

# Union Calendar No. 25

113TH CONGRESS  
1ST SESSION

# H. R. 624

**[Report No. 113-39]**

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)

APRIL 15, 2013

Additional sponsors: Mr. McCAUL, Mr. THORNBERRY, Mr. UPTON, Mr. WALDEN, Mr. WESTMORELAND, Mr. NUNES, Mr. POMPEO, Mr. PETERS of California, Ms. SINEMA, Mr. LANCE, Mr. LOBIONDO, Mr. KING of New York, Mr. HECK of Nevada, Mr. STIVERS, Mr. CONAWAY, Mr. MCHENRY, Mrs. MILLER of Michigan, Mr. GUTHRIE, Mr. KLINE, Mr. SCHOCK, Mr. MULVANEY, Mr. HASTINGS of Washington, Mr. CAMP, Mr. COLE, Mr. KINZINGER of Illinois, Mr. AMODEI, Mr. GRIFFIN of Arkansas, Ms. SEWELL of Alabama, Mr. CUELLAR, Mr. COSTA, Mr. HASTINGS of Florida, Mr. KILMER, Mr. LIPINSKI, Mr. ENYART, Mr. GUTIERREZ, and Mr. VARGAS

APRIL 15, 2013

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italie*]

[For text of introduced bill, see copy of bill as introduced on February 13, 2013]

# **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 Shar-*  
 5 *ing and Protection Act”.*

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

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

11 *“CYBER THREAT INTELLIGENCE AND INFORMATION*  
 12 *SHARING*

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

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

21 *“(2) SHARING AND USE OF CLASSIFIED INTEL-*  
 22 *LIGENCE.—The procedures established under para-*  
 23 *graph (1) shall provide that classified cyber threat in-*  
 24 *telligence may only be—*

25 *“(A) shared by an element of the intel-*  
 26 *ligence community with—*

1                   “(i) a certified entity; or

2                   “(ii) a person with an appropriate se-  
3                   curity clearance to receive such cyber threat  
4                   intelligence;

5                   “(B) shared consistent with the need to pro-  
6                   tect the national security of the United States;  
7                   and

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

11                 “(3) SECURITY CLEARANCE APPROVALS.—The  
12                 Director of National Intelligence shall issue guidelines  
13                 providing that the head of an element of the intel-  
14                 ligence community may, as the head of such element  
15                 considers necessary to carry out this subsection—

16                   “(A) grant a security clearance on a tem-  
17                   porary or permanent basis to an employee or of-  
18                   ficer of a certified entity;

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

22                   “(C) expedite the security clearance process  
23                   for a person or entity as the head of such element  
24                   considers necessary, consistent with the need to

1           *protect the national security of the United*  
2           *States.*

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

8           “(5) *RESTRICTION ON DISCLOSURE OF CYBER*  
9           *THREAT INTELLIGENCE.*—*Notwithstanding any other*  
10          *provision of law, a certified entity receiving cyber*  
11          *threat intelligence pursuant to this subsection shall*  
12          *not further disclose such cyber threat intelligence to*  
13          *another entity, other than to a certified entity or*  
14          *other appropriate agency or department of the Fed-*  
15          *eral Government authorized to receive such cyber*  
16          *threat intelligence.*

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

19                  “(1) *IN GENERAL.*—

20                          “(A) *CYBERSECURITY PROVIDERS.*—*Not-*  
21                          *withstanding any other provision of law, a cy-*  
22                          *bersecurity provider, with the express consent of*  
23                          *a protected entity for which such cybersecurity*  
24                          *provider is providing goods or services for cyber-*

1 security purposes, 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 pro-  
6 tected entity; and

7 “(ii) share such cyber threat informa-  
8 tion with any other entity designated by  
9 such protected entity, including, if specifi-  
10 cally designated, the Federal Government.

