

113<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION

# H. R. 624

---

## AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

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

4 **SEC. 2. FEDERAL GOVERNMENT COORDINATION WITH RE-**  
5 **SPECT TO CYBERSECURITY.**

6 (a) **COORDINATED ACTIVITIES.**—The Federal Gov-  
7 ernment shall conduct cybersecurity activities to provide  
8 shared situational awareness that enables integrated oper-  
9 ational actions to protect, prevent, mitigate, respond to,  
10 and recover from cyber incidents.

11 (b) **COORDINATED INFORMATION SHARING.**—

12 (1) **DESIGNATION OF COORDINATING ENTITY**  
13 **FOR CYBER THREAT INFORMATION.**—The President  
14 shall designate an entity within the Department of  
15 Homeland Security as the civilian Federal entity to  
16 receive cyber threat information that is shared by a  
17 cybersecurity provider or self-protected entity in ac-  
18 cordance with section 1104(b) of the National Secu-  
19 rity Act of 1947, as added by section 3(a) of this  
20 Act, except as provided in paragraph (2) and subject  
21 to the procedures established under paragraph (4).

22 (2) **DESIGNATION OF A COORDINATING ENTITY**  
23 **FOR CYBERSECURITY CRIMES.**—The President shall  
24 designate an entity within the Department of Justice  
25 as the civilian Federal entity to receive cyber threat  
26 information related to cybersecurity crimes that is

1 shared by a cybersecurity provider or self-protected  
2 entity in accordance with section 1104(b) of the Na-  
3 tional Security Act of 1947, as added by section 3(a)  
4 of this Act, subject to the procedures under para-  
5 graph (4).

6 (3) SHARING BY COORDINATING ENTITIES.—  
7 The entities designated under paragraphs (1) and  
8 (2) shall share cyber threat information shared with  
9 such entities in accordance with section 1104(b) of  
10 the National Security Act of 1947, as added by sec-  
11 tion 3(a) of this Act, consistent with the procedures  
12 established under paragraphs (4) and (5).

13 (4) PROCEDURES.—Each department or agency  
14 of the Federal Government receiving cyber threat in-  
15 formation shared in accordance with section 1104(b)  
16 of the National Security Act of 1947, as added by  
17 section 3(a) of this Act, shall establish procedures  
18 to—

19 (A) ensure that cyber threat information  
20 shared with departments or agencies of the  
21 Federal Government in accordance with such  
22 section 1104(b) is also shared with appropriate  
23 departments and agencies of the Federal Gov-  
24 ernment with a national security mission in real  
25 time;

1 (B) ensure the distribution to other de-  
2 partments and agencies of the Federal Govern-  
3 ment of cyber threat information in real time;  
4 and

5 (C) facilitate information sharing, inter-  
6 action, and collaboration among and between  
7 the Federal Government; State, local, tribal,  
8 and territorial governments; and cybersecurity  
9 providers and self-protected entities.

10 (5) PRIVACY AND CIVIL LIBERTIES.—

11 (A) POLICIES AND PROCEDURES.—The  
12 Secretary of Homeland Security, the Attorney  
13 General, the Director of National Intelligence,  
14 and the Secretary of Defense shall jointly estab-  
15 lish and periodically review policies and proce-  
16 dures governing the receipt, retention, use, and  
17 disclosure of non-publicly available cyber threat  
18 information shared with the Federal Govern-  
19 ment in accordance with section 1104(b) of the  
20 National Security Act of 1947, as added by sec-  
21 tion 3(a) of this Act. Such policies and proce-  
22 dures shall, consistent with the need to protect  
23 systems and networks from cyber threats and  
24 mitigate cyber threats in a timely manner—

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

3 (ii) reasonably limit the receipt, reten-  
4 tion, use, and disclosure of cyber threat in-  
5 formation associated with specific persons  
6 that is not necessary to protect systems or  
7 networks from cyber threats or mitigate  
8 cyber threats in a timely manner;

9 (iii) include requirements to safeguard  
10 non-publicly available cyber threat infor-  
11 mation that may be used to identify spe-  
12 cific persons from unauthorized access or  
13 acquisition;

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

18 (v) not delay or impede the flow of  
19 cyber threat information necessary to de-  
20 fend against or mitigate a cyber threat.

21 (B) SUBMISSION TO CONGRESS.—The Sec-  
22 retary of Homeland Security, the Attorney Gen-  
23 eral, the Director of National Intelligence, and  
24 the Secretary of Defense shall, consistent with  
25 the need to protect sources and methods, jointly

1 submit to Congress the policies and procedures  
2 required under subparagraph (A) and any up-  
3 dates to such policies and procedures.

