[112H3523EH]

(Original Signature of Member)

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

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

---

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".

used, retained or further disclosed by a certified entity only for cybersecurity purposes

"(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

See attached modifications

Suggested amendments to CISPA, H.R. 624 - Starting on page 4, line 13

(b) ~~USE OF~~ CYBERSECURITY ~~SYSTEMS~~ MONITORING AND SHARING OF CYBER THREAT INFORMATION.-

`(1) ~~IN GENERAL~~ MONITORING-

`(A) CYBERSECURITY PROVIDERS- Notwithstanding chapter 119, 121, or 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and sections 222 and 705 of the Communications Act of 1934 (47 U.S.C. 222 and 605), ~~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~~monitor the information systems of such protected entity and information that is stored on, processed by or transiting such information 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 chapter 119, 121, or 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and sections 222 and 705 of the Communications Act of 1934 (47 U.S.C. 222 and 605) ~~any other provision of law~~**, a self-protected entity may, for cybersecurity purposes--**

`(i) ~~use cybersecurity systems~~monitor its information systems and information that is stored on, processed by or transiting such information 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 CYBER THREAT INFORMATION AMONG PRIVATE ENTITIES. –

(A) Notwithstanding chapter 119, 121, or 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and sections 222 and 705 of the Communications Act of 1934 (47 U.S.C. 222 and 605) and title 15, United States Code [and such other provisions of law specifically identified as inhibiting cybersecurity information sharing] ~~any other provision of law~~, any cybersecurity provider that lawfully obtains cyber threat information in the course of providing goods or services to a protected entity for cybersecurity purposes may share such information for cybersecurity purposes with any utility or private entity designated by such protected entity.

(B) Notwithstanding chapter 119, 121, or 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and sections 222 and 705 of the Communications Act of 1934 (47 U.S.C. 222 and 605) and title 15, United States Code [and such other provisions of law specifically identified as inhibiting cybersecurity information sharing]~~any other provision of law~~, any self-protected entity that lawfully obtains cyber threat information in the course of conducting cybersecurity monitoring authorized by

paragraph (1)(B) may share such information for cybersecurity purposes with any utility or private entity.

(3) **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 (4), the head of a department or agency of the Federal Government receiving a cybersecurity provider, with the consent of the entity to which it is providing cybersecurity services, and a self-protected entity may, for cybersecurity purposes, provide cyber threat information acquired 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, only for cybersecurity purposes, provide such information to another department or agency of the Federal Government.

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-

identified, obtained, or

shall only be used, retained or shared for cybersecurity purposes; PB

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~~ 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.

(A) monitoring its own information systems and information that is stored on, processed by or transiting such information systems; or

(B) monitoring the information systems of a protected entity it has been hired to protect, or information stored on, processed by or transiting such information systems

"(c) ~~FEDERAL~~ GOVERNMENT USE OF INFORMATION.—

"(1) LIMITATION.—~~The~~ A Federal ~~Government~~ state, local or tribal entity may use cyber threat information shared with the entity ~~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~~ imminent 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; or

and any ~~similar~~ state, local or tribal equivalent.

~~"(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.

"(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~~ reasonably necessary to describe

"(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; and from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cyber threat.

"(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~~ reasonably necessary to describe

"(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[and from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cyber threat

"(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) Monitor — (see attached)

"(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.

( ) MONITOR.—The term "monitor" means to intercept, acquire, or collect, for cybersecurity purposes, information that is stored on, processed by or transiting an information system.