11 “(B) *SELF-PROTECTED ENTITIES.*—Not-  
12 withstanding any other provision of law, a self-  
13 protected entity may, for cybersecurity pur-  
14 poses—

15 “(i) use cybersecurity systems to iden-  
16 tify and obtain cyber threat information to  
17 protect the rights and property of such self-  
18 protected entity; and

19 “(ii) share such cyber threat informa-  
20 tion with any other entity, including the  
21 Federal Government.

22 “(2) *SHARING WITH THE FEDERAL GOVERN-*  
23 *MENT.*—

24 “(A) *INFORMATION SHARED WITH THE NA-*  
25 *TIONAL CYBERSECURITY AND COMMUNICATIONS*

1            *INTEGRATION CENTER OF THE DEPARTMENT OF*  
2            *HOMELAND SECURITY.—Subject to the use and*  
3            *protection of information requirements under*  
4            *paragraph (3), the head of a department or*  
5            *agency of the Federal Government receiving*  
6            *cyber threat information in accordance with*  
7            *paragraph (1) shall provide such cyber threat in-*  
8            *formation in as close to real time as possible to*  
9            *the National Cybersecurity and Communications*  
10           *Integration Center of the Department of Home-*  
11           *land Security.*

12                    *“(B) REQUEST TO SHARE WITH ANOTHER*  
13                    *DEPARTMENT OR AGENCY OF THE FEDERAL GOV-*  
14                    *ERNMENT.—An entity sharing cyber threat in-*  
15                    *formation that is provided to the National Cy-*  
16                    *bersecurity and Communications Integration*  
17                    *Center of the Department of Homeland Security*  
18                    *under subparagraph (A) or paragraph (1) may*  
19                    *request the head of such Center to, and the head*  
20                    *of such Center may, provide such information in*  
21                    *as close to real time as possible to another de-*  
22                    *partment or agency of the Federal Government.*

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

1           “(A) shall only be shared in accordance  
2 with any restrictions placed on the sharing of  
3 such information by the protected entity or self-  
4 protected entity authorizing such sharing, in-  
5 cluding appropriate anonymization or mini-  
6 mization of such information and excluding lim-  
7 iting a department or agency of the Federal Gov-  
8 ernment from sharing such information with an-  
9 other department or agency of the Federal Gov-  
10 ernment in accordance with this section;

11           “(B) may not be used by an entity to gain  
12 an unfair competitive advantage to the det-  
13 riment of the protected entity or the self-pro-  
14 tected entity authorizing the sharing of informa-  
15 tion;

16           “(C) may only be used by a non-Federal re-  
17 cipient of such information for a cybersecurity  
18 purpose;

19           “(D) if shared with the Federal Govern-  
20 ment—

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

1           “(ii) shall be considered proprietary  
2 information and shall not be disclosed to an  
3 entity outside of the Federal Government ex-  
4 cept as authorized by the entity sharing  
5 such information;

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

8           “(iv) shall not be provided by the de-  
9 partment or agency of the Federal Govern-  
10 ment receiving such cyber threat informa-  
11 tion to another department or agency of the  
12 Federal Government under paragraph  
13 (2)(A) if—

14           “(I) the entity providing such in-  
15 formation determines that the provi-  
16 sion of such information will under-  
17 mine the purpose for which such infor-  
18 mation is shared; or

19           “(II) unless otherwise directed by  
20 the President, the head of the depart-  
21 ment or agency of the Federal Govern-  
22 ment receiving such cyber threat infor-  
23 mation determines that the provision  
24 of such information will undermine the

1                    *purpose for which such information is*  
2                    *shared; and*

3                    *“(v) shall be handled by the Federal*  
4                    *Government consistent with the need to pro-*  
5                    *tect sources and methods and the national*  
6                    *security of the United States; and*

7                    *“(E) shall be exempt from disclosure under*  
8                    *a State, local, or tribal law or regulation that re-*  
9                    *quires public disclosure of information by a pub-*  
10                    *lic or quasi-public entity.*