4 (C) IMPLEMENTATION.—The head of each  
5 department or agency of the Federal Govern-  
6 ment receiving cyber threat information shared  
7 with the Federal Government under such sec-  
8 tion 1104(b) shall—

9 (i) implement the policies and proce-  
10 dures established under subparagraph (A);  
11 and

12 (ii) promptly notify the Secretary of  
13 Homeland Security, the Attorney General,  
14 the Director of National Intelligence, the  
15 Secretary of Defense, and the appropriate  
16 congressional committees of any significant  
17 violations of such policies and procedures.

18 (D) OVERSIGHT.—The Secretary of Home-  
19 land Security, the Attorney General, the Direc-  
20 tor of National Intelligence, and the Secretary  
21 of Defense shall jointly establish a program to  
22 monitor and oversee compliance with the poli-  
23 cies and procedures established under subpara-  
24 graph (A).

1 (6) INFORMATION SHARING RELATIONSHIPS.—

2 Nothing in this section shall be construed to—

3 (A) alter existing agreements or prohibit  
4 new agreements with respect to the sharing of  
5 cyber threat information between the Depart-  
6 ment of Defense and an entity that is part of  
7 the defense industrial base;

8 (B) alter existing information-sharing rela-  
9 tionships between a cybersecurity provider, pro-  
10 tected entity, or self-protected entity and the  
11 Federal Government;

12 (C) prohibit the sharing of cyber threat in-  
13 formation directly with a department or agency  
14 of the Federal Government for criminal inves-  
15 tigative purposes related to crimes described in  
16 section 1104(c)(1) of the National Security Act  
17 of 1947, as added by section 3(a) of this Act;  
18 or

19 (D) alter existing agreements or prohibit  
20 new agreements with respect to the sharing of  
21 cyber threat information between the Depart-  
22 ment of Treasury and an entity that is part of  
23 the financial services sector.

24 (7) TECHNICAL ASSISTANCE.—

1 (A) DISCUSSIONS AND ASSISTANCE.—  
2 Nothing in this section shall be construed to  
3 prohibit any department or agency of the Fed-  
4 eral Government from engaging in formal or in-  
5 formal technical discussion regarding cyber  
6 threat information with a cybersecurity provider  
7 or self-protected entity or from providing tech-  
8 nical assistance to address vulnerabilities or  
9 mitigate threats at the request of such a pro-  
10 vider or such an entity.

11 (B) COORDINATION.—Any department or  
12 agency of the Federal Government engaging in  
13 an activity referred to in subparagraph (A)  
14 shall coordinate such activity with the entity of  
15 the Department of Homeland Security des-  
16 ignated under paragraph (1) and share all sig-  
17 nificant information resulting from such activity  
18 with such entity and all other appropriate de-  
19 partments and agencies of the Federal Govern-  
20 ment.

21 (C) SHARING BY DESIGNATED ENTITY.—  
22 Consistent with the policies and procedures es-  
23 tablished under paragraph (5), the entity of the  
24 Department of Homeland Security designated  
25 under paragraph (1) shall share with all appro-

1           priate departments and agencies of the Federal  
2           Government all significant information resulting  
3           from—

4                   (i) formal or informal technical dis-  
5                   cussions between such entity of the De-  
6                   partment of Homeland Security and a cy-  
7                   bersecurity provider or self-protected entity  
8                   about cyber threat information; or

9                   (ii) any technical assistance such enti-  
10                  ty of the Department of Homeland Secu-  
11                  rity provides to such cybersecurity provider  
12                  or such self-protected entity to address  
13                  vulnerabilities or mitigate threats.

14           (c) REPORTS ON INFORMATION SHARING.—

15                   (1) INSPECTOR GENERAL OF THE DEPARTMENT  
16                   OF HOMELAND SECURITY REPORT.—The Inspector  
17                   General of the Department of Homeland Security, in  
18                   consultation with the Inspector General of the De-  
19                   partment of Justice, the Inspector General of the In-  
20                   telligence Community, the Inspector General of the  
21                   Department of Defense, and the Privacy and Civil  
22                   Liberties Oversight Board, shall annually submit to  
23                   the appropriate congressional committees a report  
24                   containing a review of the use of information shared  
25                   with the Federal Government under subsection (b)

1 of section 1104 of the National Security Act of  
2 1947, as added by section 3(a) of this Act, includ-  
3 ing—

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

7 (B) a review of the type of information  
8 shared with the Federal Government under  
9 such subsection;

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

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

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

18 (F) a review of the sharing of such infor-  
19 mation within the Federal Government to iden-  
20 tify inappropriate stovepiping of shared infor-  
21 mation; and

22 (G) any recommendations of the Inspector  
23 General of the Department of Homeland Secu-  
24 rity for improvements or modifications to the  
25 authorities under such section.

