

CYBER INTELLIGENCE SHARING AND PROTECTION ACT

APRIL 15, 2013.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. ROGERS of Michigan, from the Permanent Select Committee on Intelligence, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 624]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, 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.**

This Act may be cited as the “Cyber Intelligence Sharing and Protection Act”.

**SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION SHARING.**

(a) **IN GENERAL.**—Title XI of the National Security Act of 1947 (50 U.S.C. 442 et seq.) is amended by adding at the end the following new section:

“CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

“SEC. 1104. (a) **INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR AND UTILITIES.**—

“(1) **IN GENERAL.**—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and utilities and to encourage the sharing of such intelligence.

“(2) **SHARING AND USE OF CLASSIFIED INTELLIGENCE.**—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—

- “(A) shared by an element of the intelligence community with—
    - “(i) a certified entity; or
    - “(ii) a person with an appropriate security clearance to receive such cyber threat intelligence;
  - “(B) shared consistent with the need to protect the national security of the United States; and
  - “(C) used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.
- “(3) SECURITY CLEARANCE APPROVALS.—The Director of National Intelligence shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection—
- “(A) grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity;
  - “(B) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and
  - “(C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.
- “(4) NO RIGHT OR BENEFIT.—The provision of information to a private-sector entity or a utility under this subsection shall not create a right or benefit to similar information by such entity or such utility or any other private-sector entity or utility.
- “(5) RESTRICTION ON DISCLOSURE OF CYBER THREAT INTELLIGENCE.—Notwithstanding any other provision of law, a certified entity receiving cyber threat intelligence pursuant to this subsection shall not further disclose such cyber threat intelligence to another entity, other than to a certified entity or other appropriate agency or department of the Federal Government authorized to receive such cyber threat intelligence.
- “(b) USE OF CYBERSECURITY SYSTEMS AND SHARING OF CYBER THREAT INFORMATION.—
- “(1) IN GENERAL.—
- “(A) CYBERSECURITY PROVIDERS.—Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes—
    - “(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and
    - “(ii) share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.
  - “(B) SELF-PROTECTED ENTITIES.—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—
    - “(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and
    - “(ii) share such cyber threat information with any other entity, including the Federal Government.
- “(2) SHARING WITH THE FEDERAL GOVERNMENT.—
- “(A) INFORMATION SHARED WITH THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER OF THE DEPARTMENT OF HOMELAND SECURITY.—Subject to the use and protection of information requirements under paragraph (3), the head of a department or agency of the Federal Government receiving cyber threat information in accordance with paragraph (1) shall provide such cyber threat information in as close to real time as possible to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security.
  - “(B) REQUEST TO SHARE WITH ANOTHER DEPARTMENT OR AGENCY OF THE FEDERAL GOVERNMENT.—An entity sharing cyber threat information that is provided to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security under subparagraph (A) or paragraph (1) may request the head of such Center to, and the head of such Center may, provide such information in as close to real time as possible to another department or agency of the Federal Government.
- “(3) USE AND PROTECTION OF INFORMATION.—Cyber threat information shared in accordance with paragraph (1)—
- “(A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected en-

tity authorizing such sharing, including appropriate anonymization or minimization of such information and excluding limiting a department or agency of the Federal Government from sharing such information with another department or agency of the Federal Government in accordance with this section;

“(B) may not be used by an entity to gain an unfair competitive advantage to the detriment of the protected entity or the self-protected entity authorizing the sharing of information;

“(C) may only be used by a non-Federal recipient of such information for a cybersecurity purpose;

“(D) if shared with the Federal Government—

“(i) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly known as the ‘Freedom of Information Act’);

“(ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information;

“(iii) shall not be used by the Federal Government for regulatory purposes;

“(iv) shall not be provided by the department or agency of the Federal Government receiving such cyber threat information to another department or agency of the Federal Government under paragraph (2)(A) if—

“(I) the entity providing such information determines that the provision of such information will undermine the purpose for which such information is shared; or

“(II) unless otherwise directed by the President, the head of the department or agency of the Federal Government receiving such cyber threat information determines that the provision of such information will undermine the purpose for which such information is shared; and

“(v) shall be handled by the Federal Government consistent with the need to protect sources and methods and the national security of the United States; and

“(E) shall be exempt from disclosure under a State, local, or tribal law or regulation that requires public disclosure of information by a public or quasi-public entity.

“(4) EXEMPTION FROM LIABILITY.—

“(A) EXEMPTION.—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith—

“(i) for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or

“(ii) for decisions made for cybersecurity purposes and based on cyber threat information identified, obtained, or shared under this section.

“(B) LACK OF GOOD FAITH.—For purposes of the exemption from liability under subparagraph (A), a lack of good faith includes, but is not limited to, any act or omission taken with intent to injure, defraud, or otherwise endanger any individual, government entity, private entity, or utility.

“(5) RELATIONSHIP TO OTHER LAWS REQUIRING THE DISCLOSURE OF INFORMATION.—The submission of information under this subsection to the Federal Government shall not satisfy or affect—

“(A) any requirement under any other provision of law for a person or entity to provide information to the Federal Government; or

“(B) the applicability of other provisions of law, including section 552 of title 5, United States Code (commonly known as the ‘Freedom of Information Act’), with respect to information required to be provided to the Federal Government under such other provision of law.

“(6) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide new authority to—

“(A) a cybersecurity provider to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes; or

“(B) a self-protected entity to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by such self-protected entity.

“(c) FEDERAL GOVERNMENT USE OF INFORMATION.—

“(1) LIMITATION.—The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection (b)—

“(A) for cybersecurity purposes;

“(B) for the investigation and prosecution of cybersecurity crimes;

“(C) for the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger of death or serious bodily harm; or

“(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking and the investigation and prosecution of crimes involving child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking, and any crime referred to in section 2258A(a)(2) of title 18, United States Code.

“(2) AFFIRMATIVE SEARCH RESTRICTION.—The Federal Government may not affirmatively search cyber threat information shared with the Federal Government under subsection (b) for a purpose other than a purpose referred to in paragraph (1).

“(3) ANTI-TASKING RESTRICTION.—Nothing in this section shall be construed to permit the Federal Government to—

“(A) require a private-sector entity or utility to share information with the Federal Government; or

“(B) condition the sharing of cyber threat intelligence with a private-sector entity or utility on the provision of cyber threat information to the Federal Government.

“(4) PROTECTION OF SENSITIVE PERSONAL DOCUMENTS.—The Federal Government may not use the following information, containing information that identifies a person, shared with the Federal Government in accordance with subsection (b) unless such information is used in accordance with the policies and procedures established under paragraph (7):

“(A) Library circulation records.

“(B) Library patron lists.

“(C) Book sales records.

“(D) Book customer lists.

“(E) Firearms sales records.

“(F) Tax return records.

“(G) Educational records.

“(H) Medical records.

“(5) NOTIFICATION OF NON-CYBER THREAT INFORMATION.—If a department or agency of the Federal Government receiving information pursuant to subsection (b)(1) determines that such information is not cyber threat information, such department or agency shall notify the entity or provider sharing such information pursuant to subsection (b)(1).

“(6) RETENTION AND USE OF CYBER THREAT INFORMATION.—No department or agency of the Federal Government shall retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

“(7) PRIVACY AND CIVIL LIBERTIES.—

“(A) POLICIES AND PROCEDURES.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security and the Attorney General, shall establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the Federal Government in accordance with subsection (b)(1). Such policies and procedures shall, consistent with the need to protect systems and networks from cyber threats and mitigate cyber threats in a timely manner—

“(i) minimize the impact on privacy and civil liberties;

“(ii) reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is not necessary to protect systems or networks from cyber threats or mitigate cyber threats in a timely manner;

“(iii) include requirements to safeguard non-publicly available cyber threat information that may be used to identify specific persons from unauthorized access or acquisition;

“(iv) protect the confidentiality of cyber threat information associated with specific persons to the greatest extent practicable; and

“(v) not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

“(B) SUBMISSION TO CONGRESS.—The Director of National Intelligence shall, consistent with the need to protect sources and methods, submit to Congress the policies and procedures required under subparagraph (A) and any updates to such policies and procedures.

“(C) IMPLEMENTATION.—The head of each department or agency of the Federal Government receiving cyber threat information shared with the Federal Government under subsection (b)(1) shall—

“(i) implement the policies and procedures established under subparagraph (A); and

“(ii) promptly notify the Director of National Intelligence, the Attorney General, and the congressional intelligence committees of any significant violations of such policies and procedures.

“(D) OVERSIGHT.—The Director of National Intelligence, in consultation with the Attorney General, the Secretary of Homeland Security, and the Secretary of Defense, shall establish a program to monitor and oversee compliance with the policies and procedures established under subparagraph (A).

“(d) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF RESTRICTIONS ON THE DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED INFORMATION.—

“(1) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates subsection (b)(3)(D) or subsection (c) with respect to the disclosure, use, or protection of voluntarily shared cyber threat information shared under this section, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

“(A) the actual damages sustained by the person as a result of the violation or \$1,000, whichever is greater; and

“(B) the costs of the action together with reasonable attorney fees as determined by the court.

“(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

“(A) the district in which the complainant resides;

“(B) the district in which the principal place of business of the complainant is located;

“(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

“(D) the District of Columbia.

“(3) 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 subsection (b)(3)(D) or subsection (c) that is the basis for the action.

“(4) 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 of subsection (b)(3)(D) or subsection (c).

“(e) REPORTS ON INFORMATION SHARING.—

“(1) INSPECTOR GENERAL REPORT.—The Inspector General of the Intelligence Community, in consultation with the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Privacy and Civil Liberties Oversight Board, shall annually submit to the congressional intelligence committees a report containing a review of the use of information shared with the Federal Government under this section, including—

“(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;

“(B) a review of the type of information shared with the Federal Government under this section;

“(C) a review of the actions taken by the Federal Government based on such information;

“(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any;

“(E) a list of the departments or agencies receiving such information;

“(F) a review of the sharing of such information within the Federal Government to identify inappropriate stovepiping of shared information; and

“(G) any recommendations of the Inspector General for improvements or modifications to the authorities under this section.

“(2) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Civil Liberties Protection Officer of the Office of the Director of National Intelligence and the

Chief Privacy and Civil Liberties Officer of the Department of Justice, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Intelligence Community, and the senior privacy and civil liberties officer of each department or agency of the Federal Government that receives cyber threat information shared with the Federal Government under this section, shall annually and jointly submit to Congress a report assessing the privacy and civil liberties impact of the activities conducted by the Federal Government under this section. Such report shall include any recommendations the Civil Liberties Protection Officer and Chief Privacy and Civil Liberties Officer consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat information under this section.

“(3) FORM.—Each report required under paragraph (1) or (2) shall be submitted in unclassified form, but may include a classified annex.

“(f) FEDERAL PREEMPTION.—This section supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under subsection (b).

“(g) SAVINGS CLAUSES.—

“(1) EXISTING AUTHORITIES.—Nothing in this section shall be construed to limit any other authority to use a cybersecurity system or to identify, obtain, or share cyber threat intelligence or cyber threat information.

“(2) LIMITATION ON MILITARY AND INTELLIGENCE COMMUNITY INVOLVEMENT IN PRIVATE AND PUBLIC SECTOR CYBERSECURITY EFFORTS.—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, the Department of Defense or the National Security Agency or any other element of the intelligence community to control, modify, require, or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.

“(3) INFORMATION SHARING RELATIONSHIPS.—Nothing in this section shall be construed to—

“(A) limit or modify an existing information sharing relationship;

“(B) prohibit a new information sharing relationship;

“(C) require a new information sharing relationship between the Federal Government and a private-sector entity or utility;

“(D) modify the authority of a department or agency of the Federal Government to protect sources and methods and the national security of the United States; or

“(E) preclude the Federal Government from requiring an entity to report significant cyber incidents if authorized or required to do so under another provision of law.

“(4) LIMITATION ON FEDERAL GOVERNMENT USE OF CYBERSECURITY SYSTEMS.—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, any entity to use a cybersecurity system owned or controlled by the Federal Government on a private-sector system or network to protect such private-sector system or network.

“(5) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this section shall be construed to subject a protected entity, self-protected entity, cyber security provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, to liability for choosing not to engage in the voluntary activities authorized under this section.

“(6) USE AND RETENTION OF INFORMATION.—Nothing in this section shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

“(h) DEFINITIONS.—In this section:

“(1) AVAILABILITY.—The term ‘availability’ means ensuring timely and reliable access to and use of information.

“(2) CERTIFIED ENTITY.—The term ‘certified entity’ means a protected entity, self-protected entity, or cybersecurity provider that—

“(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

“(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence.

“(3) CONFIDENTIALITY.—The term ‘confidentiality’ means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

“(4) CYBER THREAT INFORMATION.—

“(A) IN GENERAL.—The term ‘cyber threat information’ means information directly pertaining to—

“(i) a vulnerability of a system or network of a government or private entity or utility;

“(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

“(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

“(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

“(B) EXCLUSION.—Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

“(5) CYBER THREAT INTELLIGENCE.—

“(A) IN GENERAL.—The term ‘cyber threat intelligence’ means intelligence in the possession of an element of the intelligence community directly pertaining to—

“(i) a vulnerability of a system or network of a government or private entity or utility;

“(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

“(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

“(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

“(B) EXCLUSION.—Such term does not include intelligence pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

“(6) CYBERSECURITY CRIME.—The term ‘cybersecurity crime’ means—

“(A) a crime under a Federal or State law that involves—

“(i) efforts to deny access to or degrade, disrupt, or destroy a system or network;

“(ii) efforts to gain unauthorized access to a system or network; or

“(iii) efforts to exfiltrate information from a system or network without authorization; or

“(B) the violation of a provision of Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, created or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99-474).

“(7) CYBERSECURITY PROVIDER.—The term ‘cybersecurity provider’ means a non-Federal entity that provides goods or services intended to be used for cybersecurity purposes.