11                    *“(4) EXEMPTION FROM LIABILITY.—*

12                    *“(A) EXEMPTION.—No civil or criminal*  
13                    *cause of action shall lie or be maintained in*  
14                    *Federal or State court against a protected entity,*  
15                    *self-protected entity, cybersecurity provider, or*  
16                    *an officer, employee, or agent of a protected enti-*  
17                    *ty, self-protected entity, or cybersecurity pro-*  
18                    *vider, acting in good faith—*

19                    *“(i) for using cybersecurity systems to*  
20                    *identify or obtain cyber threat information*  
21                    *or for sharing such information in accord-*  
22                    *ance with this section; or*

23                    *“(ii) for decisions made for cybersecu-*  
24                    *rity purposes and based on cyber threat in-*

1           *formation identified, obtained, or shared*  
2           *under this section.*

3           “(B) *LACK OF GOOD FAITH.*—*For purposes*  
4           *of the exemption from liability under subpara-*  
5           *graph (A), a lack of good faith includes, but is*  
6           *not limited to, any act or omission taken with*  
7           *intent to injure, defraud, or otherwise endanger*  
8           *any individual, government entity, private enti-*  
9           *ty, or utility.*

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

14                 “(A) *any requirement under any other pro-*  
15                 *vision of law for a person or entity to provide*  
16                 *information to the Federal Government; or*

17                 “(B) *the applicability of other provisions of*  
18                 *law, including section 552 of title 5, United*  
19                 *States Code (commonly known as the ‘Freedom*  
20                 *of Information Act’), with respect to information*  
21                 *required to be provided to the Federal Govern-*  
22                 *ment under such other provision of law.*

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

1           “(A) a cybersecurity provider to use a cy-  
2           bersecurity system to identify or obtain cyber  
3           threat information from a system or network  
4           other than a system or network owned or oper-  
5           ated by a protected entity for which such cyberse-  
6           curity provider is providing goods or services for  
7           cybersecurity purposes; or

8           “(B) a self-protected entity to use a cyberse-  
9           curity system to identify or obtain cyber threat  
10          information from a system or network other than  
11          a system or network owned or operated by such  
12          self-protected entity.

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

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

18                         “(A) *for cybersecurity purposes;*

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

21                         “(C) *for the protection of individuals from*  
22                         *the danger of death or serious bodily harm and*  
23                         *the investigation and prosecution of crimes in-*  
24                         *volving such danger of death or serious bodily*  
25                         *harm; or*

1           “(D) for the protection of minors from child  
2           pornography, any risk of sexual exploitation,  
3           and serious threats to the physical safety of mi-  
4           nors, including kidnapping and trafficking and  
5           the investigation and prosecution of crimes in-  
6           volving child pornography, any risk of sexual ex-  
7           ploitation, and serious threats to the physical  
8           safety of minors, including kidnapping and traf-  
9           ficking, and any crime referred to in section  
10          2258A(a)(2) of title 18, United States Code.

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

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

19                 “(A) require a private-sector entity or util-  
20                 ity to share information with the Federal Gov-  
21                 ernment; or

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

1           “(4) *PROTECTION OF SENSITIVE PERSONAL DOC-*  
2           *UMENTS.—The Federal Government may not use the*  
3           *following information, containing information that*  
4           *identifies a person, shared with the Federal Govern-*  
5           *ment in accordance with subsection (b) unless such*  
6           *information is used in accordance with the policies*  
7           *and procedures established under paragraph (7):*

8                   “(A) *Library circulation records.*

9                   “(B) *Library patron lists.*

10                  “(C) *Book sales records.*

11                  “(D) *Book customer lists.*

12                  “(E) *Firearms sales records.*

13                  “(F) *Tax return records.*

14                  “(G) *Educational records.*

15                  “(H) *Medical records.*

16           “(5) *NOTIFICATION OF NON-CYBER THREAT IN-*  
17           *FORMATION.—If a department or agency of the Fed-*  
18           *eral Government receiving information pursuant to*  
19           *subsection (b)(1) determines that such information is*  
20           *not cyber threat information, such department or*  
21           *agency shall notify the entity or provider sharing*  
22           *such information pursuant to subsection (b)(1).*