1           (2) PRIVACY AND CIVIL LIBERTIES OFFICERS  
2           REPORT.—The Officer for Civil Rights and Civil  
3           Liberties of the Department of Homeland Security,  
4           in consultation with the Privacy and Civil Liberties  
5           Oversight Board, the Inspector General of the Intel-  
6           ligence Community, and the senior privacy and civil  
7           liberties officer of each department or agency of the  
8           Federal Government that receives cyber threat infor-  
9           mation shared with the Federal Government under  
10          such subsection (b), shall annually and jointly sub-  
11          mit to Congress a report assessing the privacy and  
12          civil liberties impact of the activities conducted by  
13          the Federal Government under such section 1104.  
14          Such report shall include any recommendations the  
15          Civil Liberties Protection Officer and Chief Privacy  
16          and Civil Liberties Officer consider appropriate to  
17          minimize or mitigate the privacy and civil liberties  
18          impact of the sharing of cyber threat information  
19          under such section 1104.

20          (3) FORM.—Each report required under para-  
21          graph (1) or (2) shall be submitted in unclassified  
22          form, but may include a classified annex.

23          (d) DEFINITIONS.—In this section:

1           (1) APPROPRIATE CONGRESSIONAL COMMIT-  
2           TEES.—The term “appropriate congressional com-  
3           mittees” means—

4                   (A) the Committee on Homeland Security,  
5                   the Committee on the Judiciary, the Permanent  
6                   Select Committee on Intelligence, and the Com-  
7                   mittee on Armed Services of the House of Rep-  
8                   resentatives; and

9                   (B) the Committee on Homeland Security  
10                  and Governmental Affairs, the Committee on  
11                  the Judiciary, the Select Committee on Intel-  
12                  ligence, and the Committee on Armed Services  
13                  of the Senate.

14           (2) CYBER THREAT INFORMATION, CYBER  
15           THREAT INTELLIGENCE, CYBERSECURITY CRIMES,  
16           CYBERSECURITY PROVIDER, CYBERSECURITY PUR-  
17           POSE, AND SELF-PROTECTED ENTITY.—The terms  
18           “cyber threat information”, “cyber threat intel-  
19           ligence”, “cybersecurity crimes”, “cybersecurity pro-  
20           vider”, “cybersecurity purpose”, and “self-protected  
21           entity” have the meaning given those terms in sec-  
22           tion 1104 of the National Security Act of 1947, as  
23           added by section 3(a) of this Act.

24           (3) INTELLIGENCE COMMUNITY.—The term  
25           “intelligence community” has the meaning given the

1 term in section 3(4) of the National Security Act of  
2 1947 (50 U.S.C. 401a(4)).

3 (4) SHARED SITUATIONAL AWARENESS.—The  
4 term “shared situational awareness” means an envi-  
5 ronment where cyber threat information is shared in  
6 real time between all designated Federal cyber oper-  
7 ations centers to provide actionable information  
8 about all known cyber threats.

9 **SEC. 3. CYBER THREAT INTELLIGENCE AND INFORMATION**  
10 **SHARING.**

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

14 “CYBER THREAT INTELLIGENCE AND INFORMATION  
15 SHARING

16 “SEC. 1104. (a) INTELLIGENCE COMMUNITY SHAR-  
17 ING OF CYBER THREAT INTELLIGENCE WITH PRIVATE  
18 SECTOR AND UTILITIES.—

19 “(1) IN GENERAL.—The Director of National  
20 Intelligence shall establish procedures to allow ele-  
21 ments of the intelligence community to share cyber  
22 threat intelligence with private-sector entities and  
23 utilities and to encourage the sharing of such intel-  
24 ligence.

25 “(2) SHARING AND USE OF CLASSIFIED INTEL-  
26 LIGENCE.—The procedures established under para-

1 graph (1) shall provide that classified cyber threat  
2 intelligence may only be—

3 “(A) shared by an element of the intel-  
4 ligence community with—

5 “(i) a certified entity; or

6 “(ii) a person with an appropriate se-  
7 curity clearance to receive such cyber  
8 threat intelligence;

9 “(B) shared consistent with the need to  
10 protect the national security of the United  
11 States;

12 “(C) used by a certified entity in a manner  
13 which protects such cyber threat intelligence  
14 from unauthorized disclosure; and

15 “(D) used, retained, or further disclosed by  
16 a certified entity for cybersecurity purposes.

