[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.

- 1 Be it enacted by the Senate and House of Representa-
- 2 tives of the United States of America in Congress assembled,
- 3 SECTION 1. SHORT TITLE.
- 4 This Act may be cited as the "Cyber Intelligence
- 5 Sharing and Protection Act'.

	,
1	"(B) shared consistent with the need to
2	protect the national security of the United
3	States; and
4	"(Q) used by a certified entity in a manner
5	which protects such cyber threat intelligence
6	from unauthorized disclosure.
7	"(3) SECURITY CLEARANCE APPROVALS.—The
8	Director of National Intelligence shall issue guide-
9	lines providing that the head of an element of the
10	intelligence community may, as the head of such ele-
11	ment considers necessary to carry out this sub-
12	section—
13	"(A) grant a security clearance on a tem-
14	porary or permanent basis to an employee or
15	officer of a certified entity;
16	"(B) grant a security clearance on a tem-
17	porary or permanent basis to a certified entity
18	and approval to use appropriate facilities; and
19	"(C) expedite the security clearance proc-
20	ess for a person or entity as the head of such
21	element considers necessary, consistent with the
22	need to protect the national security of the
23	United States.
24	"(4) NO RIGHT OR BENEFIT.—The provision of
25	information to a private-sector entity or a utility

3

1	under this subsection shall not create a right or ben-	
2	efit to similar information by such entity or such	
3	utility or any other private-sector entity or utility.	
4	"(5) RESTRICTION ON DISCLOSURE OF CYBER.	
5	THREAT INTELLIGENCE.—Notwithstanding any	
6	other provision of law, a certified entity receiving	
7	eyler threat intelligence pursuant to this subsection	
8	shall not further disclose such exher threat intel-	
9	ligence to another entity, other than to a certified	
10	entity or other appropriate agency or department of	
11	the Federal Government authorized to receive such	
12	cyber threat intelligence.	
3	(V) USE OF CYBERSECURITY SYSTEMS AND SHAR-	
4	ING OF CREEK THREAT INFORMATION.—	
5	"(NIN GENERAL.—	
6	"A CYBERSECURITY PROVIDERS.—Not-	
7	withstanding any other provision of law a ev-	See
8	bersecurity provider, with the express consent	modifications
9	of a protected entity for which such cybersecu-	modifications
20	rity provider is providing goods or services for	
21	cybersecurity purposes, may for expersecurity	
2	purposes	
23	"(i) use cybersecurity systems to iden-	
4	tify and obtain eyber threat information to	

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-

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;

-(ii) share such cyber-throat 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 eyber 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 land 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 language 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 (43), 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) stall provide such eyber 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.

1	rotect the rights and property of such
2	protected cutity; and
3	"(ii) share such cyber threat informa-
4	tion with any other entity designated by
5	such protected entity, including, if specifi-
6	cally designated, the Federal Government.
7	"(B) SE F-PROTECTED ENTITIES,-Not-
8	withstanding any other provision of law, a self-
9	protected entity may, for eybersecurity pur-
10	poses—
11	"(i) use gypersecurity systems to iden-
12	tily and obtain cyber threat information to
13	protect the rights and property of such
14	self-protected entity; and
15	"(ii) share such ober threat informa-
16	tion with any other entity, including the
17	Federal Government.
18	"(2) SHAMNG WITH THE FEDERAL GOVERN-
19	MENT.—
20	"(A) Information shared with the
21	NATIONAL CYBERSECURITY AND COMMUNICA-
22	TIONS INTEGRATION CENTER OF THE DEPART-
23	MENT OF HOMELAND SECURITY.—Subject to
24	the use and protection of information require-
25	ments under paragraph (3), the head of a de-