“(8) CYBERSECURITY PURPOSE.—

“(A) IN GENERAL.—The term ‘cybersecurity purpose’ means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

“(i) a vulnerability of a system or network;

“(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

“(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

“(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

“(B) EXCLUSION.—Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such sys-

tem or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

**“(9) CYBERSECURITY SYSTEM.—**

**“(A) IN GENERAL.—**The term ‘cybersecurity system’ means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

“(i) a vulnerability of a system or network;

“(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

“(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

“(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

**“(B) EXCLUSION.—**Such term does not include a system designed or employed to protect a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

**“(10) INTEGRITY.—**The term ‘integrity’ means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

**“(11) PROTECTED ENTITY.—**The term ‘protected entity’ means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.

**“(12) SELF-PROTECTED ENTITY.—**The term ‘self-protected entity’ means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.

**“(13) UTILITY.—**The term ‘utility’ means an entity providing essential services (other than law enforcement or regulatory services), including electricity, natural gas, propane, telecommunications, transportation, water, or wastewater services.”.

**(b) PROCEDURES AND GUIDELINES.—**The Director of National Intelligence shall—

(1) not later than 60 days after the date of the enactment of this Act, establish procedures under paragraph (1) of section 1104(a) of the National Security Act of 1947, as added by subsection (a) of this section, and issue guidelines under paragraph (3) of such section 1104(a);

(2) in establishing such procedures and issuing such guidelines, consult with the Secretary of Homeland Security to ensure that such procedures and such guidelines permit the owners and operators of critical infrastructure to receive all appropriate cyber threat intelligence (as defined in section 1104(h)(5) of such Act, as added by subsection (a)) in the possession of the Federal Government; and

(3) following the establishment of such procedures and the issuance of such guidelines, expeditiously distribute such procedures and such guidelines to appropriate departments and agencies of the Federal Government, private-sector entities, and utilities (as defined in section 1104(h)(13) of such Act, as added by subsection (a)).

**(c) PRIVACY AND CIVIL LIBERTIES POLICIES AND PROCEDURES.—**Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Secretary of Homeland Security and the Attorney General, shall establish the policies and procedures required under section 1104(c)(7)(A) of the National Security Act of 1947, as added by subsection (a) of this section.

**(d) INITIAL REPORTS.—**The first reports required to be submitted under paragraphs (1) and (2) of subsection (e) of section 1104 of the National Security Act of 1947, as added by subsection (a) of this section, shall be submitted not later than 1 year after the date of the enactment of this Act.

**(e) TABLE OF CONTENTS AMENDMENT.—**The table of contents in the first section of the National Security Act of 1947 is amended by adding at the end the following new item:

“Sec. 1104. Cyber threat intelligence and information sharing.”.

**SEC. 3. SUNSET.**

Effective on the date that is 5 years after the date of the enactment of this Act—



- (1) section 1104 of the National Security Act of 1947, as added by section 2(a) of this Act, is repealed; and
- (2) the table of contents in the first section of the National Security Act of 1947, as amended by section 2(e) of this Act, is amended by striking the item relating to section 1104, as added by such section 2(e).

#### PURPOSE

The purpose of H.R. 624 is to provide for the sharing of certain cyber threat intelligence and cyber threat information between the Intelligence Community and cybersecurity entities, and other purposes.

#### BACKGROUND AND NEED FOR LEGISLATION

##### *112th Congress*

At the beginning of the 112th Congress, the Committee, under the direction of Chairman Rogers and Ranking Member Ruppberger, began a bipartisan effort to examine the issue of cybersecurity.<sup>1</sup> The goal of this effort was to better understand the threats facing the nation in cyberspace—with respect to both the government and in the private sector—and to determine what the Intelligence Community could do to help better protect the nation. The results of this review were stunning: a number of advanced nation-state actors are actively engaged in a series of wide-ranging, aggressive efforts to penetrate American computer systems and networks; these efforts extend well beyond government networks, and reach deep into nearly every sector of the American economy, including companies serving critical infrastructure needs.

Perhaps most troubling, these efforts are targeted not only at sensitive national security and infrastructure information but are also often aimed at stealing corporate research and development information that forms the very lifeblood of the American economy. China, in particular, is engaged in an extensive, day-in, day-out effort to pillage American intellectual property. There can be no question that in today's modern world, economic security is national security and the government must help the private sector to protect itself.

The Committee's review also revealed that while the government is already doing much to provide support and assistance to the private sector to address this threat, in particular through DHS and the FBI, more can and should be done in the immediate future. In particular, the Committee determined that the Intelligence Community is currently in possession of tremendously valuable intelligence and strategic insights derived from its extensive overseas

---

<sup>1</sup>This effort involved a series of briefings and hearings, including one open hearing, to inform Committee members and, where possible, the public, about the serious national security threat posed by nation-state actors and other adversaries in the cyber realm. These meetings, briefings, and hearings were in turn supported by numerous meetings and briefings conducted by Committee staff with agencies and individuals from the Executive Branch including, among others, the White House, the Department of Homeland Security (DHS), the Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), including the National Security Agency (NSA), and with experts from the academic and think-tank communities. The Committee staff also held numerous meetings with private sector companies and trade groups in industries including technology, telecommunications, financial services, utilities, aerospace, and defense. And the Committee staff met with representatives of privacy and civil liberties organizations including the Center for Democracy and Technology, the American Civil Liberties Union, the Electronic Frontier Foundation, and the CATO Institute, among others. In total, the Committee members and staff met with dozens of organizations in conducting its review over a seven-month period.

intelligence collection efforts that can and should be provided—in both classified and unclassified form (when possible)—to the private sector to help the owners and operators of the vast majority of America’s information infrastructure better protect themselves. The Committee believes that the Defense Industrial Base Opt-in Pilot project (“DIB Pilot”), which has now transitioned to the DIB Enhanced Cybersecurity Services (DECS) program, is a good model for demonstrating how sensitive government threat intelligence can be shared with the private sector in an operationally usable manner. Under the DECS, the government provides classified threat intelligence to key Internet Service Providers, who use the information to protect a limited number of companies in the defense industrial base, all on a voluntary basis. This program is being expanded to non-DIB American companies under DECS program, although the effort’s progress has been slow. The Committee believes that the clear legal authorities in this bill could have eliminated much of that delay.

The Committee’s review also determined that while much cybersecurity monitoring and threat information sharing takes place today within the private sector, real and perceived legal barriers to such efforts substantially hamper the efforts of even those in the private sector with the best of intentions. The Committee determined that these issues are best resolved by providing clear, positive authority to permit the monitoring—by the private sector—of privately-owned and operated networks and systems for the purpose of detecting and mitigating cybersecurity threats and to permit the voluntary sharing of information about those threats and vulnerabilities with others, including entities within the private sector and with the federal government.

While some have suggested that the private sector needs more regulation or that the government should directly help defend certain portions of the private sector, the Committee’s view is that the protection of the private sector is best left in private hands and before reaching for a regulatory “stick”, the government should provide as much intelligence as possible, in usable form, to better enable voluntary private sector efforts. In the view of the Committee, such an approach—voluntary, private sector defense of private sector systems and networks informed by government intelligence information—best protects individual privacy and takes advantage of the natural incentives built into our economic system, including harnessing private sector drive and innovation.

The Committee’s review revealed that America’s cyber infrastructure is distressingly vulnerable to espionage and attacks by nation-states and others with advanced capabilities.

### *113th Congress*

The Committee has continued its oversight of the advanced cyber threats facing the nation, as well as the ongoing efforts to protect our nation and our economy from these dangerous threats. The Committee focused in particular on the state of cyber threat information sharing between the U.S. government and private sector, as well as cyber information sharing within the private sector. The threat from advanced nation state cyber actors, like China and Iran, has only grown since the Committee first began its review in the 112th Congress. As the Committee continued its work in the

113th Congress a series of high profile press revelations concerning Chinese government cyber economic espionage directed against American companies and institutions, including major newspapers, added impetus to our work. Further emphasis was added by press revelations of state-sponsored cyber distributed denial of service (DDoS) attacks against major American financial institutions.

The Committee believes that immediate and serious action is necessary to staunch the bleeding of American intellectual capital and to better protect our national security. In particular, the Committee believes that the Intelligence Community must take immediate and decisive action to provide intelligence to the private sector to help it better protect itself. In turn, the private sector must act aggressively to better monitor its own systems and to share information—both within the private sector and with the federal government. The Committee recognizes that because it focused on the issues within its jurisdiction, this legislation does not address many of the other issues facing the nation with respect to cybersecurity. At the same time, however, the Committee firmly believes that this legislation is an important first step in the effort to better protect the nation from advanced cyber threat actors.

#### *Evolution of Legislation*

Following Committee consideration of H.R. 3523 in the 112th Congress, several improvements and changes were made to the legislation. Many of those changes were an attempt to address perceived privacy and civil liberties deficiencies and are detailed below. The bill passed the House of Representatives in April, 2012 by a wide bipartisan vote of 248–168. However, neither it nor a companion bill moved in the Senate before the 112th Congress ended. Since that time, the Committee has maintained an open dialogue with the Administration, Members of Congress and private sector entities, and has actively sought to discuss constructive changes to the language in H.R. 624 that would help allay privacy fears without comprising the purpose of the bill.

On February 13, 2013, Chairman Rogers and Ranking Member Ruppertsberger introduced H.R. 624 in the same form H.R. 3523 passed the House during the 112th Congress. That bill included the various changes to the language that were adopted in an attempt to address privacy and civil liberties concerns and served as a starting point for additional modifications and improvements in the 113th Congress.

Following introduction, the Committee held an open hearing on February 14, 2013 to examine advanced cyber threats facing our nation. The witnesses for the hearing were Governor John Engler, the former three-term governor of Michigan and currently the President of the Business Roundtable; Mr. Ken DeFontes, the President and CEO of Baltimore Gas & Electric; Mr. Paul Smocer, the President of BITS, the technology policy division of the Financial Services Roundtable; and Mr. Kevin Mandia, the CEO of MANDIANT Corporation. The hearing largely focused on the state of cyber threat information sharing between the U.S. government and private sector, as well as cyber information sharing within the private sector.

The Committee considered and favorably reported H.R. 624 on April 10, 2013 with amendments by a bipartisan vote of 18–2.

Many of the amendments were based on further dialogue with the private sector, the Administration, and privacy and civil liberties advocates. As discussed below, the most notable amendments to the bill during Committee consideration were designed to further clarify the authorities in response to privacy and civil liberties concerns.

#### *Privacy and Civil Liberties*

The Committee has made changes to this legislation at every step in the process starting prior to introduction in the 112th Congress through the Committee markup in the 113th Congress to address privacy and civil liberties concerns. The following illustrates extensive changes made to address privacy and civil liberties concerns the bill has undergone since the Committee last favorably reported the bill.

#### *112th Congress*

1. Changes to the definitions.—The definitions for several key provisions in the bill were modified and more narrowly crafted to ensure that the legislation works to permit the sharing of the types of information necessary to detect protect against the cyber threat and to remain adaptable to new technology and new intrusion methods over time.

2. Limits on Government Use.—Throughout the process, the Government's use of information share by the private sector has been an issue of concern for some and it is an area that has been repeatedly clarified in a way to not impede the Government's use of cyber threat information to address the cyber threat.

3. IG Provision.—A provision was added that requires the Intelligence Community Inspector General to conduct a review of activities authorized under the bill and provide a report to Congress.

4. Federal Government Liability.—A private right of action against the Federal Government was added to the bill to provide federal liability for intentional or willful violations of the use or information protection provisions, including damages and costs.

5. Government minimization procedures.—The bill was originally silent on government minimization, but a floor amendment during the 112th Congress provided the authority for the Federal Government to adopt minimization procedures, but did not require such.

#### *113th Congress*

During Committee consideration of H.R. 624 several provisions were added to further clarify the existing language and add adopted language in response to privacy and civil liberties concerns raised with the Committee.

1. Government Minimization.—Mr. Himes offered and the Committee adopted an amendment that would require the government to establish procedures that minimize the impact on privacy and civil liberties, reasonably limit the receipt, retention, use and disclosure of cyber threat information that is associated with specific persons that is not necessary to protect systems or networks from cyber threats in a timely manner. The procedures include requirements to safeguard from unauthorized access and protect the confidentiality of such information non-publicly available cyber threat information that could be used to identify specific persons. Impor-

tantly, however, the procedures must be designed in a way so as not to delay or impede the flow of cyber threat information necessary to defend against a cyber threat. It is critical that the correct balance be struck between creating procedures that protect any personally identifying information and ensuring that cyber threat information critical to securing our networks from cyber intrusion can move in as close to real time as possible to and between federal agencies. The amendment also included provisions designed to oversee and report compliance with the procedures.

2. National Security Purpose.—Ms. Sewell offered and the Committee adopted an amendment that would strike the “national security purpose” use from the list of five permissible uses of shared cyberthreat information by the Federal Government. When CISPA was considered on the House Floor during the 112th Congress, language was adopted that limited the Federal Government’s use of cyberthreat information shared by the private sector under the bill to five areas: (1) cybersecurity purposes; (2) investigation and prosecution of cybersecurity crimes; (3) the protection of individuals from bodily harm; (4) the protection of minors from child pornography and exploitation; and (5) to protect the national security of the United States. The “national security use” restriction was created to give the government flexibility moving forward and ensure the bill remained technology neutral. However, many opponents of the bill interpreted this as an avenue for the Federal Government to do anything it wanted with information received under the guise of national security. The Committee strongly disagrees with both this interpretation of the bill and the insinuation that the Federal Government would use “national security” as a catch-all for otherwise impermissible uses of information.

Given the concerns, however, the Committee voted to remove the “national security purpose” use in the interest of moving the core, critical authorities provided in the legislation forward. We recognize that this may mean that the authorities have to be revisited sooner than they might have before, but in the interest of moving forward adopted the amendment.