23           “(6) *RETENTION AND USE OF CYBER THREAT IN-*  
24           *FORMATION.—No department or agency of the Federal*  
25           *Government shall retain or use information shared*

1       *pursuant to subsection (b)(1) for any use other than*  
2       *a use permitted under subsection (c)(1).*

3           “(7) *PRIVACY AND CIVIL LIBERTIES.*—

4                   “(A) *POLICIES AND PROCEDURES.*—*The Di-*  
5       *rector of National Intelligence, in consultation*  
6       *with the Secretary of Homeland Security and*  
7       *the Attorney General, shall establish and periodi-*  
8       *cally review policies and procedures governing*  
9       *the receipt, retention, use, and disclosure of non-*  
10       *publicly available cyber threat information*  
11       *shared with the Federal Government in accord-*  
12       *ance with subsection (b)(1). Such policies and*  
13       *procedures shall, consistent with the need to pro-*  
14       *tect systems and networks from cyber threats and*  
15       *mitigate cyber threats in a timely manner—*

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

18                           “(ii) *reasonably limit the receipt, re-*  
19       *tention, use, and disclosure of cyber threat*  
20       *information associated with specific persons*  
21       *that is not necessary to protect systems or*  
22       *networks from cyber threats or mitigate*  
23       *cyber threats in a timely manner;*

24                           “(iii) *include requirements to safe-*  
25       *guard non-publicly available cyber threat*

1            *information that may be used to identify*  
2            *specific persons from unauthorized access or*  
3            *acquisition;*

4            *“(iv) protect the confidentiality of*  
5            *cyber threat information associated with*  
6            *specific persons to the greatest extent prac-*  
7            *ticable; and*

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

11           *“(B) SUBMISSION TO CONGRESS.—The Di-*  
12           *rector of National Intelligence shall, consistent*  
13           *with the need to protect sources and methods,*  
14           *submit to Congress the policies and procedures*  
15           *required under subparagraph (A) and any up-*  
16           *dates to such policies and procedures.*

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

22           *“(i) implement the policies and proce-*  
23           *dures established under subparagraph (A);*  
24           *and*

1                   “(ii) promptly notify the Director of  
2                   National Intelligence, the Attorney General,  
3                   and the congressional intelligence commit-  
4                   tees of any significant violations of such  
5                   policies and procedures.

6                   “(D) OVERSIGHT.—The Director of Na-  
7                   tional Intelligence, in consultation with the At-  
8                   torney General, the Secretary of Homeland Secu-  
9                   rity, and the Secretary of Defense, shall establish  
10                  a program to monitor and oversee compliance  
11                  with the policies and procedures established  
12                  under subparagraph (A).

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

16                  “(1) IN GENERAL.—If a department or agency of  
17                  the Federal Government intentionally or willfully vio-  
18                  lates subsection (b)(3)(D) or subsection (c) with re-  
19                  spect to the disclosure, use, or protection of volun-  
20                  tarily shared cyber threat information shared under  
21                  this section, the United States shall be liable to a per-  
22                  son adversely affected by such violation in an amount  
23                  equal to the sum of—

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

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

7           “(2) *VENUE.—An action to enforce liability cre-*  
8           *ated under this subsection may be brought in the dis-*  
9           *trict court of the United States in—*

10           “(A) *the district in which the complainant*  
11           *resides;*

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

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

17           “(D) *the District of Columbia.*

18           “(3) *STATUTE OF LIMITATIONS.—No action shall*  
19           *lie under this subsection unless such action is com-*  
20           *menced not later than two years after the date of the*  
21           *violation of subsection (b)(3)(D) or subsection (c) that*  
22           *is the basis for the action.*

23           “(4) *EXCLUSIVE CAUSE OF ACTION.—A cause of*  
24           *action under this subsection shall be the exclusive*  
25           *means available to a complainant seeking a remedy*

