Nunes,

I am writing concerning H.R. 1560, the "Protecting Cyber Networks Act," which your Committee ordered reported on March 26, 2015.

As you know, H.R. 1560 contains provisions within the Committee on the Judiciary's Rule X jurisdiction. As a result of your having consulted with the Committee and in order to expedite the House's consideration of H.R. 1560, the Committee on the Judiciary will not assert a jurisdictional claim over this bill by seeking a sequential referral. However, this is conditional on our mutual understanding and agreement that doing so will in no way diminish or alter the jurisdiction of the Committee on the Judiciary with respect to the appointment of conferees or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation.

I would appreciate your response to this letter confirming this understanding, and would request that you include a copy of this letter and your response in the Committee Report and in the *Congressional Record* during the floor consideration of this bill. Thank you in advance for your cooperation.

Sincerely,


Bob Goodlatte
Chairman

cc: The Honorable John Boehner, Speaker
The Honorable John Conyers
The Honorable Adam Schiff
The Honorable Thomas J. Wickham, Jr., Parliamentarian

Devin Nunes, California, Chairman
 Jeff Miller, Florida
 K. Michael Conaway, Texas
 Peter T. King, New York
 Frank A. Loufaro, New Jersey
 Lynn A. Westerman, Georgia
 Thomas J. Rosaway, Florida
 Joseph P. Heck, Nevada
 Mike B. Pompeo, Kansas
 Neena Rao, Louisiana, Florida
 Michael R. Turner, Ohio
 Brad R. Vener, Ohio
 Chris Stewart, Utah
 Adam B. Schiff, California,
 Ranking Member
 Luis W. Gohmert, Texas
 James A. Hoyer, Connecticut
 Tom A. Graves, Virginia
 Andy Cuccinelli, Virginia
 Jackie Speier, California
 Mike Conaway, Texas
 Eric Swalwell, California
 Patrick E. Murphy, Florida
 John A. Boehner, Speaker of the House
 Nancy Pelosi, Democratic Leader

U.S. HOUSE OF REPRESENTATIVES
 PERMANENT SELECT COMMITTEE
 ON INTELLIGENCE

HVC-304, THE CAPITOL
 WASHINGTON, DC 20515
 (202) 225-4121
 JEFF BRUNER,
 Staff Director
 MICHAEL BISHOP,
 Majority Staff Director

April 10, 2015

The Honorable Bob Goodlatte
 Chairman
 U.S. House Committee on the Judiciary
 2138 Rayburn House Office Building
 Washington, DC 20515

Dear Chairman Goodlatte:

Thank you for your letter regarding H.R. 1560, the Protecting Cyber Networks Act. As you noted, certain provisions of the bill fall within the jurisdiction of the Committee on the Judiciary. As you also noted, the language of those provisions was the result of consultations with you in advance of the Permanent Select Committee on Intelligence's consideration of the bill. I agree that your letter in no way diminishes or alters the jurisdiction of the Committee on the Judiciary with respect to the appointment of conferees or to any future jurisdictional claim over the subject matters contained in the bill or any similar legislation.

I appreciate your willingness to forego consideration of the bill in the interest of expediting this legislation for floor consideration. I will include a copy of your letter and this response in our Committee's report on H.R. 1560 and the Congressional Record during consideration of the legislation on the House floor. Thank you for your assistance with this matter.

Sincerely,


 Devin Nunes
 Chairman

JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5061
<http://oversight.house.gov>

April 13, 2015

The Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
HVC-304, The Capitol
Washington, DC 20515

Dear Mr. Chairman:

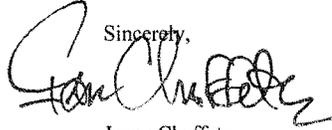
On March 26, 2015, the Permanent Select Committee on Intelligence ordered H.R. 1560, the Protecting Cyber Networks Act reported to the House. Thank you for consulting with the Committee on Oversight and Government Reform with regard to H.R. 1560 on those matters within the Committee's jurisdiction. I am writing to confirm our mutual understanding with respect to the consideration of the bill.