3. Limitation on Private Sector Use.—Mr. Heck and Mr. Himes offered and the Committee adopted an amendment that would limit the use of cyberthreat information shared with and in the private sector by the recipients of such information to “cybersecurity purposes.” It is and has been the intent of the Committee that the information shared under these authorities could be used by the private sector to better secure their networks. However, in response to concerns about the private sector selling consumer information for marketing purposes and other non cybersecurity purposes, this amendment was adopted to clarify this point in the text of the legislation.

4. Oversight and Reporting.—Mr. Thompson offered and the Committee adopted an amendment that would enhance the Intelligence Community Inspector General review and reporting requirement already contained in the bill by adding a requirement to consult with the DOD and DOJ Inspectors General, as well as the Privacy and Civil Liberties Oversight Board (PCLOB). It would also add a new report by senior privacy and civil liberties officers. Mr. Thompson’s amendment will provide even more oversight and accountability within the federal government, for the activities au-

thorized under this bill. The Committee is mindful of the reporting burden on the Intelligence Community, but also recognizes the concern with ensuring the government is appropriately handling and using cyberthreat information obtained under this legislation.

#### COMMITTEE CONSIDERATION AND ROLLCALL VOTES

On April 10, 2013, the Committee met in open and closed session and ordered the bill H.R. 624 favorably reported, as amended.

#### OPEN SESSION

In open session, the Committee considered the text of the bill H.R. 624.

Chairman Rogers offered an amendment. The amendment clarified limitations that could be placed on information shared with the Federal Government, requires sharing within the Federal Government in as close to real time as possible, clarifies that this legislation does not affect other requirements in law to report cyber incidents, and made various technical changes. The amendment also provided clarification to the legislation's liability protection provision. Mr. Schiff offered a modification to the amendment, which was agreed to by unanimous consent. The amendment, as modified, was agreed to by voice vote.

Mr. Thompson offered an amendment, which amended a provision requiring an annual report by the Inspector General of the Intelligence Community (ICIG) reviewing the use of cyber threat information provided to the government pursuant to the bill. It required the ICIG to consult with the Inspectors General of the Justice and Defense Departments, as well as the Privacy and Civil Liberties Oversight Board. Additionally, the amendment creates a new review and report by senior privacy and civil liberties officers. The amendment was agreed to by voice vote.

Mr. Langevin offered an amendment that would make clear that none of the authorities in the bill could be construed to permit a cybersecurity provider or self protected entity to "hack back" into others' systems under the authority to identify and obtain cyberthreats on its own systems or the systems its operating on with consent. The amendment was agreed to by voice vote.

Mr. Heck offered an amendment on behalf of himself and Mr. Himes. The amendment would limit the private sector's use of cyber threat information received under the authorities in the bill to cybersecurity purposes. The amendment was agreed to by voice vote.

Mr. Himes offered an amendment that would require the government to establish procedures governing the receipt, retention, use and disclosure of non-publicly available cyber threat information shared with the Federal Government. It would also require the Director of National Intelligence to establish a program to monitor and report compliance with the procedures. The amendment was agreed to by voice vote.

Ms. Sewell offered an amendment that would strike "national security purpose" from the enumerated list of permissible government uses under (c)(1). There was a motion to conduct a portion of debate in closed session, which was agreed to by recorded vote of 21 ayes to 0 noes.

Voting Aye: Mr. Rogers (Chairman), Mr. Thornberry, Mr. Miller, Mr. Conaway, Mr. King, Mr. LoBiondo, Mr. Nunes, Mr. Westmoreland, Mrs. Bachmann, Mr. Rooney, Mr. Heck, Mr. Pompeo, Mr. Ruppertsberger, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Schiff, Mr. Gutierrez, Mr. Pastor, Mr. Himes, Ms. Sewell.

Voting No: None.

The Committee returned to open session. The amendment was agreed to by voice vote.

Ms. Schakowsky offered an amendment that would remove the Department of Defense, the National Security Agency, the Army, the Navy, the Air Force, the Marine Corps and the Coast Guard from the term "Federal Government" as set forth in (b)(1)(B)(ii). The amendment was not agreed to by a voted of 14 noes to 5 ayes.

Voting Aye: Ms. Schakowsky, Mr. Schiff, Mr. Pastor, Mr. Himes, Ms. Sewell.

Voting No: Mr. Rogers (Chairman), Mr. Miller, Mr. Conaway, Mr. King, Mr. LoBiondo, Mr. Nunes, Mr. Westmoreland, Mrs. Bachmann, Mr. Rooney, Mr. Heck, Mr. Pompeo, Mr. Ruppertsberger, Mr. Thompson, Mr. Langevin.

Ms. Schakowsky offered an amendment that would require the President to designate an officer who shall establish policies and procedures governing the retention, use, and disclosure of communications, records, system traffic, or other information associated with specific persons by officers, employees and agents of the Federal Government in accordance with this section, and would establish annual reviews of such. The amendment was not agreed to by a voted of 16 noes to 3 ayes.

Voting Aye: Ms. Schakowsky, Mr. Schiff, Mr. Pastor.

Voting No: Mr. Rogers (Chairman), Mr. Miller, Mr. Conaway, Mr. King, Mr. LoBiondo, Mr. Nunes, Mr. Westmoreland, Mrs. Bachmann, Mr. Rooney, Mr. Heck, Mr. Pompeo, Mr. Ruppertsberger, Mr. Thompson, Mr. Langevin, Mr. Himes, Ms. Sewell.

Ms. Schakowsky offered an amendment that would amend the Exemption from Liability provision in (b)(4). The amendment was not agreed to by a voted of 16 noes to 4 ayes.

Voting Aye: Ms. Schakowsky, Mr. Schiff, Mr. Pastor, Mr. Himes.

Voting No: Mr. Rogers (Chairman), Mr. Thornberry, Mr. Miller, Mr. Conaway, Mr. King, Mr. LoBiondo, Mr. Nunes, Mr. Westmoreland, Mrs. Bachmann, Mr. Rooney, Mr. Heck, Mr. Pompeo, Mr. Ruppertsberger, Mr. Thompson, Mr. Langevin, Ms. Sewell.

Mr. Schiff offered an amendment that would require the private sector to take reasonable efforts to remove any information that could identify a specific person from cyber threat information shared. The amendment was not agreed to by a vote of 16 noes to 4 ayes.

Voting Aye: Ms. Schakowsky, Mr. Schiff, Mr. Pastor, Mr. Himes.

Voting No: Mr. Rogers (Chairman), Mr. Thornberry, Mr. Miller, Mr. Conaway, Mr. King, Mr. LoBiondo, Mr. Nunes, Mr. Westmoreland, Mrs. Bachmann, Mr. Rooney, Mr. Heck, Mr. Pompeo, Mr. Ruppersberger, Mr. Thompson, Mr. Langevin, Ms. Sewell.

The Committee then adopted a motion by the Chairman to favorably report the bill H.R. 624 to the House, as amended. The motion was agreed to by a record vote of 18 ayes to 2 noes:

Voting Aye: Mr. Rogers (Chairman), Mr. Thornberry, Mr. Miller, Mr. Conaway, Mr. King, Mr. LoBiondo, Mr. Nunes, Mr. Westmoreland, Mrs. Bachmann, Mr. Rooney, Mr. Heck, Mr. Pompeo, Mr. Ruppersberger, Mr. Thompson, Mr. Langevin, Mr. Pastor, Mr. Himes, Ms. Sewell.

Voting No: Ms. Schakowsky and Mr. Schiff.

## SECTION-BY-SECTION ANALYSIS AND EXPLANATION

### SECTION 1. SHORT TITLE

The short title of the Act is the Cyber Intelligence Sharing and Protection Act.

### SECTION 2. CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

#### *Section 2(a): In General*

This subsection of the Act amends Title XI of the National Security Act of 1947 by adding a new section, Section 1104.

#### Section 1104(a) of Title 50: Intelligence Community Sharing of Cyber Threat Intelligence with Private Sector

Subsection (a) of new Section 1104 provides for the sharing of cyber threat intelligence—both classified and unclassified—by elements of the Intelligence Community with entities in the private sector. It is the view of the Committee that the routine and fulsome sharing of such intelligence information with appropriate cleared entities and individuals within the private sector is critically important to protecting the nation from advanced cyber threats. It is critical that as much information as possible be shared at machine-speed, in real-time, and in a manner that the information—whether classified or not—is operationally usable by entities within the private sector.

This subsection seeks to set forth a general framework and requires the establishment of specific procedures and guidelines to make such sharing happen in the immediate future and to make it continue so long as the nation faces this significant threat to our national security. The Committee intends to engage in vigorous oversight of the Intelligence Community use of the authorities under this section and, in particular, the Office of the Director of National Intelligence (ODNI), which is charged with promulgating appropriate procedures and guidelines under this subsection. The Committee expects to be consulted by ODNI in the formulation of these guidelines to ensure that the Committee's intent is achieved by them.

While the term “private sector” is not defined in the legislation, the Committee intends that term to be given the broadest possible meaning and specifically intends the term to include utilities,



whether organized as public, private, or quasi-public entities, to ensure at the entities that provide Americans with access to power, water, gas, and other critical services are also provided with access to critical federal government intelligence regarding cyber threats.

In addition, the Committee expects that private sector entities receiving classified intelligence pursuant to this subsection will use this information not only to protect their own systems and networks, but also, where they find appropriate as a business matter, to sell cybersecurity goods and services appropriately incorporating this information to protect other corporate customers.

*Paragraph 1: In General*

Paragraph (1) of subsection (a) requires the Director of National Intelligence to establish procedures to allow Intelligence Community elements to share cyber threat intelligence with the private sector and to encourage the sharing of such intelligence. The Committee intends the DNI's procedures to create a sea change in the current intelligence sharing practices of the Intelligence Community with respect to the private sector.

First, the DNI's procedures should ensure that as much cyber threat intelligence as possible is downgraded to the lowest classification level possible, including declassification where appropriate, and made available to as broad an audience in the private sector as possible, consistent with the need to protect the national security.

Second, the DNI's procedures should ensure that cyber threat intelligence, including classified information, is routinely and consistently provided out to entities and individuals in the private sector with the appropriate clearances.

*Paragraph 2: Sharing and Use of Classified Intelligence*

Paragraph (2) of subsection (a) requires that the DNI's procedures with respect to classified cyber threat intelligence require that classified information only be shared with certified entities, as defined by the legislation, or with individuals who possess appropriate security clearances. Certified entities are cybersecurity providers, protected entities, or self-protected entities that possess or are eligible to obtain a security clearance and can demonstrate to the Director of National Intelligence that they are able to appropriately protect such classified cyber threat intelligence.

Paragraph (2) also requires that the DNI's procedures provide that the sharing of classified cyber threat intelligence be consistent with the need to protect national security, which as noted above, includes the protection of the nation's economic security. As such, the legislation makes clear that the Intelligence Community can and should provide classified information to the private sector to enable American industry to protect itself from the theft of the intellectual property that is at the heart of our economic system.

Finally, paragraph (2) requires that the DNI's procedures provide that classified cyber threat intelligence only be used by certified entities in a manner that protects the classified information from unauthorized disclosure. This provision ensures that when certified entities employ classified intelligence to protect unclassified systems or networks, they do so in a way that does not reveal classified information directly or indirectly.

The Committee expects that the DNI's procedures will be flexible in nature and will take account of private sector innovation and incorporate current and future information sharing and security best practices. As a result, the Committee expects the DNI to work closely with the private sector to establish these procedures, to work with the private sector to meet the requirements of the procedures, and to ensure that these procedures result in the routine and consistent sharing of operationally-usable cyber threat intelligence. The Committee also expects the DNI to review and revise these procedures on a regular basis, at least annually, and to conduct such review in cooperation with the private sector, as well as to account for new technologies and cyber defense techniques developed by the private sector in each set of revised procedures. The DNI should also strongly consider the establishment of a private-sector advisory committee composed of senior executives at key private companies to advise on these procedures on a regular basis.

*Paragraph 3: Security Clearance Approvals*

Paragraph (3) requires the DNI to issue guidelines allowing the head of Intelligence Community elements to grant temporary or permanent security clearances to certified entities and their employees and officers (including non-employee officers such as board members) in order to allow the government to share classified cyber security threat intelligence with those certified entities. The Committee's intent is that the Intelligence Community grant security clearances to entities that are involved in protecting their own and their corporate customers' networks from cyber threats and that the Intelligence Community share cyber threat intelligence to protect the nation from advanced cyber threat actors. In particular, the Committee wishes to ensure that the private sector be able to receive highly classified cyber threat intelligence, including at the Top Secret/Sensitive Compartmented Information level, as appropriate to protect national security, and is concerned that certain industries and entities may currently lack sufficient clearances at the appropriate level.

Paragraph (3) also requires the DNI's guidelines to allow Intelligence Community elements to grant approval for the use of appropriate facilities and to expedite security clearances as necessary, consistent with the need to protect national security. The Committee's intent is that the approval process for the granting of security clearances and the use of facilities for the handling of classified information be expedited and broadened by these provisions.

Because additional security clearances or facility approvals may be necessary to effectuate the goals of this legislation, it is further the Committee's intent that the cost for these security clearances and facility approvals, as well as the underlying investigations and adjudications necessary to obtain and maintain them, be fully borne by the private sector. As noted above, it is the Committee's intent that private sector entities that become certified entities will be able to better protect themselves, as well as to sell cybersecurity goods and services appropriately incorporating this information to protect other corporate customers in the private sector. It is therefore the Committee's view that these entities should bear the full cost of obtaining access to the valuable cyber threat intelligence the government will provide under the legislation to certified entities.

The Committee therefore expects that the DNI's guidelines authorized by the legislation will provide for full payment of such costs by the private sector entity obtaining the security clearances or facility approvals.

*Paragraph 4: No Right or Benefit*

Paragraph (4) makes clear that while the Committee expects the Intelligence Community to work with private sector entities to help them meet the requirements to serve as a certified entity, no private sector entity is entitled to receive cyber threat intelligence from the government and that no right or benefit to cyber threat intelligence is created by the provision of such intelligence to a particular private sector entity or group of entities.