1     *for a violation of subsection (b)(3)(D) or subsection*  
2     *(c).*

3     “(e) *REPORTS ON INFORMATION SHARING.*—

4             “(1) *INSPECTOR GENERAL REPORT.*—*The Inspec-*  
5     *tor General of the Intelligence Community, in con-*  
6     *sultation with the Inspector General of the Depart-*  
7     *ment of Justice, the Inspector General of the Depart-*  
8     *ment of Defense, and the Privacy and Civil Liberties*  
9     *Oversight Board, shall annually submit to the con-*  
10    *gressional intelligence committees a report containing*  
11    *a review of the use of information shared with the*  
12    *Federal Government under this section, including—*

13             “(A) *a review of the use by the Federal Gov-*  
14     *ernment of such information for a purpose other*  
15     *than a cybersecurity purpose;*

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

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

21             “(D) *appropriate metrics to determine the*  
22     *impact of the sharing of such information with*  
23     *the Federal Government on privacy and civil lib-*  
24     *erties, if any;*

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

3           “(F) a review of the sharing of such infor-  
4           mation within the Federal Government to iden-  
5           tify inappropriate stovepiping of shared infor-  
6           mation; and

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

10           “(2) *PRIVACY AND CIVIL LIBERTIES OFFICERS*  
11           *REPORT.*—*The Civil Liberties Protection Officer of*  
12           *the Office of the Director of National Intelligence and*  
13           *the Chief Privacy and Civil Liberties Officer of the*  
14           *Department of Justice, in consultation with the Pri-*  
15           *vacancy and Civil Liberties Oversight Board, the Inspec-*  
16           *tor General of the Intelligence Community, and the*  
17           *senior privacy and civil liberties officer of each de-*  
18           *partment or agency of the Federal Government that*  
19           *receives cyber threat information shared with the Fed-*  
20           *eral Government under this section, shall annually*  
21           *and jointly submit to Congress a report assessing the*  
22           *privacy and civil liberties impact of the activities*  
23           *conducted by the Federal Government under this sec-*  
24           *tion. Such report shall include any recommendations*  
25           *the Civil Liberties Protection Officer and Chief Pri-*

1       *vacy and Civil Liberties Officer consider appropriate*  
2       *to minimize or mitigate the privacy and civil lib-*  
3       *erties impact of the sharing of cyber threat informa-*  
4       *tion under this section.*

5               “(3) *FORM.*—*Each report required under para-*  
6       *graph (1) or (2) shall be submitted in unclassified*  
7       *form, but may include a classified annex.*

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

12               “(g) *SAVINGS CLAUSES.*—

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

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

1 *direct the cybersecurity efforts of a private-sector enti-*  
2 *ty or a component of the Federal Government or a*  
3 *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 of***  
16 ***the United States; or***

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

21 **“(4) LIMITATION ON FEDERAL GOVERNMENT USE**  
22 ***OF CYBERSECURITY SYSTEMS.—Nothing in this sec-***  
23 ***tion shall be construed to provide additional author-***  
24 ***ity to, or modify an existing authority of, any entity***  
25 ***to use a cybersecurity system owned or controlled by***

1       *the Federal Government on a private-sector system or*  
2       *network to protect such private-sector system or net-*  
3       *work.*

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 security*  
7       *provider, or an officer, employee, or agent of a pro-*  
8       *tected entity, self-protected entity, or cybersecurity*  
9       *provider, to liability for choosing not to engage in the*  
10       *voluntary activities authorized under this section.*

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

18               “(h) *DEFINITIONS.*—*In this section:*

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

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

1           “(A) possesses or is eligible to obtain a secu-  
2           rity clearance, as determined by the Director of  
3           National Intelligence; and

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

8           “(3) CONFIDENTIALITY.—The term ‘confiden-  
9           tiality’ means preserving authorized restrictions on  
10          access and disclosure, including means for protecting  
11          personal privacy and proprietary information.