17 “(3) SECURITY CLEARANCE APPROVALS.—The  
18 Director of National Intelligence shall issue guide-  
19 lines providing that the head of an element of the  
20 intelligence community may, as the head of such ele-  
21 ment considers necessary to carry out this sub-  
22 section—

23 “(A) grant a security clearance on a tem-  
24 porary or permanent basis to an employee,

1 independent contractor, or officer of a certified  
2 entity;

3 “(B) grant a security clearance on a tem-  
4 porary or permanent basis to a certified entity  
5 and approval to use appropriate facilities; and

6 “(C) expedite the security clearance proc-  
7 ess for a person or entity as the head of such  
8 element considers necessary, consistent with the  
9 need to protect the national security of the  
10 United States.

11 “(4) NO RIGHT OR BENEFIT.—The provision of  
12 information to a private-sector entity or a utility  
13 under this subsection shall not create a right or ben-  
14 efit to similar information by such entity or such  
15 utility or any other private-sector entity or utility.

16 “(5) RESTRICTION ON DISCLOSURE OF CYBER  
17 THREAT INTELLIGENCE.—Notwithstanding any  
18 other provision of law, a certified entity receiving  
19 cyber threat intelligence pursuant to this subsection  
20 shall not further disclose such cyber threat intel-  
21 ligence to another entity, other than to a certified  
22 entity or other appropriate agency or department of  
23 the Federal Government authorized to receive such  
24 cyber threat intelligence.

1       “(b) USE OF CYBERSECURITY SYSTEMS AND SHAR-  
2   ING OF CYBER THREAT INFORMATION.—

3               “(1) IN GENERAL.—

4                       “(A) CYBERSECURITY PROVIDERS.—Not-  
5   withstanding any other provision of law, a cy-  
6   bersecurity provider, with the express consent  
7   of a protected entity for which such cybersecu-  
8   rity provider is providing goods or services for  
9   cybersecurity purposes, may, for cybersecurity  
10   purposes—

11                               “(i) use cybersecurity systems to iden-  
12                               tify and obtain cyber threat information to  
13                               protect the rights and property of such  
14                               protected entity; and

15                               “(ii) share such cyber threat informa-  
16                               tion with any other entity designated by  
17                               such protected entity, including, if specifi-  
18                               cally designated, the entities of the Depart-  
19                               ment of Homeland Security and the De-  
20                               partment of Justice designated under  
21                               paragraphs (1) and (2) of section 2(b) of  
22                               the Cyber Intelligence Sharing and Protec-  
23                               tion Act.

24                       “(B) SELF-PROTECTED ENTITIES.—Not-  
25   withstanding any other provision of law, a self-

1           protected entity may, for cybersecurity pur-  
2           poses—

3                   “(i) use cybersecurity systems to iden-  
4                   tify and obtain cyber threat information to  
5                   protect the rights and property of such  
6                   self-protected entity; and

7                   “(ii) share such cyber threat informa-  
8                   tion with any other entity, including the  
9                   entities of the Department of Homeland  
10                  Security and the Department of Justice  
11                  designated under paragraphs (1) and (2)  
12                  of section 2(b) of the Cyber Intelligence  
13                  Sharing and Protection Act.

14                  “(2) USE AND PROTECTION OF INFORMA-  
15                  TION.—Cyber threat information shared in accord-  
16                  ance with paragraph (1)—

17                   “(A) shall only be shared in accordance  
18                   with any restrictions placed on the sharing of  
19                   such information by the protected entity or self-  
20                   protected entity authorizing such sharing, in-  
21                   cluding appropriate anonymization or minimiza-  
22                   tion of such information and excluding limiting  
23                   a department or agency of the Federal Govern-  
24                   ment from sharing such information with an-

1 other department or agency of the Federal Gov-  
2 ernment in accordance with this section;

3 “(B) may not be used by an entity to gain  
4 an unfair competitive advantage to the det-  
5 riment of the protected entity or the self-pro-  
6 tected entity authorizing the sharing of infor-  
7 mation;

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

11 “(D) if shared with the Federal Govern-  
12 ment—

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

17 “(ii) shall be considered proprietary  
18 information and shall not be disclosed to  
19 an entity outside of the Federal Govern-  
20 ment except as authorized by the entity  
21 sharing such information;

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

1           “(iv) shall not be provided to another  
2           department or agency of the Federal Gov-  
3           ernment under paragraph (2)(A) if—

