

# Union Calendar No. 311

112<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# H. R. 3523

[Report No. 112-445]

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

NOVEMBER 30, 2011

Mr. ROGERS of Michigan (for himself, Mr. RUPPERSBERGER, Mr. KING of New York, Mr. UPTON, Mrs. MYRICK, Mr. LANGEVIN, Mr. CONAWAY, Mr. MILLER of Florida, Mr. BOREN, Mr. LOBIONDO, Mr. CHANDLER, Mr. NUNES, Mr. GUTIERREZ, Mr. WESTMORELAND, Mrs. BACHMANN, Mr. ROONEY, Mr. HECK, Mr. DICKS, Mr. MCCAUL, Mr. WALDEN, Mr. CALVERT, Mr. SHIMKUS, Mr. TERRY, Mr. BURGESS, Mr. GINGREY of Georgia, Mr. THOMPSON of California, Mr. KINZINGER of Illinois, Mr. AMODEI, and Mr. POMPEO) introduced the following bill; which was referred to the Select Committee on Intelligence (Permanent Select)

APRIL 17, 2012

Additional sponsors: Mr. LATTA, Mr. QUAYLE, Mr. MCHENRY, Mr. FRELINGHUYSEN, Mr. YODER, Mr. WALBERG, Mr. CAMP, Ms. ESHOO, Mr. MICHAUD, Mrs. MCMORRIS RODGERS, Mr. SULLIVAN, Mr. MCKINLEY, Ms. ROS-LEHTINEN, Mr. COFFMAN of Colorado, Mr. GOODLATTE, Mr. WOLF, Mr. FORBES, Mr. GARY G. MILLER of California, Mr. STEARNS, Mr. ISSA, Mr. COLE, Mr. TURNER of Ohio, Mr. BROOKS, Mr. HUIZENGA of Michigan, Mr. CARTER, Mrs. HARTZLER, Mr. GRIMM, Mrs. MILLER of Michigan, Mr. GUTHRIE, Mr. ROGERS of Alabama, Mr. BENISHEK, Mr. BROUN of Georgia, Mr. LANCE, Mr. HASTINGS of Washington, Mr. DAVIS of Kentucky, Mr. MEEHAN, Mr. SHUSTER, Mr. OLSON, Mr. KLINE, Mrs. BONO MACK, Mr. BACHUS, Mr. SCHOCK, Mr. ROE of Tennessee, Mr. FLEISCHMANN, Mr. BACA, Mr. BOSWELL, Mrs. NOEM, Mr. WITTMAN, Mr. HULTGREN, Mrs. BLACKBURN, Mr. HASTINGS of Florida, Mr. HURT, Mr. JOHNSON of Ohio, Mr. SMITH of Nebraska, Mr. CRAWFORD, Mr. FRANKS of Arizona, Mr. LARSEN of Washington, Mr. SIRES, Mr. TOWNS, Ms. BORDALLO, Mr. ROSS of Arkansas, Mr. COOPER,

Mr. PITTS, Mr. RUNYAN, Mr. COSTA, Mr. CARDOZA, Mr. WOODALL, Mr. BARTLETT, Mr. SHULER, Mr. STIVERS, Mr. WILSON of South Carolina, Mr. MCINTYRE, Mr. KISSELL, Mr. SCALISE, Mr. BILBRAY, Mr. GRIF-FITH of Virginia, Mr. PETERSON, Mr. OWENS, Mr. MULVANEY, Mr. HALL, Mr. CUELLAR, Mr. LAMBORN, Mr. AUSTRIA, and Mr. MCKEON

APRIL 17, 2012

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 *italic*]

[For text of introduced bill, see copy of bill as introduced on November 30, 2011]

---

## **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 SEC-*  
 15 *TOR.—*

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 to encour-*  
 20 *age 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) certified entities; 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 under this sub-*  
5           *section shall not create a right or benefit to similar*  
6           *information by such entity or any other private-sector*  
7           *entity.*

8           “(b) *PRIVATE SECTOR USE OF CYBERSECURITY SYS-*  
9           *TEMS AND SHARING OF CYBER THREAT INFORMATION.*—

10           “(1) *IN GENERAL.*—

11           “(A) *CYBERSECURITY PROVIDERS.*—*Not-*  
12           *withstanding any other provision of law, a cy-*  
13           *bersecurity provider, with the express consent of*  
14           *a protected entity for which such cybersecurity*  
15           *provider is providing goods or services for cyber-*  
16           *security purposes, may, for cybersecurity pur-*  
17           *poses—*