12          “(4) CYBER THREAT INFORMATION.—

13                 “(A) IN GENERAL.—The term ‘cyber threat  
14                 information’ means information directly per-  
15                 taining to—

16                         “(i) a vulnerability of a system or net-  
17                         work of a government or private entity or  
18                         utility;

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

1           “(iii) efforts to deny access to or de-  
2           grade, disrupt, or destroy a system or net-  
3           work of a government or private entity or  
4           utility; or

5           “(iv) efforts to gain unauthorized ac-  
6           cess to a system or network of a government  
7           or private entity or utility, including to  
8           gain such unauthorized access for the pur-  
9           pose of exfiltrating information stored on,  
10          processed on, or transiting a system or net-  
11          work of a government or private entity or  
12          utility.

13          “(B) *EXCLUSION.*—Such term does not in-  
14          clude information pertaining to efforts to gain  
15          unauthorized access to a system or network of a  
16          government or private entity or utility that sole-  
17          ly involve violations of consumer terms of service  
18          or consumer licensing agreements and do not  
19          otherwise constitute unauthorized access.

20          “(5) *CYBER THREAT INTELLIGENCE.*—

21                 “(A) *IN GENERAL.*—The term ‘cyber threat  
22                 intelligence’ means intelligence in the possession  
23                 of an element of the intelligence community di-  
24                 rectly pertaining to—

1           “(i) a vulnerability of a system or net-  
2           work of a government or private entity or  
3           utility;

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

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

14          “(iv) efforts to gain unauthorized ac-  
15          cess to a system or network of a government  
16          or private entity or utility, including to  
17          gain such unauthorized access for the pur-  
18          pose of exfiltrating information stored on,  
19          processed on, or transiting a system or net-  
20          work of a government or private entity or  
21          utility.

22          “(B) *EXCLUSION.*—Such term does not in-  
23          clude intelligence pertaining to efforts to gain  
24          unauthorized access to a system or network of a  
25          government or private entity or utility that sole-

1           *ly involve violations of consumer terms of service*  
2           *or consumer licensing agreements and do not*  
3           *otherwise constitute unauthorized access.*

4           “(6) *CYBERSECURITY CRIME.*—*The term ‘cyber-*  
5           *security crime’ means—*

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

8                           “(i) *efforts to deny access to or de-*  
9                           *grade, disrupt, or destroy a system or net-*  
10                           *work;*

11                           “(ii) *efforts to gain unauthorized ac-*  
12                           *cess to a system or network; or*

13                           “(iii) *efforts to exfiltrate information*  
14                           *from a system or network without author-*  
15                           *ization; or*

16                   “(B) *the violation of a provision of Federal*  
17           *law relating to computer crimes, including a*  
18           *violation of any provision of title 18, United*  
19           *States Code, created or amended by the Com-*  
20           *puter Fraud and Abuse Act of 1986 (Public Law*  
21           *99–474).*

22           “(7) *CYBERSECURITY PROVIDER.*—*The term ‘cy-*  
23           *bersecurity provider’ means a non-Federal entity that*  
24           *provides goods or services intended to be used for cy-*  
25           *bersecurity purposes.*

1           “(8) *CYBERSECURITY PURPOSE.*—

2                   “(A) *IN GENERAL.*—*The term ‘cybersecurity*  
3 *purpose’ means the purpose of ensuring the in-*  
4 *tegrity, confidentiality, or availability of, or*  
5 *safeguarding, a system or network, including*  
6 *protecting a system or network from—*

7                           “(i) *a vulnerability of a system or net-*  
8 *work;*

9                           “(ii) *a threat to the integrity, con-*  
10 *fidentiality, or availability of a system or*  
11 *network or any information stored on, proc-*  
12 *essed on, or transiting such a system or net-*  
13 *work;*

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

17                           “(iv) *efforts to gain unauthorized ac-*  
18 *cess to a system or network, including to*  
19 *gain such unauthorized access for the pur-*  
20 *pose of exfiltrating information stored on,*  
21 *processed on, or transiting a system or net-*  
22 *work.*

23                   “(B) *EXCLUSION.*—*Such term does not in-*  
24 *clude the purpose of protecting a system or net-*  
25 *work from efforts to gain unauthorized access to*