4                   “(I) the entity providing such in-  
5                   formation determines that the provi-  
6                   sion of such information will under-  
7                   mine the purpose for which such in-  
8                   formation is shared; or

9                   “(II) unless otherwise directed by  
10                  the President, the head of the depart-  
11                  ment or agency of the Federal Gov-  
12                  ernment receiving such cyber threat  
13                  information determines that the provi-  
14                  sion of such information will under-  
15                  mine the purpose for which such in-  
16                  formation is shared; and

17           “(v) shall be handled by the Federal  
18           Government consistent with the need to  
19           protect sources and methods and the na-  
20           tional security of the United States; and

21           “(E) shall be exempt from disclosure under  
22           a law or regulation of a State, political subdivi-  
23           sion of a State, or a tribe that requires public  
24           disclosure of information by a public or quasi-  
25           public entity.

1 “(3) EXEMPTION FROM LIABILITY.—

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

9 “(i) for using cybersecurity systems to  
10 identify or obtain cyber threat information  
11 or for sharing such information in accord-  
12 ance with this section; or

13 “(ii) for decisions made for cybersecu-  
14 rity purposes and based on cyber threat in-  
15 formation identified, obtained, or shared  
16 under this section.

17 “(B) LACK OF GOOD FAITH.—For pur-  
18 poses of the exemption from liability under sub-  
19 paragraph (A), a lack of good faith includes  
20 any act or omission taken with intent to injure,  
21 defraud, or otherwise endanger any individual,  
22 government entity, private entity, or utility.

23 “(4) RELATIONSHIP TO OTHER LAWS REQUIR-  
24 ING THE DISCLOSURE OF INFORMATION.—The sub-

1 mission of information under this subsection to the  
2 Federal Government shall not satisfy or affect—

3 “(A) any requirement under any other pro-  
4 vision of law for a person or entity to provide  
5 information to the Federal Government; or

6 “(B) the applicability of other provisions of  
7 law, including section 552 of title 5, United  
8 States Code (commonly known as the ‘Freedom  
9 of Information Act’), with respect to informa-  
10 tion required to be provided to the Federal Gov-  
11 ernment under such other provision of law.

12 “(5) RULE OF CONSTRUCTION.—Nothing in  
13 this subsection shall be construed to provide new au-  
14 thority to—

15 “(A) a cybersecurity provider to use a cy-  
16 bersecurity system to identify or obtain cyber  
17 threat information from a system or network  
18 other than a system or network owned or oper-  
19 ated by a protected entity for which such cyber-  
20 security provider is providing goods or services  
21 for cybersecurity purposes; or

22 “(B) a self-protected entity to use a cyber-  
23 security system to identify or obtain cyber  
24 threat information from a system or network

1           other than a system or network owned or oper-  
2           ated by such self-protected entity.

3           “(c) FEDERAL GOVERNMENT USE OF INFORMA-  
4 TION.—

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

9                   “(A) for cybersecurity purposes;

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

12                   “(C) for the protection of individuals from  
13                   the danger of death or serious bodily harm and  
14                   the investigation and prosecution of crimes in-  
15                   volving such danger of death or serious bodily  
16                   harm; or

17                   “(D) for the protection of minors from  
18                   child pornography, any risk of sexual exploi-  
19                   tation, and serious threats to the physical safe-  
20                   ty of minors, including kidnapping and traf-  
21                   ficking and the investigation and prosecution of  
22                   crimes involving child pornography, any risk of  
23                   sexual exploitation, and serious threats to the  
24                   physical safety of minors, including kidnapping  
25                   and trafficking, and any crime referred to in

1 section 2258A(a)(2) of title 18, United States  
2 Code.

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).

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 or util-  
13 ity to share information with the Federal Gov-  
14 ernment; or

15 “(B) condition the sharing of cyber threat  
16 intelligence with a private-sector entity or util-  
17 ity on the provision of cyber threat information  
18 to the 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 “(C) Book sales records.

2 “(D) Book customer lists.

3 “(E) Firearms sales records.

4 “(F) Tax return records.

5 “(G) Educational records.

6 “(H) Medical records.

7 “(5) NOTIFICATION OF NON-CYBER THREAT IN-  
8 FORMATION.—If a department or agency of the Fed-  
9 eral Government receiving information pursuant to  
10 subsection (b)(1) determines that such information  
11 is not cyber threat information, such department or  
12 agency shall notify the entity or provider sharing  
13 such information pursuant to subsection (b)(1).