Paragraph (5) places a restriction on further disclosure of cyber threat intelligence received from the Federal Government by a certified entity other than by another certified entity or other appropriate agency or department of the Federal Government authorized to receive such cyber threat intelligence.

**Section 1104(b) of Title 50: Private Sector Use of Cybersecurity Systems and Sharing of Cyber Threat Information**

Subsection (b) of new Section 1104 provides clear, positive authority, notwithstanding any other provision of law, to private sector entities to monitor their own systems and networks or those of their corporate customers through the use of cybersecurity systems to identify and obtain cyber threat information, and to mitigate threats or vulnerabilities to their own systems or networks or those of their corporate customers. The Committee intends the notwithstanding clauses contained in subsection (b), as applied to this authority, to have the effect of removing any prohibition, real or perceived, to the monitoring, for cybersecurity purposes, of private sector systems and networks by the private sector entities that own the systems or networks or by security services contracted by the system or network owner to protect those networks and systems. Potential barriers to such cybersecurity monitoring include federal laws governing electronic surveillance, such as the Foreign Intelligence Surveillance Act of 1978 and various provisions of the federal criminal code, among others.

Subsection (b) also provides clear, positive authority, notwithstanding any other provision of law, for the private sector to share cyber threat information identified and obtained through such cybersecurity monitoring with other entities within the private sector, as well as with the Federal Government on a purely voluntary basis, at the discretion of the private sector entities whose systems or networks are being protected. The Committee intends the notwithstanding clauses contained in subsection (b), as applied to this authority, to have the effect of removing any prohibition, real or perceived, to the sharing of cyber threat information within the private sector, as well as with the Federal Government. Potential barriers to such sharing absent such positive authority include, but are not limited to, provisions of federal antitrust law, which some believe may limit sharing of cyber threat information between competitors in the private sector, as well as provisions of the surveillance laws mentioned above, as well as certain provisions of federal telecommunications and privacy laws. The provision is not in-

tended to authorize the unlawful fixing of prices or other prohibited activities, but is intended to permit robust sharing of information amongst private sector entities.

The Committee notes that the protections related to the authorities provided in this section are fairly robust, even standing alone. First, as noted below, only cyber threat information—that is information about a threat to, or vulnerability of government or private systems or networks—may be identified, obtained, or shared. And any such monitoring or sharing may only take place for cybersecurity purposes. And finally, the liability protection provided in this subsection only applies when an entity is acting in good faith. These provisions, taken together and building on top of one another, in the Committee’s view, are a strong step towards protecting the privacy and civil liberties of Americans.

*Paragraph 1: In General*

Paragraph (1) of subsection (b) provides the twin authorities discussed above to cybersecurity providers, who provide goods and services to their corporate customers for cybersecurity purposes and to self-protected entities, who provide such cybersecurity goods and services for themselves. In providing these authorities, the legislation makes clear that the monitoring and sharing of information either by a cybersecurity provider or a self-protected entity may only take place for cybersecurity purposes, a defined term that, as discussed below, limits the identification, obtaining, and sharing of cyber threat information to the protection of private or government systems or networks from threats to, or vulnerabilities, of those systems or networks. Similarly, the identification and obtaining of cyber threat information by a provider or a self-protected entity may only take place as part of an effort to protect the rights and properties of the provider’s corporate customer or the self-protected entity itself, as the case may be. In this context, it is the Committee’s intent that the protection of the rights and property of a corporate entity includes, but is not limited to, the protection of the systems and networks that make up its own corporate internal and external information systems but also the systems and networks over which it provides services to its customers. For example, the Committee expects that an internet service provider or telecommunications company may seek to protect not only its own corporate networks but also the backbone communications systems and networks over which it provides services to its customers. Similarly, for example, the Committee expects that a utility may seek not only to protect its corporate network but may seek to protect the systems and networks over which it provides electricity, water, or gas services to its customers. The Committee specifically intends the authorities provided in subsection (b) to permit private sector entities to protect such systems and networks broadly.

Paragraph (1) also requires that a cybersecurity provider obtain the express consent, whether in writing, electronically, orally, or otherwise, of its corporate customer before conducting any cybersecurity monitoring or sharing under these authorities. It is the Committee’s intent that express consent may be provided on a going-forward basis by a corporate customer to a provider for a specified period of time, to be determined by the corporate customer.

In addition, paragraph (1) makes clear that the sharing of information either by a cybersecurity provider or a self-protected entity is to be purely voluntary and at the discretion of the entity whose systems or networks are being protected. Moreover, the legislation requires that where a provider is doing the sharing on behalf of a corporate customer, the customer must designate the entities or group of entities it wishes to share information with, and that it must specifically designate the Federal Government if it wishes to share information with the government.

It is the Committee's expectation that many entities will be able to take advantage of the authorities provided in paragraph (1) when acting both as a cybersecurity provider and as a self-protected entity. For example, an entity such as an internet service provider may act as a cybersecurity provider when providing managed security services to a corporate customer and may simultaneously be acting as a self-protected entity when protecting its own corporate systems and networks as well as the systems and networks over which it provides services to its customers. The Committee's intent is that private sector entities will be able to simultaneously take advantage of multiple authorities provided within the legislation.

*Paragraph 2: Sharing with the Federal Government*

Paragraph (2)(A) requires the head of a department or agency of the Federal Government receiving cyber threat information under paragraph (1) to share that information with the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security in as close to real time as possible. Paragraph 2 further authorizes an entity who is sharing information with NCCIC to request that information be provided to another federal agency or department and permits the head of NCCIC to do so in as close to real time as possible.

It is the Committee's expectation that the requirement to share cyber threat information in as close to real time as possible will mean in practice that agencies will automate the transfer of information between agencies to the greatest extent possible and that information will be provided in a form that is usable by the consumers of the information. To the extent that automation is not possible or practical, the agencies will adopt and maintain a rules based system that minimizes the number of interventions or decisions necessary before information is shared.

*Paragraph 3: Use and Protection of Information*

Paragraph (3) of subsection (b) provides protections to promote the robust sharing of cyber threat information both within the private sector as well as from the private sector to the government.

Paragraph (3) provides that cyber threat information shared pursuant to paragraph (1) may only be shared in accordance with restrictions placed upon such sharing by the protected entity or the self-protected entity whose systems and networks are being protected and who therefore authorized the sharing. Paragraph (3) further provides that these restrictions may include the appropriate anonymization or minimization as determined by the protected entity or self-protected entity authorizing the sharing, but may not limit which federal agency receives the information once shared

with the Federal Government. The Committee's intent is that through paragraphs (1), (2) and (3), a private sector entity choosing to share cyber threat information under these provisions has may decide which government agency it provides the information to, and whether the information it shares is anonymized or minimized.

Paragraph (3) also provides that information shared pursuant to paragraph (1) may not be used by a receiving entity to gain an unfair competitive advantage to the detriment of the entity sharing the information. The Committee understands that cybersecurity is enhanced by robust threat information sharing within the private sector, both amongst partners and competitors, without fear that a competitor will use the cyber threat or vulnerability information to unfairly obtain a competitive advantage—such as greater market share—rather than simply to protect itself. The situation the Committee intends this provision to address is best demonstrated by an example: Company A shares information about a cyber vulnerability in one of its products with Company B, a competitor in the same marketplace; Company B the next day puts out an advertisement saying, “Don't buy Company A's product because it has the following vulnerability . . . instead, buy our product which doesn't have the same vulnerabilities.” This provision is not intended to prevent any company from obtaining a fair competitive advantage by, for example, using the shared information to build a better, more secure product that can be marketed without reference to the vulnerability shared by the particular entity. In addition, the Committee wishes to note that the provision is not accompanied by any private or public cause of action and thus may only be enforced by a private party choosing to limit or completely curtail sharing of cyber threat information with a bad actor (as well as encouraging others to do so also).

Paragraph (3) further provides that cyber threat information voluntarily shared with the Federal Government pursuant to paragraph (1) shall be exempt from disclosure under the Freedom of Information Act, shall be considered proprietary information, shall not be disclosed by the Federal Government to an entity outside the Federal Government except as authorized by the entity sharing the information, and shall not be used by the Federal Government for regulatory purposes. The Committee intends this provision to address the key concerns expressed by the private sector regarding the sharing of their sensitive information with the federal government: first, that the government might expose its most sensitive threat and vulnerability information to a wide audience by releasing the information, thereby providing a roadmap for attacks by cyber threat actors; second, that the government might take the information provided by the private sector and use it to regulate or impose sanctions upon them.

The Committee determined that the best way to address these concerns and incentivize the sharing of cyber threat information with the government was to explicitly and clearly protect the information from being disclosed, to require the government to carefully protect the information, and finally, to prohibit the government from using information provided in this cybersecurity channel from being used for regulatory purposes. The Committee was cognizant of the fact that cyber threat information provided to the government under these authorities might also be required to be provided

by certain private sector entities to their regulators and therefore provided elsewhere in the legislation that the mere classification of the information as cyber threat information or its provision to the government under this mechanism does not satisfy those regulatory requirements nor override any appropriate regulation that may take place based on the provision of such information to the government through other channels. Rather, the limitation on regulatory action was designed by the Committee to provide a safe harbor where private sector entities could provide real-time cyber threat information to the government without fear that that particular information would be used to regulate them directly.

Paragraph 3 also provides that such information shall not be provided by the receiving agency of the Federal Government to another if the head of the receiving agency or the entity providing the information determines it will undermine the purpose of the sharing. It also provides shall be handled by the government consistent with the need to protect sources and methods and the national security.

*Paragraph 4: Exemption from Liability*

Paragraph (4) provides a bar to civil or criminal causes of action being brought or maintained in federal or state court against an entity or its officers, employees, or agents acting in good faith to use cybersecurity systems for monitoring to identify and obtain cyber threat information in accordance with the provisions of the legislation. The Committee's intent is to provide strong liability protection for private sector entities when they act to take advantage of the authorities provided under paragraph (1) of subsection (b) to do what the statute seeks to encourage them to do: robustly monitor their own systems and networks and those of their corporate customers and share information about threats and vulnerabilities to better protect their systems. Specifically, the Committee intends that civil or criminal actions based on the use of cybersecurity systems to monitor systems or networks to identify and obtain cyber threat information using the authorities of this statute shall be dismissed immediately by the courts and prior to significant discovery and extensive motion practice.

Paragraph (4) also provides an identical bar to actions against such entities acting in good faith for decisions made for cybersecurity purposes based on cyber threat information identified, obtained or shared under this section. The Committee believes that if information sharing does become truly robust, the amount of cyber threat information and the speed with which such information will be shared will make it nearly impossible to always protect against every threat in real-time and, as such, private sector entities ought not be held liable for such actions. Similarly, the Committee recognizes that particular entities may engage in a cost-benefit analysis with respect to implementing protections against particular threats and the Committee intends this provision to help ensure that a private sector entity making such a judgment not be held liable for making such reasonable determinations.

At the same time, the Committee was fully cognizant of the concern that it not create a moral hazard by providing too broad a liability protection provision and that it not incentivize bad acts. As a result, Paragraph (4) requires that the entity be acting in good

faith to obtain the benefits of this liability protection. Therefore, the Committee included an amendment during markup which is intended to construe the scope of the liability provision. It makes clear that certain acts or omissions taken with intent to injure, defraud, or otherwise endanger an individual, government or private entity or utility would not receive protection from liability. That is, where an entity acts in bad faith, it does not receive the benefit of the strong liability protection provided by the legislation. Of course, where an entity is seeking to take advantage of specific statutory authority provided by Congress and where Congress is seeking to incentivize cybersecurity activities, as with government action taken pursuant to statutory authority and the presumption of regularity that attaches to such actions, the Committee expects that good faith will be presumed in the absence of substantial evidence to the contrary.

*Paragraph 5: Relationship to Other Laws Requiring the Disclosure of Information*

Paragraph (5)(A) provides that the provision of cyber threat information to the government under the voluntary system established by this statute does not satisfy or affect any requirement under other provisions of law to provide information to the Federal Government. As noted briefly earlier, the Committee intends this provision to ensure that while information provided to the government under this legislation is protected from use by the government for regulatory purposes, that information otherwise required to be provided to the government must still be provided and that such information—required by other law to be provided to the government—may still be used for all lawful purposes, including, as required by law, for regulatory purposes.

Paragraph (5)(B) provides that provision of cyber threat information to the government under these authorities would also not satisfy or affect the applicability of other provisions of law including FOIA, with respect to information required to be provided to the Federal Government.

**Section 1104(c) of Title 50: Federal Government Use of Information**

Subsection (c) of new Section 1104 provides certain limitations on the government's use of cyber threat information provided by the private sector and ensures that the private sector's provision of information to the government is purely voluntary. The Committee intends these provisions, along with others in the legislation, to help protect the privacy and civil liberties of Americans.

*Paragraph (1): Limitation*

Paragraph (1) of subsection (c) limits the Federal Government's use of information shared with the government by the private sector to four specific areas: 1) for cybersecurity purposes; 2) to investigate and prosecute cybersecurity crimes; 3) to protect individuals from the danger of death or serious bodily harm and the investigation and prosecution of such; and 4) to protect minors from child pornography, sexual exploitation, and serious threats to the physical safety of such minors and to investigate and prosecute such crimes.



*Paragraph 2: Affirmative Search Restriction*

Paragraph (2) limits the Federal Government's affirmative searching of data provided exclusively under this legislation to the government by the private sector to only the permissible uses enumerated in paragraph (1). The Committee intends this provision to ensure that information provided under this authority not be affirmatively searched by the government for other purposes. At the same time, however, the Committee does not intend this provision to limit in any way the government's ability to act on information that is discovered in the process of searching or analyzing the information provided for the specified purposes.

*Paragraph 3: Anti-Tasking Restrictions*

Paragraph (3) makes clear that nothing in this legislation permits the government to require a private sector entity to share with the Federal Government nor to condition the sharing of cyber threat intelligence under subsection (a) on the provision of cyber threat information back to the Federal Government under subsection (b). The Committee intends this provision to ensure that cyber threat information sharing by the private sector with the Federal Government remains purely voluntary and that the government not attempt to compel such sharing by withholding valuable cyber threat intelligence. The Committee believes that this provision also prevents the government from "tasking" the collection of information as the government might do under appropriate criminal or foreign intelligence surveillance authority because it ensures that the private sector cannot be required to provide information back to the government.