1	barranent or agrack of the redeast coccument	
2	receiving cyber threat information in accordance	
3	with paragraph (1) shall provide such cyber	
4	threat information to the National Cybersecu-	
5	rity and Communications Integration Center of	
6	the Department of Nomeland Security.	
7	"(B) REQUEST TO MADE WITH ANOTHER	
8	DEPARTMENT OF AGENCY OF THE PEDERAL	
9	GOVERNMENT An entity shaving cyber threat	
10	information that is provided to the National Cy-	
11	hersecurity and Communications Integration	
12	Center of the Department of Homeland Secu-	
13	rity under subparagraph (A) or paragraph (1)	identified, obtained,
14	may request the head of such Center to, and	•
15	the head of such Center may, provide such it-	or
16	formation to another department or agency of	
17	the Pederal Government.	1
18	"(3) USE AND PROTECTION OF INFORMA-	shall only le
19	TION.—Cyber threat information shared in accord-	shall only le used, netained or shared
20	ance with paragraph (1)—	or shared
21	"(A) shall only be shared in accordance	for abcreecurif
22	with any restrictions placed on the sharing of	Loses, 178
23	such information by the protected entity or self-	
24	protected entity authorizing such sharing, in-	

1	Federal or State court against a protected entity,
2	self-protected entity, cybersecurity provider, or an
3	officer, employee, or agent of a protected entity, self-
4	protected entity, or cybersecurity provider, acting in
5	good faith information information systems and information information information information in stored on, processed
6	((A)) for using cybersecurity systems to 2 by or fransiting such
7	to identify or obtain cyber threat information or or
8	for sharing such information in accordance with information systems
9	this section; or of a protected
10	"(B) for decisions made based on cyber has been hired
11	threat information identified, obtained, or) to protect, or
12	shared under this section. information stored
13	"(5) RELATIONSHIP TO OTHER LAWS REQUIR- or fransiting such
14	ing the disclosure of information.—The sub- information systems
15	mission of information under this subsection to the
16	Federal Government shall not satisfy or affect—
17	"(A) any requirement under any other pro-
18	vision of law for a person or entity to provide
19	information to the Federal Government; or
20	"(B) the applicability of other provisions of
21	law, including section 552 of title 5, United
22	States Code (commonly known as the 'Freedom
23	of Information Act'), with respect to informa-
24	tion required to be provided to the Federal Gov-
25	ernment under such other provision of law.

1	"(c) FEDERAL GOVERNMENT USE OF INFORMA-
2	TION.— PA pstate, local or tribal
3	"(1) LIMITATION.—The Federal Governmental entity
4	may use cyber threat information shared with the entity
5	Federal Government in accordance with subsection
6	(b)—
7	"(A) for cybersecurity purposes;
8	"(B) for the investigation and prosecution
9	of cybersecurity crimes;
10	inminent"(C) for the protection of individuals from
11	the danger of death or serious bodily harm and
12	the investigation and prosecution of crimes in-
13	volving such danger of death or serious bodily
14	harm; or
15	"(D) for the protection of minors from
16	child pornography, any risk of sexual exploi-
17	tation, and serious threats to the physical safe-
18	ty of minors, including kidnapping and traf-
19	ficking and the investigation and prosecution of
20	crimes involving child pornography, any risk of
21	sexual exploitation, and serious threats to the
22	physical safety of minors, including kidnapping
23	and trafficking, and any crime referred to in
24	section 2258A(a)(2) of title 18, United States
25	Code of Q and any sinder state, local or tribal equivalent.

1	"(E) to protect the national security of the
2	United States
3	"(2) AFFIRMATIVE SEARCH RESTRICTION.—
4	The Federal Government may not affirmatively
5	search cyber threat information shared with the
6	Federal Government under subsection (b) for a pur-
7	pose other than a purpose referred to in paragraph
8	(1)(B).
9	"(3) ANTI-TASKING RESTRICTION.—Nothing in
10	this section shall be construed to permit the Federal
11	Government to—
12	"(A) require a private-sector entity to
13	share information with the Federal Govern-
14	ment; or
15	"(B) condition the sharing of cyber threat
16	intelligence with a private-sector entity on the
17	provision of cyber threat information to the
18	Federal Government.
19	"(4) PROTECTION OF SENSITIVE PERSONAL
20	DOCUMENTS.—The Federal Government may not
21	use the following information, containing informa-
22	tion that identifies a person, shared with the Federal
23	Government in accordance with subsection (b):
24	"(A) Library circulation records.
25	"(B) Library patron lists.