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

19 “(d) FEDERAL GOVERNMENT LIABILITY FOR VIOLA-  
20 TIONS OF RESTRICTIONS ON THE DISCLOSURE, USE, AND  
21 PROTECTION OF VOLUNTARILY SHARED INFORMATION.—

22 “(1) IN GENERAL.—If a department or agency  
23 of the Federal Government intentionally or willfully  
24 violates subsection (b)(3)(D) or subsection (c) with  
25 respect to the disclosure, use, or protection of volun-

1       tarily shared cyber threat information shared under  
2       this section, the United States shall be liable to a  
3       person adversely affected by such violation in an  
4       amount equal to the sum of—

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

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

11             “(2) VENUE.—An action to enforce liability cre-  
12             ated under this subsection may be brought in the  
13             district court of the United States in—

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

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

18               “(C) the district in which the department  
19               or agency of the Federal Government that dis-  
20               closed the information is located; or

21               “(D) the District of Columbia.

22             “(3) STATUTE OF LIMITATIONS.—No action  
23             shall lie under this subsection unless such action is  
24             commenced not later than two years after the date

1 of the violation of subsection (b)(3)(D) or subsection  
2 (c) that is the basis for the action.

3 “(4) EXCLUSIVE CAUSE OF ACTION.—A cause  
4 of action under this subsection shall be the exclusive  
5 means available to a complainant seeking a remedy  
6 for a violation of subsection (b)(3)(D) or subsection  
7 (c).

8 “(e) FEDERAL PREEMPTION.—This section super-  
9 sedes any statute of a State or political subdivision of a  
10 State that restricts or otherwise expressly regulates an ac-  
11 tivity authorized under subsection (b).

12 “(f) SAVINGS CLAUSES.—

13 “(1) EXISTING AUTHORITIES.—Nothing in this  
14 section shall be construed to limit any other author-  
15 ity to use a cybersecurity system or to identify, ob-  
16 tain, or share cyber threat intelligence or cyber  
17 threat information.

18 “(2) LIMITATION ON MILITARY AND INTEL-  
19 LIGENCE COMMUNITY INVOLVEMENT IN PRIVATE  
20 AND PUBLIC SECTOR CYBERSECURITY EFFORTS.—  
21 Nothing in this section shall be construed to provide  
22 additional authority to, or modify an existing au-  
23 thority of, the Department of Defense or the Na-  
24 tional Security Agency or any other element of the  
25 intelligence community to control, modify, require,

1 or otherwise direct the cybersecurity efforts of a pri-  
2 vate-sector entity or a component of the Federal  
3 Government or a State, local, or tribal government.

4 “(3) INFORMATION SHARING RELATIONSHIPS.—

5 Nothing in this section shall be construed to—

6 “(A) limit or modify an existing informa-  
7 tion sharing relationship;

8 “(B) prohibit a new information sharing  
9 relationship;

10 “(C) require a new information sharing re-  
11 lationship between the Federal Government and  
12 a private-sector entity or utility;

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

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

21 “(4) LIMITATION ON FEDERAL GOVERNMENT  
22 USE OF CYBERSECURITY SYSTEMS.—Nothing in this  
23 section shall be construed to provide additional au-  
24 thority to, or modify an existing authority of, any  
25 entity to use a cybersecurity system owned or con-

1 trolled by the Federal Government on a private-sec-  
2 tor system or network to protect such private-sector  
3 system or network.

4 “(5) NO LIABILITY FOR NON-PARTICIPATION.—  
5 Nothing in this section shall be construed to subject  
6 a protected entity, self-protected entity, cyber secu-  
7 rity provider, or an officer, employee, or agent of a  
8 protected entity, self-protected entity, or cybersecu-  
9 rity provider, to liability for choosing not to engage  
10 in the voluntary activities authorized under this sec-  
11 tion.

12 “(6) USE AND RETENTION OF INFORMATION.—  
13 Nothing in this section shall be construed to author-  
14 ize, or to modify any existing authority of, a depart-  
15 ment or agency of the Federal Government to retain  
16 or use information shared pursuant to subsection  
17 (b)(1) for any use other than a use permitted under  
18 subsection (c)(1).

19 “(7) LIMITATION ON SURVEILLANCE.—Nothing  
20 in this section shall be construed to authorize the  
21 Department of Defense or the National Security  
22 Agency or any other element of the intelligence com-  
23 munity to target a United States person for surveil-  
24 lance.

25 “(g) DEFINITIONS.—In this section:

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

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

7                   “(A) possesses or is eligible to obtain a se-  
8 curity clearance, as determined by the Director  
9 of National Intelligence; and

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

14           “(3) CONFIDENTIALITY.—The term ‘confiden-  
15 tiality’ means preserving authorized restrictions on  
16 access and disclosure, including means for protecting  
17 personal privacy and proprietary information.