*Paragraph 4: Protection of Sensitive Personal Documents*

Paragraph (4) limits the Federal Government's use of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records and medical records.

Paragraph (5) requires the Federal Government to notify the provider of information shared under (b)(1) if it determines the information is not cyber threat information.

Paragraph (6) prohibits the Federal Government from retaining or using information shared under (b)(1) for any use other than a permissible use under (c)(1).

Paragraph (7) requires the DNI to establish procedures governing the receipt, retention, use and disclosure of non-publicly available cyber threat information shared with the Federal Government under (b)(1). The policies and procedures must minimize the impact on privacy and civil liberties, reasonably limit the receipt, retention, use and disclosure of cyber threat information not necessary to protect systems from cyber threats, and to protect the confidentiality of cyber threat information associated with specific persons as well as to guard such information from unauthorized access. The procedures must also not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat. The procedures must be implemented by agencies receiving cyber threat information under (b)(1) and must be submitted to Congress. Additionally, the DNI must establish a program to monitor and oversee compliance with the procedures, and

agencies receiving cyber threat information under (b)(1) must report compliance incidents to the DNI, AG and the intelligence committees.

**Section 1104(d) of Title 50: Federal Government Liability for Violations of Restrictions on the Disclosure, Use, and Protection of Voluntarily Shared Information**

Subsection (d) creates a cause of action for persons adversely affected by a willful or intentional violation of (b)(3)(D) or (c) of the section. The liability avenue also provides for damages and costs and attorney fees.

**Section 1104(e) of Title 50: Report on Information Sharing**

Subsection (e) of new Section 1104 requires the Inspector General of the Intelligence Community, in consultation with the Inspectors General of the Justice and Defense Departments, and the Privacy and Civil Liberties Oversight Board to report annually to the Congressional intelligence committees, in unclassified form accompanied by a classified annex as needed, on the use of the information shared with the Federal Government under this legislation. The report on the use of information shared with the Federal Government will include: (1) a review of the use of such information for purposes other than cybersecurity; (2) a review of the type of information shared with the Federal Government; (3) a review of the actions taken by the Federal Government based on the information shared; (4) appropriate metrics to determine the impact of such sharing on privacy and civil liberties, if any such impact exists; and (5) any recommendations of the Inspector General for improvements or modifications to the authorities provided under this legislation. It is the Committee's intent that this report provide the Committee with the information it needs to ensure that the privacy and civil liberties of Americans are being appropriately protected.

**Section 1104(f) of Title 50: Federal Preemption**

Subsection (f) of new Section 1104 provides that the legislation supersedes any provision of state or local law that may prohibit the activities authorized by this legislation. The Committee's intent is to ensure, as with the federal provisions discussed above, that state and local law on wiretapping, antitrust, and public disclosure, to name but a few, do not stand as a bar to the kind of robust cyber threat intelligence and information sharing that the Committee hopes to engender through the process of legislation.

**Section 1104(g) of Title 50: Savings Clauses**

Subsection (g)(1) of new Section 1104 makes clear that nothing in this legislation trumps existing laws or authorities permitting the use of cybersecurity systems or efforts to identify, obtain, or share cyber threat information. Many private sector entities today take advantage of certain provisions of federal law to conduct the limited monitoring for cybersecurity purposes. While this legislation provides much more robust authorities, the Committee believed it important to ensure that existing authorities remained in place and that those authorities could continue to be used by the appropriate government agencies and entities.

Paragraph (2) makes clear that nothing in the legislation may be construed as providing additional authority to or modifying existing authority of the Department of Defense including the National Security Agency or any other element of the Intelligence Community to control or direct the cybersecurity efforts of a private sector entity or component of the Federal Government or state, local or tribal government.

Paragraph (3) makes clear that nothing in the legislation can be construed to limit or modify an existing information sharing relationship, or prohibit or require a new information sharing relationship. It also makes clear that nothing in this legislation modifies the authority of a department or agency of the Federal Government to protect sources and methods and the national security of the United States, and nothing shall be construed to preclude the Federal Government from requiring reporting on significant cyber incidents already authorized or required under law.

Paragraph (4) makes clear that the legislation cannot be construed to provide additional authority to or modify existing authority of any entity to use a cybersecurity system owned or controlled by the federal Government on a private sector system or network to protect such.

Paragraph (5) makes clear that nothing in the legislation can be construed to subject anyone to liability for choosing not to engage in the voluntary activities authorized under the legislation.

Paragraph (6) makes clear that the legislation cannot be construed to authorize the Federal Government to retain or use information shared under (b)(1) of the legislation for any use other than those authorized under (c)(1).

#### Section 1104(g) of Title 50: Definitions

Subsection (g) of the new Section 1104 provides important definitions for the purpose of this legislation. The Committee notes that much of the work on limiting the scope and breadth of this legislation is done by the definitions and commends those interested in this legislation to carefully review these definitions in the context of the legislation.

##### *Paragraph 1: Availability*

Defines the term “availability” to mean ensuring timely and reliable access to and use of information.

##### *Paragraph 2: Certified Entity*

As noted briefly above, a certified entity is defined as a cybersecurity provider, a protected entity, or a self-protected entity that also possesses or is eligible to obtain a security clearance at the level appropriate to receive classified cyber threat intelligence, as determined by the DNI, and can demonstrate to the Director of National Intelligence that it can appropriately protect that classified information.

##### *Paragraph 3: Confidentiality*

The term confidentiality is defined as preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

*Paragraph 4: Cyber Threat Information*

Cyber threat information is defined to mean information that directly pertains to a vulnerability of, or threat to the integrity, confidentiality or availability of, a system or network of a government or private entity. Such information includes, but is not limited to, information pertaining to the protection of a system or network from efforts to deny access to, degrade, disrupt or destroy the network, as well as efforts to gain unauthorized access to such system for the purpose of exfiltrating information from the system or network. The Committee specifically excluded from the definition of cyberthreat information pertaining to efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

*Paragraph 5: Cyber Threat Intelligence*

The definition of cyber threat intelligence is consistent with the definition of cyber threat information except that cyber threat intelligence is information that is originally in the possession of an element of the Intelligence Community. The Committee used different terms in this legislation with similar definitions in order to distinguish the origin of information.

*Paragraph 6: Cybersecurity Crime*

Cybersecurity crime is defined as a crime a crime under federal or state law that involves efforts to deny access, degrade, disrupt, destroy, gain unauthorized access to a system or network or to exfiltrate information from a system or network without authorization. The definition also means a violation of federal law relating to computer crimes including a violation of any provision of Title 18 of the United States code that was created or amended by the Computer Fraud and Abuse Act of 1986.

*Paragraph 7: Cybersecurity Provider*

A cybersecurity provider is defined to be a non federal entity that provides goods or services intended to be used for cybersecurity purposes. The Committee intentionally excluded federal entities from this construct to avoid any concern that federal government agencies might serve as cybersecurity providers to private sector entities.

*Paragraph 8: Cybersecurity Purpose*

A cybersecurity purpose is defined as the purpose of ensuring the integrity, confidentiality, and availability of, or safeguarding, a system or network. This includes, but is not limited to, the protection of a system or network from a vulnerability of a system or network, a threat to the integrity, confidentiality, or availability of a network, efforts to deny access to, degrade, disrupt or destroy a network, as well as the protection of a system or network from efforts to gain unauthorized access for the purpose of exfiltrating information.

*Paragraph 9: Cybersecurity System*

A cybersecurity system is defined as a system designed or employed to ensure the integrity, confidentiality, and availability of,

or safeguard, a system or network. This includes, but is not limited to, a system designed or employed to protect a system or network from a vulnerability of a system or network, a threat to the integrity, confidentiality, or availability of a network, efforts to deny access to, degrade, disrupt or destroy a network, as well as the protection of a system or network from efforts to gain unauthorized access for the purpose of exfiltrating information. It does not include, however, a system designed or employed to protect a system or network from efforts to gain unauthorized access to such that solely involves violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

*Paragraph 10: Integrity*

The term integrity as used in this legislation means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

*Paragraph 11: Protected Entity*

A protected entity is defined as an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes. The Committee intentionally excluded individuals from this definition so as to limit the direct scope of the legislation to the protection of corporate entities.

*Paragraph 12: Self-Protected Entity*

A self-protected entity is defined as an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself. As with the definition of a protected entity, the Committee intentionally excluded individuals from this definition so as to limit the direct scope of the legislation to the protection of corporate entities.

*Paragraph 13: Utility*

The term utility means an entity providing essential services (other than law enforcement or regulatory services), including electricity, natural gas, propane, telecommunications, transportation, water or wastewater services.

*Section 2(b): Procedures and Guidelines*

This subsection of the Act requires the DNI to establish the procedures for sharing of cyber threat intelligence and to issue the guidelines for granting security clearances within 60 days of the date of enactment of the Act. This subsection of the Act also requires the DNI to expeditiously distribute the procedures and guidelines to appropriate federal government and private sector entities. The Committee intends to require the DNI to meet these deadlines and to broadly distribute the procedures and guidelines. As previously noted, the Committee expects the DNI to work closely with the private sector in developing these procedures and guidelines.

*Section 2(c): Privacy and Civil Liberties Policies and Procedures*

This subsection requires the DNI to establish the procedures for minimizing privacy and civil liberties within 60 days of the date of enactment of the Act.

*Section 2(d): Initial Reports*

This subsection of the Act requires the first reports to be provided to the Congressional intelligence committees by the Inspector General of the Intelligence Community under paragraphs (1) and (2) of subsection (e) of section 1104 to be provided no later than one year after the date of the enactment of this Act.

*Section 2(e): Table of Contents Amendment*

This subsection of the Act provides for amendments to the table of contents of the National Security Act of 1947.

*Section 3: Sunset*

Section (3) sets a five year sunset on the legislation from the date of enactment.

## 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 one open hearing, and numerous informal information meetings or briefings during the 113th Congress. The Committee also held hearings, briefings and informational meetings during the 112th Congress, detailed in footnote 1, above. The Committee's extensive oversight of the cyber threat resulted in the subject matter bill which would authorize cyber threat information sharing between and amongst the private sector and government for the purposes of better securing systems and networks against the cyber threat.

## STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The goals and objectives of H.R. 624 are to provide clear legal authority for sharing cyber threat information between and among private sector entities and the Federal Government, and to enhance the security of networks from the growing cyber intrusion threat.

## 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. 624 from the Director of the Congressional Budget Office.

APRIL 12, 2013.

Hon. MIKE ROGERS,  
*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. 624, the Cyber Intelligence Sharing and Protection Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Jason Wheelock and Ray Hall.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

*H.R. 624—Cyber Intelligence Sharing and Protection Act*

H.R. 624 would amend the National Security Act of 1947 to require the Director of National Intelligence (DNI) to establish procedures to promote the sharing of information about cyber threats between intelligence agencies and the private sector. The DNI also would be directed to establish guidelines for granting security clearances to employees of the private-sector entities with which the government shares such information. CBO estimates that implementing the bill would have a discretionary cost of \$20 million over the 2014–2018 period, assuming appropriation of the necessary amounts. Enacting H.R. 624 could affect direct spending or revenues; therefore, pay-as-you-go procedures apply. However, CBO estimates that those effects would be insignificant for each year.

CBO anticipates additional personnel would be needed to administer the program and to manage the exchange of information between intelligence agencies and the private sector. Based on information from the DNI and the Office of Personnel Management, CBO estimates that those activities would cost approximately \$4 million annually over the 2014–2018 period, assuming appropriation of the necessary amounts.

H.R. 624 would allow for a person to collect damages and attorney's fees if the federal government intentionally or willfully violated the conditions in the bill regarding the handling and use of information shared with the government and that person was harmed by such actions. Because any costs borne by the government for those cases would probably be paid from the Treasury's Judgment Fund (a permanent, indefinite appropriation for claims and judgments against the United States), the bill could affect direct spending. However, CBO anticipates that any such cases would be rare and that the impact on direct spending would be insignificant in every year.

The bill would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to entities and cybersecurity providers that share or use cyber threat information. The bill also would impose additional intergovernmental mandates on state governments by preempting state disclosure and liability laws. Because of uncertainty about the number of cases that would be limited and any forgone compensation that would result from compensatory damages, CBO cannot determine whether the costs of the mandate would exceed the annual threshold established in UMRA for private-sector mandates (\$150 million in 2013, adjusted annually for inflation). However, CBO estimates that the aggregate costs of the mandates on public entities would fall below the threshold for intergovernmental mandates (\$75 million in 2013, adjusted annually for inflation).

The CBO staff contacts for this estimate are Jason Wheelock and Ray Hall (for federal costs), J'nell J. Blanco (for the intergovernmental impact), and Elizabeth Bass (for the private-sector impact). This estimate was approved by Theresa Gullo, Deputy 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 italic, 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

Sec. 2. Declaration of policy.