1	(6) Use and retention of information.—
2	Nothing in this section shall be construed to author-
3	ize, or to modify any existing authority of, a depart-
4	ment or agency of the Federal Government to retain
5	or use information shared pursuant to subsection
6	(b)(1) for any use other than a use permitted under
7	subsection (c)(1).
8	"(h) DEFINITIONS.—In this section:
9	"(1) AVAILABILITY.—The term 'availability'
10	means ensuring timely and reliable access to and use
11	of information.
12	"(2) CERTIFIED ENTITY.—The term 'certified
13	entity' means a protected entity, self-protected enti-
14	ty, or cybersecurity provider that—
15	"(A) possesses or is eligible to obtain a se-
16	curity clearance, as determined by the Director
17	of National Intelligence; and
18	"(B) is able to demonstrate to the Director
19	of National Intelligence that such provider or
20	such entity can appropriately protect classified
21	cyber threat intelligence.
22	"(3) CONFIDENTIALITY.—The term 'confiden-
23	tiality' means preserving authorized restrictions on
24	access and disclosure, including means for protecting
25	personal privacy and proprietary information.

1	"(4) Cyber threat information,—
2	"(A) IN GENERAL.—The term 'eyber
3	threat information means information directly reasons by
4	portaining to "(i) a vulnerability of a system or not- describe
5	"(i) a vulnerability of a system or net- describe
6	work of a government or private entity:
7	"(ii) a threat to the integrity, con-
8	fidentiality, or availability of a system or
9	network of a government or private entity
10	or any information stored on, processed on,
11	or transiting such a system or network;
12	"(iii) efforts to deny access to or de-
13	grade, disrupt, or destroy a system or net-
14	work of a government or private entity; or
15	"(iv) efforts to gain unauthorized ac-
16	cess to a system or network of a govern-
17	ment or private entity, including to gain
18	such unauthorized access for the purpose
19	of exfiltrating information stored on, proc-
20	essed on, or transiting a system or network
21	of a government or private entity, and from
22	"(B) Exclusion.— Such term does not reasones to
23	include information pertaining to efforts to gain efforts kine
24	unauthorized access to a system or network of feen male to
25	a government or private entity that solely in- intermet:
	that can be used
	•HR 624 IH
	HR 624 IM to identify specific persons unrelated to the cyber threat
	the cyber three

1	volve violations of consumer terms of service or
2	consumer licensing agreements and do not oth-
3	erwise constitute unauthorized access.
4	"(5) CYBER THREAT INTELLIGENCE.—
5	"(A) IN GENERAL.—The term 'cyber
6	threat intelligence' means intelligence in the
7	possession of an element of the intelligence reasonably
8	possession of an element of the intelligence reasonably community directly pertaining to describe
9	"(i) a vulnerability of a system or net-
10	work of a government or private entity;
11	"(ii) a threat to the integrity, con-
12	fidentiality, or availability of a system or
13	network of a government or private entity
14	or any information stored on, processed on,
15	or transiting such a system or network;
16	"(iii) efforts to deny access to or de-
17	grade, disrupt, or destroy a system or net-
18	work of a government or private entity; or
19	"(iv) efforts to gain unauthorized ac-
20	cess to a system or network of a govern-
21	ment or private entity, including to gain
22	such unauthorized access for the purpose
23	of exfiltrating information stored on, proc-
24	essed on, or transiting a system or network
25	of a government or private entity, efforts have seen made
	to remove information
21213.008.xml (10:06 a.m.)	(54038217) that can be used to identify specific persons unrelated to the cyberthreat
	persons unreporca to the cyber threat

1	"(iii) efforts to deny access to or de-
2	grade, disrupt, or destroy a system or net-
3	work; or
4	"(iv) efforts to gain unauthorized ac-
5	cess to a system or network, including to
6	gain such unauthorized access for the pur-
7	pose of exfiltrating information stored on,
8	processed on, or transiting a system or
9	network.
10	"(B) EXCLUSION.— Such term does not
11	include a system designed or employed to pro-
12	tect a system or network from efforts to gain
13	unauthorized access to such system or network
14	that solely involve violations of consumer terms
15	of service or consumer licensing agreements and
16	do not otherwise constitute unauthorized access.
17	"(10) INTEGRITY.—The term 'integrity' means
18	guarding against improper information modification
19	or destruction, including ensuring information non-
20	repudiation and authenticity.
21	repudiation and authenticity. (11) Monitor — (see attached) "(11) PROTECTED ENTITY.—The term 'pro-
22	tected entity' means an entity, other than an indi-
23	vidual, that contracts with a cybersecurity provider
24	for goods or services to be used for cybersecurity
25	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.