18                     “(i) *use cybersecurity systems to iden-*  
19                     *tify and obtain cyber threat information to*  
20                     *protect the rights and property of such pro-*  
21                     *tected entity; and*

22                     “(ii) *share such cyber threat informa-*  
23                     *tion with any other entity designated by*  
24                     *such protected entity, including, if specifi-*  
25                     *cally designated, the Federal Government.*

1           “(B) *SELF-PROTECTED ENTITIES.*—Not-  
2           withstanding any other provision of law, a self-  
3           protected entity may, for cybersecurity pur-  
4           poses—

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

9                   “(ii) share such cyber threat informa-  
10                  tion with any other entity, including the  
11                  Federal Government.

12           “(2) *USE AND PROTECTION OF INFORMATION.*—  
13           Cyber threat information shared in accordance with  
14           paragraph (1)—

15                   “(A) shall only be shared in accordance  
16                   with any restrictions placed on the sharing of  
17                   such information by the protected entity or self-  
18                   protected entity authorizing such sharing, in-  
19                   cluding appropriate anonymization or mini-  
20                   mization of such information;

21                   “(B) may not be used by an entity to gain  
22                   an unfair competitive advantage to the det-  
23                   riment of the protected entity or the self-pro-  
24                   tected entity authorizing the sharing of informa-  
25                   tion; and

1           “(C) if shared with the Federal Govern-  
2           ment—

3                   “(i) shall be exempt from disclosure  
4                   under section 552 of title 5, United States  
5                   Code;

6                   “(ii) shall be considered proprietary  
7                   information and shall not be disclosed to an  
8                   entity outside of the Federal Government ex-  
9                   cept as authorized by the entity sharing  
10                  such information; and

11                  “(iii) shall not be used by the Federal  
12                  Government for regulatory purposes.

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

20                   “(A) for using cybersecurity systems or  
21                   sharing information in accordance with this sec-  
22                   tion; or

23                   “(B) for not acting on information obtained  
24                   or shared in accordance with this section.

1           “(4) *RELATIONSHIP TO OTHER LAWS REQUIRING*  
2           *THE DISCLOSURE OF INFORMATION.*—*The submission*  
3           *of information under this subsection to the Federal*  
4           *Government shall not satisfy or affect any require-*  
5           *ment under any other provision of law for a person*  
6           *or entity to provide information to the Federal Gov-*  
7           *ernment.*

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

9           “(1) *LIMITATION.*—*The Federal Government*  
10           *may use cyber threat information shared with the*  
11           *Federal Government in accordance with subsection (b)*  
12           *for any lawful purpose only if—*

13                   “(A) *the use of such information is not for*  
14                   *a regulatory purpose; and*

15                   “(B) *at least one significant purpose of the*  
16                   *use of such information is—*

17                           “(i) *a cybersecurity purpose; or*

18                           “(ii) *the protection of the national se-*  
19                           *curity of the United States.*

20           “(2) *AFFIRMATIVE SEARCH RESTRICTION.*—*The*  
21           *Federal Government may not affirmatively search*  
22           *cyber threat information shared with the Federal*  
23           *Government under subsection (b) for a purpose other*  
24           *than a purpose referred to in paragraph (1)(B).*



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

4                   “(A) *require a private-sector entity to share*  
5 *information with the Federal Government; or*

6                   “(B) *condition the sharing of cyber threat*  
7 *intelligence with a private-sector entity on the*  
8 *provision of cyber threat information to the Fed-*  
9 *eral Government.*

10          “(d) *REPORT ON INFORMATION SHARING.*—

11                   “(1) *REPORT.*—*The Inspector General of the In-*  
12 *telligence Community shall annually submit to the*  
13 *congressional intelligence committees a report con-*  
14 *taining a review of the use of information shared*  
15 *with the Federal Government under this section, in-*  
16 *cluding—*

17                   “(A) *a review of the use by the Federal Gov-*  
18 *ernment of such information for a purpose other*  
19 *than a cybersecurity purpose;*

20                   “(B) *a review of the type of information*  
21 *shared with the Federal Government under this*  
22 *section;*

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

1           “(D) appropriate metrics to determine the  
2           impact of the sharing of such information with  
3           the Federal Government on privacy and civil lib-  
4           erties, if any; and

5           “(E) any recommendations of the Inspector  
6           General for improvements or modifications to the  
7           authorities under this section.