The bill contains provisions that fall within the Rule X subject matter jurisdiction of the Committee on Oversight and Government Reform. The Committee has purview over the Freedom of Information Act (FOIA, 5 U.S.C. 552), which H.R. 1560 directly amends. Section 10 of the bill directly amends 5 U.S.C. 552 to create a new 5 U.S.C. 552(b) provision that exempts the entire Act from FOIA, including any subsequent amendments. Prior to floor consideration, we will work together to remove section 10 and consider improvements to other sections of the bill referencing 5 U.S.C. 552.

In the interest of expediting the House's consideration of H.R. 1560, I will not request a sequential referral of the bill. However, I do so only with the understanding that this procedural route will not be construed to prejudice the Committee on Oversight and Government Reform's jurisdictional interest and prerogatives on this bill or any other similar legislation and will not be considered as precedent for consideration of matters of jurisdictional interest to my Committee in the future.

I respectfully request your support for the appointment of outside conferees from the Committee on Oversight and Government Reform should this bill or a similar bill be considered in a conference with the Senate. I also request that you include our exchange of letters on this matter in the Committee Report on H.R. 1560 and in the *Congressional Record* during consideration of this bill on the House floor. Thank you for your attention to these matters.

Sincerely,

A handwritten signature in black ink, appearing to read "Jason Chaffetz", written over a faint, larger version of the same signature.

Jason Chaffetz
Chairman

cc: The Honorable John Boehner, Speaker
The Honorable Elijah E. Cummings
The Honorable Adam B. Schiff
The Honorable Thomas J. Wickham, Parliamentarian

Devin Nunes, California, Co-Chairman

Jeff Miller, Florida
K. Michael Conaway, Texas
Peter T. King, New York
Frank A. LoBiondo, New Jersey
Lynn A. Westmoreland, Georgia
Thomson J. Ross, Florida
Joseph J. Heck, Nevada
Mike R. Pompeo, Kansas
Rousselle LaHinton, Florida
Michael H. Turner, Ohio
Bob H. Workman, Ohio
Chris Stewart, Utah

Jason B. Schiff, California
Patience M. Miller, Michigan

Luis V. Gohmert, Texas
James A. Harris, Connecticut
Terry A. Sewell, Alabama
Andie Elchert, Indiana
Jackie Spier, California
Mike Gable, Illinois
Eric Swalwell, California
Patrick E. Murphy, Florida

John A. Boehner, Speaker of the House
Nancy Pelosi, Democratic Leader

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

HVC-304, THE CAPITOL
WASHINGTON, DC 20515
(202) 225-4121

JEFF BRIDGES
STAFF DIRECTOR

MICHAEL BOONE
MANAGING STAFF DIRECTOR

April 13, 2015

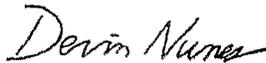
The Honorable Jason Chaffetz
Chairman
U.S. House Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Chaffetz:

Thank you for your letter regarding H.R. 1560, the Protecting Cyber Networks Act. As you noted, certain provisions of the bill related to 5 U.S.C. § 552 fall within the jurisdiction of the Committee on Oversight and Government Reform. As you also noted, we have agreed to continue to work with you on these provisions. I agree that your letter in no way diminishes or alters the jurisdiction of the Committee on Oversight and Government Reform with respect to the appointment of conferees or to any future jurisdictional claim over the subject matters contained in the bill or any similar legislation.

I appreciate your willingness to forego consideration of the bill in the interest of expediting this legislation for floor consideration. I will include a copy of your letter and this response in our Committee's report on H.R. 1560 and the Congressional Record during consideration of the legislation on the House floor. Thank you for your assistance with this matter.

Sincerely,



Devin Nunes
Chairman