1           *such system or network that solely involve viola-*  
2           *tions of consumer terms of service or consumer*  
3           *licensing agreements and do not otherwise con-*  
4           *stitute unauthorized access.*

5           “(9) *CYBERSECURITY SYSTEM.*—

6           “(A) *IN GENERAL.*—*The term ‘cybersecurity*  
7           *system’ means a system designed or employed to*  
8           *ensure the integrity, confidentiality, or avail-*  
9           *ability of, or safeguard, a system or network, in-*  
10          *cluding protecting a system or network from—*

11                   “(i) *a vulnerability of a system or net-*  
12                   *work;*

13                   “(ii) *a threat to the integrity, con-*  
14                   *fidentiality, or availability of a system or*  
15                   *network or any information stored on, proc-*  
16                   *essed on, or transiting such a system or net-*  
17                   *work;*

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

21                   “(iv) *efforts to gain unauthorized ac-*  
22                   *cess to a system or network, including to*  
23                   *gain such unauthorized access for the pur-*  
24                   *pose of exfiltrating information stored on,*

1                    *processed on, or transiting a system or net-*  
2                    *work.*

3                    “(B) *EXCLUSION.*—*Such term does not in-*  
4                    *clude a system designed or employed to protect*  
5                    *a system or network from efforts to gain unau-*  
6                    *thorized access to such system or network that*  
7                    *solely involve violations of consumer terms of*  
8                    *service or consumer licensing agreements and do*  
9                    *not otherwise constitute unauthorized access.*

10                  “(10) *INTEGRITY.*—*The term ‘integrity’ means*  
11                  *guarding against improper information modification*  
12                  *or destruction, including ensuring information non-*  
13                  *repudiation and authenticity.*

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

18                  “(12) *SELF-PROTECTED ENTITY.*—*The term ‘self-*  
19                  *protected entity’ means an entity, other than an indi-*  
20                  *vidual, that provides goods or services for cybersecu-*  
21                  *rity purposes to itself.*

22                  “(13) *UTILITY.*—*The term ‘utility’ means an en-*  
23                  *tity providing essential services (other than law en-*  
24                  *forcement or regulatory services), including elec-*

1        *tricity, natural gas, propane, telecommunications,*  
2        *transportation, water, or wastewater services.”.*

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

5                *(1) not later than 60 days after the date of the*  
6                *enactment of this Act, establish procedures under*  
7                *paragraph (1) of section 1104(a) of the National Se-*  
8                *curity Act of 1947, as added by subsection (a) of this*  
9                *section, and issue guidelines under paragraph (3) of*  
10               *such section 1104(a);*

11               *(2) in establishing such procedures and issuing*  
12               *such guidelines, consult with the Secretary of Home-*  
13               *land Security to ensure that such procedures and such*  
14               *guidelines permit the owners and operators of critical*  
15               *infrastructure to receive all appropriate cyber threat*  
16               *intelligence (as defined in section 1104(h)(5) of such*  
17               *Act, as added by subsection (a)) in the possession of*  
18               *the Federal Government; and*

19               *(3) following the establishment of such proce-*  
20               *dures and the issuance of such guidelines, expedi-*  
21               *tiously distribute such procedures and such guidelines*  
22               *to appropriate departments and agencies of the Fed-*  
23               *eral Government, private-sector entities, and utilities*  
24               *(as defined in section 1104(h)(13) of such Act, as*  
25               *added by subsection (a)).*

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

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

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

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

19 **SEC. 3. SUNSET.**

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

22                   (1) *section 1104 of the National Security Act of*  
23                   *1947, as added by section 2(a) of this Act, is repealed;*  
24                   *and*

1           (2) *the table of contents in the first section of the*  
2           *National Security Act of 1947, as amended by section*  
3           *2(e) of this Act, is amended by striking the item relat-*  
4           *ing to section 1104, as added by such section 2(e).*

Union Calendar No. 25

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

**H. R. 624**

[Report No. 113-39]

---

---

**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.

---

---

APRIL 15, 2013

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed