I

113TH CONGRESS
1ST SESSION

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.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 13, 2013

Mr. ROGERS of Michigan (for himself and Mr. RUPPERSBERGER) introduced the following bill; which was referred to the Select Committee on Intelligence (Permanent Select)

A BILL

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

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 de-

partment or agency of the Federal Government receiving cyber threat information in accordance with paragraph (1) shall provide such cyber threat information 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 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, in-

cluding appropriate anonymization or minimization of such information;

''(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) 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

''(D) 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.—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—

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

"(B) for decisions made based on cyber threat information identified, obtained, or shared under this section.

"(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.

''(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;

''(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; or

''(E) to protect the national security of the United States.

''(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)(B).

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

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

''(B) condition the sharing of cyber threat intelligence with a private-sector entity 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):

''(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) PROTECTION OF INDIVIDUAL INFORMATION.—The Federal Government may, consistent with the need to protect Federal systems and critical information infrastructure from cybersecurity threats and to mitigate such threats, undertake reasonable efforts to limit the impact on privacy and civil liberties of the sharing of cyber threat informa-

tion with the Federal Government pursuant to this subsection.

''(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)(C) 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)(C) 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)(C) or subsection (c).

"(e) REPORT ON INFORMATION SHARING.—

"(1) REPORT.—The Inspector General of the Intelligence Community 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) FORM.—Each report required under paragraph (1) 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

"(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.

"(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;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity 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

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity, 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.

''(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 that solely in-

volve 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;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity 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

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity, 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.

''(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 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-governmental 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.''.

(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)(3) 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)(9) of such Act, as added by subsection (a)).

(c) INITIAL REPORT.—The first report required to be submitted under 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.

(d) 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(d) of this Act, is amended by striking the

item relating to section 1104, as added by such section 2(d).

○