\* \* \* \* \*

#### TITLE XI—OTHER PROVISIONS

\* \* \* \* \*

*Sec. 1104. Cyber threat intelligence and information sharing.*

\* \* \* \* \*

#### TITLE XI—ADDITIONAL MISCELLANEOUS PROVISIONS

\* \* \* \* \*

#### CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

**SEC. 1104. (a) INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR AND UTILITIES.—**

*(1) IN GENERAL.—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector en-*



*tities and utilities and to encourage the sharing of such intelligence.*

(2) *SHARING AND USE OF CLASSIFIED INTELLIGENCE.—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—*

(A) *shared by an element of the intelligence community with—*

(i) *a certified entity; or*

(ii) *a person with an appropriate security clearance to receive such cyber threat intelligence;*

(B) *shared consistent with the need to protect the national security of the United States; and*

(C) *used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.*

(3) *SECURITY CLEARANCE APPROVALS.—The Director of National Intelligence shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection—*

(A) *grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity;*

(B) *grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and*

(C) *expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.*

(4) *NO RIGHT OR BENEFIT.—The provision of information to a private-sector entity or a utility under this subsection shall not create a right or benefit to similar information by such entity or such utility or any other private-sector entity or utility.*

(5) *RESTRICTION ON DISCLOSURE OF CYBER THREAT INTELLIGENCE.—Notwithstanding any other provision of law, a certified entity receiving cyber threat intelligence pursuant to this subsection shall not further disclose such cyber threat intelligence to another entity, other than to a certified entity or other appropriate agency or department of the Federal Government authorized to receive such cyber threat intelligence.*

(b) *USE OF CYBERSECURITY SYSTEMS AND SHARING OF CYBER THREAT INFORMATION.—*

(1) *IN GENERAL.—*

(A) *CYBERSECURITY PROVIDERS.—Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes—*

(i) *use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and*

(ii) *share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.*

(B) *SELF-PROTECTED ENTITIES.*—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—

(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and

(ii) share such cyber threat information with any other entity, including the Federal Government.

(2) *SHARING WITH THE FEDERAL GOVERNMENT.*—

(A) *INFORMATION SHARED WITH THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER OF THE DEPARTMENT OF HOMELAND SECURITY.*—Subject to the use and protection of information requirements under paragraph (3), the head of a department or agency of the Federal Government receiving cyber threat information in accordance with paragraph (1) shall provide such cyber threat information in as close to real time as possible to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security.

(B) *REQUEST TO SHARE WITH ANOTHER DEPARTMENT OR AGENCY OF THE FEDERAL GOVERNMENT.*—An entity sharing cyber threat information that is provided to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security under subparagraph (A) or paragraph (1) may request the head of such Center to, and the head of such Center may, provide such information in as close to real time as possible to another department or agency of the Federal Government.

(3) *USE AND PROTECTION OF INFORMATION.*—Cyber threat information shared in accordance with paragraph (1)—

(A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected entity authorizing such sharing, including appropriate anonymization or minimization of such information and excluding limiting a department or agency of the Federal Government from sharing such information with another department or agency of the Federal Government in accordance with this section;

(B) may not be used by an entity to gain an unfair competitive advantage to the detriment of the protected entity or the self-protected entity authorizing the sharing of information;

(C) may only be used by a non-Federal recipient of such information for a cybersecurity purpose;

(D) if shared with the Federal Government—

(i) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly known as the “Freedom of Information Act”);

(ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information;

(iii) shall not be used by the Federal Government for regulatory purposes;

(iv) shall not be provided by the department or agency of the Federal Government receiving such cyber threat information to another department or agency of the Federal Government under paragraph (2)(A) if—

(I) the entity providing such information determines that the provision of such information will undermine the purpose for which such information is shared; or

(II) unless otherwise directed by the President, the head of the department or agency of the Federal Government receiving such cyber threat information determines that the provision of such information will undermine the purpose for which such information is shared; and

(v) shall be handled by the Federal Government consistent with the need to protect sources and methods and the national security of the United States; and

(E) shall be exempt from disclosure under a State, local, or tribal law or regulation that requires public disclosure of information by a public or quasi-public entity.

**(4) EXEMPTION FROM LIABILITY.—**

(A) **EXEMPTION.**—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith—

(i) for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or

(ii) for decisions made for cybersecurity purposes and based on cyber threat information identified, obtained, or shared under this section.

(B) **LACK OF GOOD FAITH.**—For purposes of the exemption from liability under subparagraph (A), a lack of good faith includes, but is not limited to, any act or omission taken with intent to injure, defraud, or otherwise endanger any individual, government entity, private entity, or utility.

**(5) RELATIONSHIP TO OTHER LAWS REQUIRING THE DISCLOSURE OF INFORMATION.**—The submission of information under this subsection to the Federal Government shall not satisfy or affect—

(A) any requirement under any other provision of law for a person or entity to provide information to the Federal Government; or

(B) the applicability of other provisions of law, including section 552 of title 5, United States Code (commonly known as the “Freedom of Information Act”), with respect to information required to be provided to the Federal Government under such other provision of law.

**(6) RULE OF CONSTRUCTION.**—Nothing in this subsection shall be construed to provide new authority to—

(A) a cybersecurity provider to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or oper-

ated by a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes; or

(B) a self-protected entity to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by such self-protected entity.

(c) **FEDERAL GOVERNMENT USE OF INFORMATION.**—

(1) **LIMITATION.**—The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection (b)—

(A) for cybersecurity purposes;

(B) for the investigation and prosecution of cybersecurity crimes;

(C) for the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger of death or serious bodily harm; or

(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking and the investigation and prosecution of crimes involving child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking, and any crime referred to in section 2258A(a)(2) of title 18, United States Code.

(2) **AFFIRMATIVE SEARCH RESTRICTION.**—The Federal Government may not affirmatively search cyber threat information shared with the Federal Government under subsection (b) for a purpose other than a purpose referred to in paragraph (1).

(3) **ANTI-TASKING RESTRICTION.**—Nothing in this section shall be construed to permit the Federal Government to—

(A) require a private-sector entity or utility to share information with the Federal Government; or

(B) condition the sharing of cyber threat intelligence with a private-sector entity or utility on the provision of cyber threat information to the Federal Government.

(4) **PROTECTION OF SENSITIVE PERSONAL DOCUMENTS.**—The Federal Government may not use the following information, containing information that identifies a person, shared with the Federal Government in accordance with subsection (b) unless such information is used in accordance with the policies and procedures established under paragraph (7):

(A) Library circulation records.

(B) Library patron lists.

(C) Book sales records.

(D) Book customer lists.

(E) Firearms sales records.

(F) Tax return records.

(G) Educational records.

(H) Medical records.

(5) **NOTIFICATION OF NON-CYBER THREAT INFORMATION.**—If a department or agency of the Federal Government receiving information pursuant to subsection (b)(1) determines that such information is not cyber threat information, such department or

agency shall notify the entity or provider sharing such information pursuant to subsection (b)(1).

(6) *RETENTION AND USE OF CYBER THREAT INFORMATION.*—No department or agency of the Federal Government shall retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

(7) *PRIVACY AND CIVIL LIBERTIES.*—

(A) *POLICIES AND PROCEDURES.*—The Director of National Intelligence, in consultation with the Secretary of Homeland Security and the Attorney General, shall establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the Federal Government in accordance with subsection (b)(1). Such policies and procedures shall, consistent with the need to protect systems and networks from cyber threats and mitigate cyber threats in a timely manner—

(i) minimize the impact on privacy and civil liberties;

(ii) reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is not necessary to protect systems or networks from cyber threats or mitigate cyber threats in a timely manner;

(iii) include requirements to safeguard non-publicly available cyber threat information that may be used to identify specific persons from unauthorized access or acquisition;

(iv) protect the confidentiality of cyber threat information associated with specific persons to the greatest extent practicable; and

(v) not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

(B) *SUBMISSION TO CONGRESS.*—The Director of National Intelligence shall, consistent with the need to protect sources and methods, submit to Congress the policies and procedures required under subparagraph (A) and any updates to such policies and procedures.

(C) *IMPLEMENTATION.*—The head of each department or agency of the Federal Government receiving cyber threat information shared with the Federal Government under subsection (b)(1) shall—

(i) implement the policies and procedures established under subparagraph (A); and

(ii) promptly notify the Director of National Intelligence, the Attorney General, and the congressional intelligence committees of any significant violations of such policies and procedures.

(D) *OVERSIGHT.*—The Director of National Intelligence, in consultation with the Attorney General, the Secretary of Homeland Security, and the Secretary of Defense, shall establish a program to monitor and oversee compliance with the policies and procedures established under subparagraph (A).

*(d) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF RESTRICTIONS ON THE DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED INFORMATION.—*

*(1) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates subsection (b)(3)(D) or subsection (c) with respect to the disclosure, use, or protection of voluntarily shared cyber threat information shared under this section, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—*

*(A) the actual damages sustained by the person as a result of the violation or \$1,000, whichever is greater; and*

*(B) the costs of the action together with reasonable attorney fees as determined by the court.*

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

*(A) the district in which the complainant resides;*

*(B) the district in which the principal place of business of the complainant is located;*

*(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or*

*(D) the District of Columbia.*

*(3) 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 subsection (b)(3)(D) or subsection (c) that is the basis for the action.*

*(4) 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 of subsection (b)(3)(D) or subsection (c).*

*(e) REPORTS ON INFORMATION SHARING.—*

*(1) INSPECTOR GENERAL REPORT.—The Inspector General of the Intelligence Community, in consultation with the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Privacy and Civil Liberties Oversight Board, shall annually submit to the congressional intelligence committees a report containing a review of the use of information shared with the Federal Government under this section, including—*

*(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;*

*(B) a review of the type of information shared with the Federal Government under this section;*

*(C) a review of the actions taken by the Federal Government based on such information;*

*(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any;*

*(E) a list of the departments or agencies receiving such information;*

(F) a review of the sharing of such information within the Federal Government to identify inappropriate stove-piping of shared information; and

(G) any recommendations of the Inspector General for improvements or modifications to the authorities under this section.

(2) *PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.*—The Civil Liberties Protection Officer of the Office of the Director of National Intelligence and the Chief Privacy and Civil Liberties Officer of the Department of Justice, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Intelligence Community, and the senior privacy and civil liberties officer of each department or agency of the Federal Government that receives cyber threat information shared with the Federal Government under this section, shall annually and jointly submit to Congress a report assessing the privacy and civil liberties impact of the activities conducted by the Federal Government under this section. Such report shall include any recommendations the Civil Liberties Protection Officer and Chief Privacy and Civil Liberties Officer consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat information under this section.

(3) *FORM.*—Each report required under paragraph (1) or (2) shall be submitted in unclassified form, but may include a classified annex.

(f) *FEDERAL PREEMPTION.*—This section supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under subsection (b).

(g) *SAVINGS CLAUSES.*—

(1) *EXISTING AUTHORITIES.*—Nothing in this section shall be construed to limit any other authority to use a cybersecurity system or to identify, obtain, or share cyber threat intelligence or cyber threat information.

(2) *LIMITATION ON MILITARY AND INTELLIGENCE COMMUNITY INVOLVEMENT IN PRIVATE AND PUBLIC SECTOR CYBERSECURITY EFFORTS.*—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, the Department of Defense or the National Security Agency or any other element of the intelligence community to control, modify, require, or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.

(3) *INFORMATION SHARING RELATIONSHIPS.*—Nothing in this section shall be construed to—

(A) limit or modify an existing information sharing relationship;

(B) prohibit a new information sharing relationship;

(C) require a new information sharing relationship between the Federal Government and a private-sector entity or utility;

(D) modify the authority of a department or agency of the Federal Government to protect sources and methods and the national security of the United States; or

(E) preclude the Federal Government from requiring an entity to report significant cyber incidents if authorized or required to do so under another provision of law.

(4) *LIMITATION ON FEDERAL GOVERNMENT USE OF CYBERSECURITY SYSTEMS.*—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, any entity to use a cybersecurity system owned or controlled by the Federal Government on a private-sector system or network to protect such private-sector system or network.

(5) *NO LIABILITY FOR NON-PARTICIPATION.*—Nothing in this section shall be construed to subject a protected entity, self-protected entity, cyber security provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, to liability for choosing not to engage in the voluntary activities authorized under this section.

(6) *USE AND RETENTION OF INFORMATION.*—Nothing in this section shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

(h) *DEFINITIONS.*—In this section:

(1) *AVAILABILITY.*—The term “availability” means ensuring timely and reliable access to and use of information.

(2) *CERTIFIED ENTITY.*—The term “certified entity” means a protected entity, self-protected entity, or cybersecurity provider that—

(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence.

(3) *CONFIDENTIALITY.*—The term “confidentiality” means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

(4) *CYBER THREAT INFORMATION.*—

(A) *IN GENERAL.*—The term “cyber threat information” means information directly pertaining to—

(i) a vulnerability of a system or network of a government or private entity or utility;

(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.



(B) *EXCLUSION.*—Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

(5) *CYBER THREAT INTELLIGENCE.*—

(A) *IN GENERAL.*—The term “cyber threat intelligence” means intelligence in the possession of an element of the intelligence community directly pertaining to—

(i) a vulnerability of a system or network of a government or private entity or utility;

(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

(B) *EXCLUSION.*—Such term does not include intelligence pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

(6) *CYBERSECURITY CRIME.*—The term “cybersecurity crime” means—

(A) a crime under a Federal or State law that involves—

(i) efforts to deny access to or degrade, disrupt, or destroy a system or network;

(ii) efforts to gain unauthorized access to a system or network; or

(iii) efforts to exfiltrate information from a system or network without authorization; or

(B) the violation of a provision of Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, created or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99-474).

(7) *CYBERSECURITY PROVIDER.*—The term “cybersecurity provider” means a non-Federal entity that provides goods or services intended to be used for cybersecurity purposes.

(8) *CYBERSECURITY PURPOSE.*—

(A) *IN GENERAL.*—The term “cybersecurity purpose” means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

(i) a vulnerability of a system or network;

(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

(B) *EXCLUSION.*—Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

(9) *CYBERSECURITY SYSTEM.*—

(A) *IN GENERAL.*—The term “cybersecurity system” means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

(i) a vulnerability of a system or network;

(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

(B) *EXCLUSION.*—Such term does not include a system designed or employed to protect a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

(10) *INTEGRITY.*—The term “integrity” means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

(11) *PROTECTED ENTITY.*—The term “protected entity” means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.

(12) *SELF-PROTECTED ENTITY.*—The term “self-protected entity” means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.

(13) *UTILITY.*—The term “utility” means an entity providing essential services (other than law enforcement or regulatory services), including electricity, natural gas, propane, telecommunications, transportation, water, or wastewater services.