18           “(4) CYBER THREAT INFORMATION.—

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

22                           “(i) a vulnerability of a system or net-  
23 work of a government or private entity or  
24 utility;

1           “(ii) a threat to the integrity, con-  
2           fidentiality, or availability of a system or  
3           network of a government or private entity  
4           or utility or any information stored on,  
5           processed on, or transiting such a system  
6           or network;

7           “(iii) efforts to deny access to or de-  
8           grade, disrupt, or destroy a system or net-  
9           work of a government or private entity or  
10          utility; or

11          “(iv) efforts to gain unauthorized ac-  
12          cess to a system or network of a govern-  
13          ment or private entity or utility, including  
14          to gain such unauthorized access for the  
15          purpose of exfiltrating information stored  
16          on, processed on, or transiting a system or  
17          network of a government or private entity  
18          or utility.

19          “(B) EXCLUSION.—Such term does not in-  
20          clude information pertaining to efforts to gain  
21          unauthorized access to a system or network of  
22          a government or private entity or utility that  
23          solely involve violations of consumer terms of  
24          service or consumer licensing agreements and  
25          do not otherwise constitute unauthorized access.

1           “(5) CYBER THREAT INTELLIGENCE.—

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

6           “(i) a vulnerability of a system or net-  
7 work of a government or private entity or  
8 utility;

9           “(ii) a threat to the integrity, con-  
10 fidentiality, or availability of a system or  
11 network of a government or private entity  
12 or utility or any information stored on,  
13 processed on, or transiting such a system  
14 or network;

15           “(iii) efforts to deny access to or de-  
16 grade, disrupt, or destroy a system or net-  
17 work of a government or private entity or  
18 utility; or

19           “(iv) efforts to gain unauthorized ac-  
20 cess to a system or network of a govern-  
21 ment or private entity or utility, including  
22 to gain such unauthorized access for the  
23 purpose of exfiltrating information stored  
24 on, processed on, or transiting a system or

1 network of a government or private entity  
2 or utility.

3 “(B) EXCLUSION.—Such term does not in-  
4 clude intelligence pertaining to efforts to gain  
5 unauthorized access to a system or network of  
6 a government or private entity or utility that  
7 solely involve violations of consumer terms of  
8 service or consumer licensing agreements and  
9 do not otherwise constitute unauthorized access.

10 “(6) CYBERSECURITY CRIME.—The term ‘cy-  
11 bersecurity crime’ means—

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

14 “(i) efforts to deny access to or de-  
15 grade, disrupt, or destroy a system or net-  
16 work;

17 “(ii) efforts to gain unauthorized ac-  
18 cess to a system or network; or

19 “(iii) efforts to exfiltrate information  
20 from a system or network without author-  
21 ization; or

22 “(B) the violation of a provision of Federal  
23 law relating to computer crimes, including a  
24 violation of any provision of title 18, United  
25 States Code, created or amended by the Com-

1           puter Fraud and Abuse Act of 1986 (Public  
2           Law 99–474).

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

7           “(8) CYBERSECURITY PURPOSE.—

8           “(A) IN GENERAL.—The term ‘cybersecu-  
9           rity purpose’ means the purpose of ensuring the  
10          integrity, confidentiality, or availability of, or  
11          safeguarding, a system or network, including  
12          protecting a system or network from—

13                  “(i) a vulnerability of a system or net-  
14                  work;

15                  “(ii) a threat to the integrity, con-  
16                  fidentiality, or availability of a system or  
17                  network or any information stored on,  
18                  processed on, or transiting such a system  
19                  or network;

20                  “(iii) efforts to deny access to or de-  
21                  grade, disrupt, or destroy a system or net-  
22                  work; or

23                  “(iv) efforts to gain unauthorized ac-  
24                  cess to a system or network, including to  
25                  gain such unauthorized access for the pur-

1           pose of exfiltrating information stored on,  
2           processed on, or transiting a system or  
3           network.

4           “(B) EXCLUSION.—Such term does not in-  
5           clude the purpose of protecting a system or net-  
6           work from efforts to gain unauthorized access  
7           to such system or network that solely involve  
8           violations of consumer terms of service or con-  
9           sumer licensing agreements and do not other-  
10          wise constitute unauthorized access.