8           “(2) FORM.—Each report required under para-  
9           graph (1) shall be submitted in unclassified form, but  
10          may include a classified annex.

11          “(e) FEDERAL PREEMPTION.—This section supersedes  
12          any statute of a State or political subdivision of a State  
13          that restricts or otherwise expressly regulates an activity  
14          authorized under subsection (b).

15          “(f) SAVINGS CLAUSE.—Nothing in this section shall  
16          be construed to limit any other authority to use a cybersecu-  
17          rity system or to identify, obtain, or share cyber threat in-  
18          telligence or cyber threat information.

19          “(g) DEFINITIONS.—In this section:

20                  “(1) CERTIFIED ENTITY.—The term ‘certified en-  
21                  tity’ means a protected entity, self-protected entity, or  
22                  cybersecurity provider that—

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

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

5           “(2) *CYBER THREAT INFORMATION*.—The term  
6           ‘cyber threat information’ means information directly  
7           pertaining to a vulnerability of, or threat to, a system  
8           or network of a government or private entity, includ-  
9           ing information pertaining to the protection of a sys-  
10          tem or network from—

11           “(A) efforts to degrade, disrupt, or destroy  
12          such system or network; or

13           “(B) theft or misappropriation of private or  
14          government information, intellectual property, or  
15          personally identifiable information.

16          “(3) *CYBER THREAT INTELLIGENCE*.—The term  
17          ‘cyber threat intelligence’ means information in the  
18          possession of an element of the intelligence community  
19          directly pertaining to a vulnerability of, or threat to,  
20          a system or network of a government or private enti-  
21          ty, including information pertaining to the protection  
22          of a system or network from—

23           “(A) efforts to degrade, disrupt, or destroy  
24          such system or network; or

1                   “(B) theft or misappropriation of private or  
2                   government information, intellectual property, or  
3                   personally identifiable information.

4                   “(4) *CYBERSECURITY PROVIDER*.—The term ‘cy-  
5                   bersecurity provider’ means a non-governmental enti-  
6                   ty that provides goods or services intended to be used  
7                   for cybersecurity purposes.

8                   “(5) *CYBERSECURITY PURPOSE*.—The term ‘cy-  
9                   bersecurity purpose’ means the purpose of ensuring  
10                  the integrity, confidentiality, or availability of, or  
11                  safeguarding, a system or network, including pro-  
12                  tecting a system or network from—

13                  “(A) efforts to degrade, disrupt, or destroy  
14                  such system or network; or

15                  “(B) theft or misappropriation of private or  
16                  government information, intellectual property, or  
17                  personally identifiable information.

18                  “(6) *CYBERSECURITY SYSTEM*.—The term ‘cyber-  
19                  security system’ means a system designed or employed  
20                  to ensure the integrity, confidentiality, or availability  
21                  of, or safeguard, a system or network, including pro-  
22                  tecting a system or network from—

23                  “(A) efforts to degrade, disrupt, or destroy  
24                  such system or network; or

1           “(B) theft or misappropriation of private or  
2           government information, intellectual property, or  
3           personally identifiable information.

4           “(7) *PROTECTED ENTITY*.—The term ‘protected  
5           entity’ means an entity, other than an individual,  
6           that contracts with a cybersecurity provider for goods  
7           or services to be used for cybersecurity purposes.

8           “(8) *SELF-PROTECTED ENTITY*.—The term ‘self-  
9           protected entity’ means an entity, other than an indi-  
10          vidual, that provides goods or services for cybersecu-  
11          rity purposes to itself.”

12          (b) *PROCEDURES AND GUIDELINES*.—The Director of  
13          National Intelligence shall—

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

20               (2) following the establishment of such proce-  
21               dures and the issuance of such guidelines, expedi-  
22               tiously distribute such procedures and such guidelines  
23               to appropriate Federal Government and private-sector  
24               entities.

1       (c) *INITIAL REPORT.*—*The first report required to be*  
2 *submitted under subsection (d) of section 1104 of the Na-*  
3 *tional Security Act of 1947, as added by subsection (a) of*  
4 *this section, shall be submitted not later than one year after*  
5 *the date of the enactment of this Act.*

6       (d) *TABLE OF CONTENTS AMENDMENT.*—*The table of*  
7 *contents in the first section of the National Security Act*  
8 *of 1947 is amended by adding at the end the following new*  
9 *item:*

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



Union Calendar No. 311

112<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

**H. R. 3523**

[Report No. 112-445]

---

---

## **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 17, 2012

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