[Effective 5 years after the date of enactment, section 3 of H.R. 624 (as reported) provides for a sunset provision to amendments made by section 2 of H.R. 624 to the National Security Act of 1947. The version below reflects the execution of the amendments made by section 2 of H.R. 624 as if they reflect current law in order to show the repeal of such provisions on such effective date.]

\* \* \* \* \*

TABLE OF CONTENTS

Sec. 2. Declaration of policy.

\* \* \* \* \*

TITLE XI—OTHER PROVISIONS

\* \* \* \* \*

[Sec. 1104. Cyber threat intelligence and information sharing.]

\* \* \* \* \*

TITLE XI—ADDITIONAL MISCELLANEOUS PROVISIONS

\* \* \* \* \*

[CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

[SEC. 1104. (a) INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR AND UTILITIES.—

[(1) IN GENERAL.—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and utilities and to encourage the sharing of such intelligence.

[(2) SHARING AND USE OF CLASSIFIED INTELLIGENCE.—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—

[(A) shared by an element of the intelligence community with—

[(i) a certified entity; or

[(ii) a person with an appropriate security clearance to receive such cyber threat intelligence;

[(B) shared consistent with the need to protect the national security of the United States; and

[(C) used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.

[(3) SECURITY CLEARANCE APPROVALS.—The Director of National Intelligence shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection—

[(A) grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity;

[(B) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and

[(C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.

[(4) NO RIGHT OR BENEFIT.—The provision of information to a private-sector entity or a utility under this subsection shall not create a right or benefit to similar information by such entity or such utility or any other private-sector entity or utility.

[(5) RESTRICTION ON DISCLOSURE OF CYBER THREAT INTELLIGENCE.—Notwithstanding any other provision of law, a certified entity receiving cyber threat intelligence pursuant to this subsection shall not further disclose such cyber threat intelligence to another entity, other than to a certified entity or other appropriate agency or department of the Federal Government authorized to receive such cyber threat intelligence.

[(b) USE OF CYBERSECURITY SYSTEMS AND SHARING OF CYBER THREAT INFORMATION.—

[(1) IN GENERAL.—

[(A) CYBERSECURITY PROVIDERS.—Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes—

[(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and

[(ii) share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.

[(B) SELF-PROTECTED ENTITIES.—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—

[(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and

[(ii) share such cyber threat information with any other entity, including the Federal Government.

[(2) SHARING WITH THE FEDERAL GOVERNMENT.—

[(A) INFORMATION SHARED WITH THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER OF THE DEPARTMENT OF HOMELAND SECURITY.—Subject to the use and protection of information requirements under paragraph (3), the head of a department or agency of the Federal Government receiving cyber threat information in accordance with paragraph (1) shall provide such cyber threat information in as close to real time as possible to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security.

[(B) REQUEST TO SHARE WITH ANOTHER DEPARTMENT OR AGENCY OF THE FEDERAL GOVERNMENT.—An entity sharing cyber threat information that is provided to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security under subparagraph (A) or paragraph (1) may request the head of such Center to, and the head of such Center may, provide such information in as close to real time as possible to another department or agency of the Federal Government.

[(3) USE AND PROTECTION OF INFORMATION.—Cyber threat information shared in accordance with paragraph (1)—

[(A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected entity authorizing such sharing, including appropriate anonymization or minimization of such information and excluding limiting a department or agency of the Federal Government from sharing such information with another department or agency of the Federal Government in accordance with this section;

[(B) may not be used by an entity to gain an unfair competitive advantage to the detriment of the protected entity or the self-protected entity authorizing the sharing of information;

[(C) may only be used by a non-Federal recipient of such information for a cybersecurity purpose;

[(D) if shared with the Federal Government—

[(i) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly known as the “Freedom of Information Act”);

[(ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information;

[(iii) shall not be used by the Federal Government for regulatory purposes;

[(iv) shall not be provided by the department or agency of the Federal Government receiving such cyber threat information to another department or agency of the Federal Government under paragraph (2)(A) if—

[(I) the entity providing such information determines that the provision of such information will undermine the purpose for which such information is shared; or

[(II) unless otherwise directed by the President, the head of the department or agency of the Federal Government receiving such cyber threat information determines that the provision of such information will undermine the purpose for which such information is shared; and

[(v) shall be handled by the Federal Government consistent with the need to protect sources and methods and the national security of the United States; and

[(E) shall be exempt from disclosure under a State, local, or tribal law or regulation that requires public disclosure of information by a public or quasi-public entity.

[(4) EXEMPTION FROM LIABILITY.—

[(A) EXEMPTION.—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith—

[(i) for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or

[(ii) for decisions made for cybersecurity purposes and based on cyber threat information identified, obtained, or shared under this section.

[(B) LACK OF GOOD FAITH.—For purposes of the exemption from liability under subparagraph (A), a lack of good faith includes, but is not limited to, any act or omission taken with intent to injure, defraud, or otherwise endanger any individual, government entity, private entity, or utility.

[(5) RELATIONSHIP TO OTHER LAWS REQUIRING THE DISCLOSURE OF INFORMATION.—The submission of information under this subsection to the Federal Government shall not satisfy or affect—

[(A) any requirement under any other provision of law for a person or entity to provide information to the Federal Government; or

[(B) the applicability of other provisions of law, including section 552 of title 5, United States Code (commonly known as the “Freedom of Information Act”), with respect to information required to be provided to the Federal Government under such other provision of law.

[(6) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide new authority to—

[(A) a cybersecurity provider to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes; or

[(B) a self-protected entity to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by such self-protected entity.

[(c) FEDERAL GOVERNMENT USE OF INFORMATION.—

[(1) LIMITATION.—The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection (b)—

[(A) for cybersecurity purposes;

[(B) for the investigation and prosecution of cybersecurity crimes;

[(C) for the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger of death or serious bodily harm; or

[(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking and the investigation and prosecution of crimes involving child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking, and any crime referred to in section 2258A(a)(2) of title 18, United States Code.

[(2) AFFIRMATIVE SEARCH RESTRICTION.—The Federal Government may not affirmatively search cyber threat information shared with the Federal Government under subsection (b) for a purpose other than a purpose referred to in paragraph (1).

[(3) ANTI-TASKING RESTRICTION.—Nothing in this section shall be construed to permit the Federal Government to—

[(A) require a private-sector entity or utility to share information with the Federal Government; or

[(B) condition the sharing of cyber threat intelligence with a private-sector entity or utility on the provision of cyber threat information to the Federal Government.

[(4) PROTECTION OF SENSITIVE PERSONAL DOCUMENTS.—The Federal Government may not use the following information, containing information that identifies a person, shared with the Federal Government in accordance with subsection (b) unless such information is used in accordance with the policies and procedures established under paragraph (7):

[(A) Library circulation records.

[(B) Library patron lists.

[(C) Book sales records.

[(D) Book customer lists.

[(E) Firearms sales records.

[(F) Tax return records.

[(G) Educational records.

[(H) Medical records.

[(5) NOTIFICATION OF NON-CYBER THREAT INFORMATION.—If a department or agency of the Federal Government receiving information pursuant to subsection (b)(1) determines that such information is not cyber threat information, such department or agency shall notify the entity or provider sharing such information pursuant to subsection (b)(1).

[(6) RETENTION AND USE OF CYBER THREAT INFORMATION.—No department or agency of the Federal Government shall retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

[(7) PRIVACY AND CIVIL LIBERTIES.—

[(A) POLICIES AND PROCEDURES.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security and the Attorney General, shall establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the Federal Government in accordance with subsection (b)(1). Such policies and procedures shall, consistent with the need to protect systems and networks from cyber threats and mitigate cyber threats in a timely manner—

[(i) minimize the impact on privacy and civil liberties;

[(ii) reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is not necessary to protect systems or networks from cyber threats or mitigate cyber threats in a timely manner;

[(iii) include requirements to safeguard non-publicly available cyber threat information that may be used to

identify specific persons from unauthorized access or acquisition;

[(iv) protect the confidentiality of cyber threat information associated with specific persons to the greatest extent practicable; and

[(v) not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

[(B) SUBMISSION TO CONGRESS.—The Director of National Intelligence shall, consistent with the need to protect sources and methods, submit to Congress the policies and procedures required under subparagraph (A) and any updates to such policies and procedures.

[(C) IMPLEMENTATION.—The head of each department or agency of the Federal Government receiving cyber threat information shared with the Federal Government under subsection (b)(1) shall—

[(i) implement the policies and procedures established under subparagraph (A); and

[(ii) promptly notify the Director of National Intelligence, the Attorney General, and the congressional intelligence committees of any significant violations of such policies and procedures.

[(D) OVERSIGHT.—The Director of National Intelligence, in consultation with the Attorney General, the Secretary of Homeland Security, and the Secretary of Defense, shall establish a program to monitor and oversee compliance with the policies and procedures established under subparagraph (A).

[(d) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF RESTRICTIONS ON THE DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED INFORMATION.—

[(1) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates subsection (b)(3)(D) or subsection (c) with respect to the disclosure, use, or protection of voluntarily shared cyber threat information shared under this section, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

[(A) the actual damages sustained by the person as a result of the violation or \$1,000, whichever is greater; and

[(B) the costs of the action together with reasonable attorney fees as determined by the court.

[(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

[(A) the district in which the complainant resides;

[(B) the district in which the principal place of business of the complainant is located;

[(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

[(D) the District of Columbia.

[(3) 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 subsection (b)(3)(D) or subsection (c) that is the basis for the action.

[(4) 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 of subsection (b)(3)(D) or subsection (c).

[(e) REPORTS ON INFORMATION SHARING.—

[(1) INSPECTOR GENERAL REPORT.—The Inspector General of the Intelligence Community, in consultation with the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Privacy and Civil Liberties Oversight Board, shall annually submit to the congressional intelligence committees a report containing a review of the use of information shared with the Federal Government under this section, including—

[(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;

[(B) a review of the type of information shared with the Federal Government under this section;

[(C) a review of the actions taken by the Federal Government based on such information;

[(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any;

[(E) a list of the departments or agencies receiving such information;

[(F) a review of the sharing of such information within the Federal Government to identify inappropriate stove-piping of shared information; and

[(G) any recommendations of the Inspector General for improvements or modifications to the authorities under this section.

[(2) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Civil Liberties Protection Officer of the Office of the Director of National Intelligence and the Chief Privacy and Civil Liberties Officer of the Department of Justice, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Intelligence Community, and the senior privacy and civil liberties officer of each department or agency of the Federal Government that receives cyber threat information shared with the Federal Government under this section, shall annually and jointly submit to Congress a report assessing the privacy and civil liberties impact of the activities conducted by the Federal Government under this section. Such report shall include any recommendations the Civil Liberties Protection Officer and Chief Privacy and Civil Liberties Officer consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat information under this section.

[(3) FORM.—Each report required under paragraph (1) or (2) shall be submitted in unclassified form, but may include a classified annex.

[(f) FEDERAL PREEMPTION.—This section supersedes any statute of a State or political subdivision of a State that restricts or other-

wise expressly regulates an activity authorized under subsection (b).

**[(g) SAVINGS CLAUSES.—**

**[(1) EXISTING AUTHORITIES.—**Nothing in this section shall be construed to limit any other authority to use a cybersecurity system or to identify, obtain, or share cyber threat intelligence or cyber threat information.

**[(2) LIMITATION ON MILITARY AND INTELLIGENCE COMMUNITY INVOLVEMENT IN PRIVATE AND PUBLIC SECTOR CYBERSECURITY EFFORTS.—**Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, the Department of Defense or the National Security Agency or any other element of the intelligence community to control, modify, require, or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.

**[(3) INFORMATION SHARING RELATIONSHIPS.—**Nothing in this section shall be construed to—

**[(A)** limit or modify an existing information sharing relationship;

**[(B)** prohibit a new information sharing relationship;

**[(C)** require a new information sharing relationship between the Federal Government and a private-sector entity or utility;

**[(D)** modify the authority of a department or agency of the Federal Government to protect sources and methods and the national security of the United States; or

**[(E)** preclude the Federal Government from requiring an entity to report significant cyber incidents if authorized or required to do so under another provision of law.

**[(4) LIMITATION ON FEDERAL GOVERNMENT USE OF CYBERSECURITY SYSTEMS.—**Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, any entity to use a cybersecurity system owned or controlled by the Federal Government on a private-sector system or network to protect such private-sector system or network.

**[(5) NO LIABILITY FOR NON-PARTICIPATION.—**Nothing in this section shall be construed to subject a protected entity, self-protected entity, cyber security provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, to liability for choosing not to engage in the voluntary activities authorized under this section.

**[(6) USE AND RETENTION OF INFORMATION.—**Nothing in this section shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

**[(h) DEFINITIONS.—**In this section:

**[(1) AVAILABILITY.—**The term “availability” means ensuring timely and reliable access to and use of information.

**[(2) CERTIFIED ENTITY.—**The term “certified entity” means a protected entity, self-protected entity, or cybersecurity provider that—

[(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

[(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence.

[(3) CONFIDENTIALITY.—The term “confidentiality” means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

[(4) CYBER THREAT INFORMATION.—

[(A) IN GENERAL.—The term “cyber threat information” means information directly pertaining to—

[(i) a vulnerability of a system or network of a government or private entity or utility;

[(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

[(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

[(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

[(B) EXCLUSION.—Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

[(5) CYBER THREAT INTELLIGENCE.—

[(A) IN GENERAL.—The term “cyber threat intelligence” means intelligence in the possession of an element of the intelligence community directly pertaining to—

[(i) a vulnerability of a system or network of a government or private entity or utility;

[(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

[(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

[(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

[(B) EXCLUSION.—Such term does not include intelligence pertaining to efforts to gain unauthorized access to

a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

[(6) CYBERSECURITY CRIME.—The term “cybersecurity crime” means—

[(A) a crime under a Federal or State law that involves—

[(i) efforts to deny access to or degrade, disrupt, or destroy a system or network;

[(ii) efforts to gain unauthorized access to a system or network; or

[(iii) efforts to exfiltrate information from a system or network without authorization; or

[(B) the violation of a provision of Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, created or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99–474).