11          “(9) CYBERSECURITY SYSTEM.—

12           “(A) IN GENERAL.—The term ‘cybersecu-  
13           rity system’ means a system designed or em-  
14           ployed to ensure the integrity, confidentiality,  
15           or availability of, or safeguard, a system or net-  
16           work, including protecting a system or network  
17           from—

18                   “(i) a vulnerability of a system or net-  
19                   work;

20                   “(ii) a threat to the integrity, con-  
21                   fidentiality, or availability of a system or  
22                   network or any information stored on,  
23                   processed on, or transiting such a system  
24                   or network;

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 in-  
11          clude a system designed or employed to protect  
12          a system or network from efforts to gain unau-  
13          thorized access to such system or network that  
14          solely involve violations of consumer terms of  
15          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          “(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.

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

5           “(13) UTILITY.—The term ‘utility’ means an  
6           entity providing essential services (other than law  
7           enforcement or regulatory services), including elec-  
8           tricity, natural gas, propane, telecommunications,  
9           transportation, water, or wastewater services.”.

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

12           (1) not later than 60 days after the date of the  
13           enactment of this Act, establish procedures under  
14           paragraph (1) of section 1104(a) of the National Se-  
15           curity Act of 1947, as added by subsection (a) of  
16           this section, and issue guidelines under paragraph  
17           (3) of such section 1104(a);

18           (2) in establishing such procedures and issuing  
19           such guidelines, consult with the Secretary of Home-  
20           land Security to ensure that such procedures and  
21           such guidelines permit the owners and operators of  
22           critical infrastructure to receive all appropriate cyber  
23           threat intelligence (as defined in section 1104(h)(5)  
24           of such Act, as added by subsection (a)) in the pos-  
25           session of the Federal Government; and

1           (3) following the establishment of such proce-  
2           dures and the issuance of such guidelines, expedi-  
3           tiously distribute such procedures and such guide-  
4           lines to appropriate departments and agencies of the  
5           Federal Government, private-sector entities, and  
6           utilities (as defined in section 1104(h)(13) of such  
7           Act, as added by subsection (a)).

8           (c) PRIVACY AND CIVIL LIBERTIES POLICIES AND  
9           PROCEDURES.—Not later than 60 days after the date of  
10          the enactment of this Act, the Director of National Intel-  
11          ligence, in consultation with the Secretary of Homeland  
12          Security and the Attorney General, shall establish the poli-  
13          cies and procedures required under section 1104(c)(7)(A)  
14          of the National Security Act of 1947, as added by sub-  
15          section (a) of this section.

16          (d) INITIAL REPORTS.—The first reports required to  
17          be submitted under paragraphs (1) and (2) of subsection  
18          (e) of section 1104 of the National Security Act of 1947,  
19          as added by subsection (a) of this section, shall be sub-  
20          mitted not later than 1 year after the date of the enact-  
21          ment of this Act.

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

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

1 **SEC. 4. SUNSET.**

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

4 (1) section 1104 of the National Security Act of  
5 1947, as added by section 2(a) of this Act, is re-  
6 pealed; and

7 (2) the table of contents in the first section of  
8 the National Security Act of 1947, as amended by  
9 section 2(d) of this Act, is amended by striking the  
10 item relating to section 1104, as added by such sec-  
11 tion 2(d).

12 **SEC. 5. SENSE OF CONGRESS ON INTERNATIONAL CO-**  
13 **OPERATION.**

14 It is the sense of Congress that international coopera-  
15 tion with regard to cybersecurity should be encouraged  
16 wherever possible under this Act and the amendments  
17 made by this Act.

18 **SEC. 6. RULE OF CONSTRUCTION RELATING TO CONSUMER**  
19 **DATA.**

20 Nothing in this Act or the amendments made by this  
21 Act shall be construed to provide new or alter any existing  
22 authority for an entity to sell personal information of a  
23 consumer to another entity for marketing purposes.

1 **SEC. 7. SAVINGS CLAUSE WITH REGARD TO CYBERSECU-**  
2 **RITY PROVIDER OBLIGATION TO REPORT**  
3 **CYBER THREAT INCIDENT INFORMATION TO**  
4 **FEDERAL GOVERNMENT.**

5 Nothing in this Act or the amendments made by this  
6 Act shall be construed to provide authority to a depart-  
7 ment or agency of the Federal Government to require a  
8 cybersecurity provider that has contracted with the Fed-  
9 eral Government to provide information services to provide  
10 information about cybersecurity incidents that do not pose  
11 a threat to the Federal Government's information.

Passed the House of Representatives April 18, 2013.

Attest:

*Clerk.*

113<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION

---

---

# H. R. 624

## AN ACT

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.