[(7) CYBERSECURITY PROVIDER.—The term “cybersecurity provider” means a non-Federal entity that provides goods or services intended to be used for cybersecurity purposes.

[(8) CYBERSECURITY PURPOSE.—

[(A) IN GENERAL.—The term “cybersecurity purpose” means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

[(i) a vulnerability of a system or network;

[(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

[(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

[(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

[(B) EXCLUSION.—Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

[(9) CYBERSECURITY SYSTEM.—

[(A) IN GENERAL.—The term “cybersecurity system” means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

[(i) a vulnerability of a system or network;

[(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

[(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

[(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

[(B) EXCLUSION.—Such term does not include a system designed or employed to protect a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

[(10) INTEGRITY.—The term “integrity” means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

[(11) PROTECTED ENTITY.—The term “protected entity” means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.

[(12) SELF-PROTECTED ENTITY.—The term “self-protected entity” means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.

[(13) UTILITY.—The term “utility” means an entity providing essential services (other than law enforcement or regulatory services), including electricity, natural gas, propane, telecommunications, transportation, water, or wastewater services.]

#### DISCLOSURE OF DIRECTED RULE MAKING

The Committee estimates that H.R. 624 specifically directs no specific rule makings to be completed within the meaning of 5 U.S.C. 551.

#### DUPLICATION OF FEDERAL PROGRAMS

H.R. 624 does not duplicate or reauthorize an established Federal program 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.

## COMMITTEE CORRESPONDENCE

BOB GOODLATTE, Virginia  
CHAIRMAN

F JAMES HENDERSON, Jr., Wisconsin  
HOWARD COBLE, North Carolina  
LAMAR SMITH, Texas  
STEVE CHABOT, Ohio  
SPENCER BACCHUS, Alabama  
DANIEL E. ROSS, California  
J. RAYMOND FISHER, Virginia  
STEVE KING, Iowa  
BRETT FRANKS, Arizona  
LOUIE GOHmert, Texas  
JIM JOHNSON, Ohio  
TED LEE, Texas  
JACQUE GOSPEL, Utah  
TODD MATHIS, Pennsylvania  
TREV FUMER, South Carolina  
MARK E. AMODEI, Nevada  
RALPH H. LAMARCA, Rhode  
BLAKE FARENTHOLD, Texas  
GEORGE HOLDING, North Carolina  
DOLU SCALINO, Chicago  
RON OLSANTO, Florida  
KEITH J. ROTHFUSS, Pennsylvania

ONE HUNDRED THIRTEENTH CONGRESS  
Congress of the United States

House of Representatives  
COMMITTEE ON THE JUDICIARY

213B RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

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

April 10, 2013

JOHN CONYERS, JR., Michigan  
RANKING MEMBER

JEROME NADLER, New York  
ROBERT C. "BOBBY" SCOTT, Virginia  
MELVIN L. WATTS, North Carolina  
ZOE LOFGREEN, California  
SHELIA JACKSON LEE, Texas  
STEVE COHEN, Tennessee  
HENRY C. "BOB" JOHNSON, Jr., Georgia  
PETER H. PERILLO, Puerto Rico  
JUDY CURT, California  
REGIS IFFERT, Florida  
LARRY V. GUTERREZ, Illinois  
KAREN BASCO, California  
CEORIC L. BUCHANON, Louisiana  
SIOZAN K. ELSBERG, Washington  
JES GARNER, Florida  
HARVEEN S. JEFFRIES, New York

The Honorable Mike Rogers  
Chairman  
House Permanent Select Committee on Intelligence  
HVC-304  
Washington, D.C. 20515

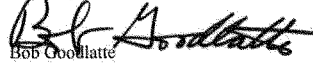
Dear Chairman Rogers,

I am writing concerning H.R. 624, the "Cyber Intelligence Sharing and Protection Act," which is scheduled for consideration in your Committee today. This bill contains provisions that fall within the Rule X jurisdiction of the Committee on the Judiciary.

As a result of your having made mutually agreed-upon changes to the provisions in question, and in order to expedite the House's consideration of H.R. 624, the Committee on the Judiciary will not assert its jurisdictional claim over this bill by seeking a sequential referral. The Committee takes this action with our mutual understanding that by foregoing consideration of H.R. 624 at this time, we do not waive any jurisdiction over subject matter contained in this or similar legislation, and that our Committee will be appropriately consulted and involved as the bill or similar legislation moves forward so that we may address any remaining issues in our jurisdiction. Our Committee also reserves the right to seek appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, and requests your support for any such request.

I would appreciate your response to this letter confirming this understanding with respect to H.R. 624, and would ask that a copy of our exchange of letters on this matter be included in the *Congressional Record* during floor consideration.

Sincerely,



Bob Goodlatte  
Chairman

cc: The Honorable John Boehner  
The Honorable C.A. Dutch Ruppersberger  
The Honorable John Conyers, Jr.  
Mr. Thomas J. Wickham, Jr., Parliamentarian

Mike Rogers, Michigan, CHAIRMAN

Mac Thornberry, Texas  
Jeff Miller, Florida  
K. Michael Conaway, Texas  
Peter T. King, New York  
Frank A. LoBiondo, New Jersey  
David Nunes, California  
Lynn A. Westmoreland, Georgia  
Michele Bachmann, Minnesota  
Thomas J. Rooney, Florida  
Joseph J. Heck, Nevada  
Mike R. Pompeo, Kansas

C.A. Dutch Ruppersberger, Maryland,  
RANKING MEMBER

Mike Thompson, California  
Janice D. Schakowsky, Illinois  
James R. Langevin, Rhode Island  
Adam B. Schiff, California  
Luis V. Guterrez, Illinois  
Ed Pastor, Arizona  
James A. Himes, Connecticut  
Terri A. Sewell, Alabama

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

J. Michael Allen  
STAFF DIRECTOR  
Heather M. Mosko  
MAJORITY STAFF DIRECTOR

April 11, 2013

The Honorable Bob Goodlatte  
Chairman  
Committee on the Judiciary  
U.S. House of Representatives  
Washington, D.C. 20515

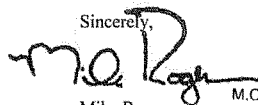
Dear Chairman Goodlatte:

Thank you for your letter regarding H.R. 624, the Cyber Intelligence Sharing and Protection Act. As you noted, elements of the bill fall within the jurisdiction of the Committee on the Judiciary. As you also noted, mutually agreed upon changes to the provisions in question were adopted by the Permanent Select Committee on Intelligence during its consideration of the bill, and we will be glad to continue to work with you on these provisions. We will also support the request of the Committee on the Judiciary for conferees in any conference that may occur on the bill.

I appreciate your willingness to forego consideration of the bill in the interest of expediting this legislation for floor consideration. I acknowledge that by agreeing to waive consideration of the bill, the Committee on the Judiciary does not waive any jurisdiction it may have over provisions of the bill or any matters under your jurisdiction. I will include a copy of your letter and this response in our Committee's report on H.R. 624 and the Congressional Record during consideration of the legislation on the House floor.

Thank you for your assistance in this matter.

Sincerely,



Mike Rogers  
Chairman

MICHAEL T. MCCAUL, TEXAS  
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI  
RANKING MEMBER



One Hundred Thirteenth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515

April 11, 2013

The Honorable Mike Rogers  
Chairman  
House Permanent Select Committee on Intelligence  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Chairman Rogers:

On April 10, 2013, the House Permanent Select Committee on Intelligence ordered H.R. 624, the "Cyber Intelligence Sharing and Protection Act", reported favorably to the House with certain provisions in the legislation that fall within the Rule X jurisdiction of the Committee on Homeland Security. Specifically, this legislation identifies the Department of Homeland Security's National Cybersecurity and Communications Integrations Center (NCCIC) as a principal entity for sharing cybersecurity information with the Federal government and amongst stakeholders.

The NCCIC partners with all Federal departments and agencies, State, local, Tribal, and territorial governments, as well as private sector and international entities. The Center works with critical infrastructure owners and operators to reduce risk, coordinates national response efforts to significant cyber incidents, and shares cybersecurity threat and vulnerability assessment information throughout the Federal government. These actions, along with the cybersecurity information provided through the NCCIC, trigger the jurisdiction of the Committee on Homeland Security over functions of the Department of Homeland Security relating to integration, analysis, and dissemination of homeland security information.

In the interest of permitting your committee to proceed expeditiously with consideration of this important legislation, the Committee on Homeland Security will not request a sequential referral over provisions within our jurisdiction. However, I do so with the mutual understanding that the Committee's jurisdictional claims over subject matters contained in this and similar legislation are in no way diminished or altered. I request that you urge the Speaker to name members of this Committee to any conference committee for consideration of provisions that fall within the jurisdiction of the Committee on Homeland Security in the House-Senate conference on this bill or similar legislation.



Finally, I ask that you place this letter and your response into the committee report on H.R. 624 and into the *Congressional Record* during consideration of the measure on the House floor. Thank you for your consideration of this matter.

Sincerely,

A handwritten signature in black ink that reads "Michael T. McCaul". The signature is written in a cursive, slightly slanted style.

MICHAEL T. McCAUL  
Chairman

cc: The Honorable John A. Boehner, Speaker  
The Honorable Eric Cantor, Majority Leader  
The Honorable C.A. Dutch Ruppersberger, Ranking Member  
The Honorable Bennie G. Thompson, Ranking Member  
The Honorable Thomas J. Wickham, Jr., Parliamentarian

Mike Rogers, Michigan, CHAIRMAN

Mac Thornberry, Texas  
Jeff Miller, Florida  
K. Michael Conaway, Texas  
Peter T. King, New York  
Frank A. LoBiondo, New Jersey  
Devin Nunes, California  
Lynn A. Westmoreland, Georgia  
Michelle Bachmann, Minnesota  
Thomas J. Rooney, Florida  
Joseph J. Heck, Nevada  
Mike R. Pompeo, Kansas

C.A. Dutch Ruppersberger, Maryland,  
REPUBLICAN MEMBER

Mike Thompson, California  
Janice D. Schakowsky, Illinois  
James R. Langevin, Rhode Island  
Adam B. Schiff, California  
Luis V. Guterrez, Illinois  
Ed Pastor, Arizona  
James A. Himes, Connecticut  
Trent A. Sewell, Alabama

John A. Boehner, SPEAKER OF THE HOUSE  
Nancy Pelosi, DEPUTY SPEAKER

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

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

J. Michael Allen  
STAFF DIRECTOR

HARVEY M. MALINO  
MANAGING STAFF DIRECTOR

April 12, 2013

The Honorable Michael T. McCaul  
Chairman  
Committee on Homeland Security  
Washington, DC 20515

Dear Chairman McCaul:

This responds to your letter dated April 11, 2013 concerning H.R. 624 the Cyber Intelligence Sharing and Protection Act (CISPA). Specifically, you noted the provision contained in the legislation relating to the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC).

I appreciate your decision to forego requesting referral of H.R. 624 to the House Homeland Security Committee in the interest of expediting floor consideration of this legislation. I also acknowledge that this decision will not diminish or alter the Homeland Security Committee's jurisdictional claims over subject matters contained in this and similar legislation. I will also support your request that the Speaker name members of the Homeland Security Committee to any conference committee for consideration of provisions that fall within the jurisdiction of the Committee on Homeland Security in the House-Senate conference on this bill. Finally, I will include a copy of your letter and this response letter in the Committee's report on H.R. 624 and in the Congressional Record during consideration of H.R. 624 on the House Floor.

Sincerely,

  
Mike Rogers M.C.  
Chairman

## ADDITIONAL VIEWS

The United States faces a serious and growing threat to our cyber security. We support the creation of mechanisms to facilitate greater sharing of cybersecurity information between the government and private sector. There is an urgent need to ensure that timely, actionable information is shared between the private sector and the government so that we can secure our networks against attacks and intrusion by state and non-state actors.

We support the intent of the Cyber Intelligence Sharing and Protection Act (H.R. 624), but we are disappointed in some aspects of it and believe that it can be improved to better protect privacy and civil liberties, while still working effectively to enhance cybersecurity. While the Committee did adopt meaningful improvements that are helpful, we are disappointed that the Committee rejected a proposed amendment that would have required private sector entities to make “reasonable efforts” to remove Personally Identifiable Information (PII) unrelated to the cybersecurity threat. This requirement was included in proposals that enjoyed bipartisan support in the Senate, as well as in draft legislation submitted to Congress by the White House in 2011.

In the Committee’s hearing on H.R. 624 on February 15, 2013, witnesses representing the private sector stated clearly that removing PII prior to providing it to the government is technically feasible and not an onerous requirement. One witness testified that such a requirement was “reasonable,” while another witness stated that, “The provider of the information is in the best position to anonymize it.” Moreover, witnesses made it clear that PII is rarely if ever relevant to responding to a cybersecurity threat, with one witness informing the Committee that, “I have never seen a package of threat intelligence that’s actionable that also includes [PII].”

In addition, we believe that concerns regarding privacy and civil liberties should be addressed by requiring that civilian agencies, including the Department of Homeland Security, serve as the primary points of contact with the private sector, particularly in receiving information. Elements of the Intelligence Community within the Department of Defense have important technical expertise that should be harnessed to improve cybersecurity, but they should not be the initial recipient of cyber security information. Allowing information to go directly to military agencies significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres.

We are also concerned that the liability shield provided in the bill is overly broad and fails to provide reasonable protections for consumers. While important improvements were made in markup, we remain concerned that the broad scope of the shield may allow cybersecurity entities to claim immunity even if injuries are the result of neglect or recklessness.

We strongly support the need to secure our public and private systems from the constant, malicious attacks of foreign and domestic hackers, and we believe that information sharing is an important aspect of enhanced cybersecurity. We appreciate the changes already made to H.R. 624, and we hope that as the bill moves forward additional improvements can be made.

ADAM B. SCHIFF.  
JAMES HIMES.  
JANICE SCHAKOWSKY.  
LUIS V. GUTIERREZ.

