

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

# H. R. 3523

---

## 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. CYBER THREAT INTELLIGENCE AND INFORMATION**  
5 **SHARING.**

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

9 “CYBER THREAT INTELLIGENCE AND INFORMATION  
10 SHARING

11 “SEC. 1104. (a) INTELLIGENCE COMMUNITY SHAR-  
12 ING OF CYBER THREAT INTELLIGENCE WITH PRIVATE  
13 SECTOR AND UTILITIES.—

14 “(1) IN GENERAL.—The Director of National  
15 Intelligence shall establish procedures to allow ele-  
16 ments of the intelligence community to share cyber  
17 threat intelligence with private-sector entities and  
18 utilities and to encourage the sharing of such intel-  
19 ligence.

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

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

26 “(i) certified entities; or

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

4                   “(B) shared consistent with the need to  
5                   protect the national security of the United  
6                   States; and

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

10                  “(3) SECURITY CLEARANCE APPROVALS.—The  
11                  Director of National Intelligence shall issue guide-  
12                  lines providing that the head of an element of the  
13                  intelligence community may, as the head of such ele-  
14                  ment considers necessary to carry out this sub-  
15                  section—

16                         “(A) grant a security clearance on a tem-  
17                         porary or permanent basis to an employee or  
18                         officer 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 proc-  
23                         ess for a person or entity as the head of such  
24                         element considers necessary, consistent with the

1           need to protect the national security of the  
2           United 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  
10          other provision of law, a certified entity receiving  
11          cyber threat intelligence pursuant to this subsection  
12          shall not further disclose such cyber threat intel-  
13          ligence to another entity, other than to a certified  
14          entity or other appropriate agency or department of  
15          the Federal Government authorized to receive such  
16          cyber threat intelligence.

17          “(b) USE OF CYBERSECURITY SYSTEMS AND SHAR-  
18          ING 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  
23                         of a protected entity for which such cybersecu-  
24                         rity provider is providing goods or services for

1 cybersecurity purposes, may, for cybersecurity  
2 purposes—

3 “(i) use cybersecurity systems to iden-  
4 tify and obtain cyber threat information to  
5 protect the rights and property of such  
6 protected 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  
18 self-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  
25 NATIONAL CYBERSECURITY AND COMMUNICA-

1 TIONS INTEGRATION CENTER OF THE DEPART-  
2 MENT OF HOMELAND SECURITY.—Subject to  
3 the use and protection of information require-  
4 ments under paragraph (3), the head of a de-  
5 partment or agency of the Federal Government  
6 receiving cyber threat information in accordance  
7 with paragraph (1) shall provide such cyber  
8 threat information to the National Cybersecu-  
9 rity and Communications Integration Center of  
10 the Department of Homeland Security.

11 “(B) REQUEST TO SHARE WITH ANOTHER  
12 DEPARTMENT OR AGENCY OF THE FEDERAL  
13 GOVERNMENT.—An entity sharing cyber threat  
14 information that is provided to the National Cy-  
15 bersecurity and Communications Integration  
16 Center of the Department of Homeland Secu-  
17 rity under subparagraph (A) or paragraph (1)  
18 may request the head of such Center to, and  
19 the head of such Center may, provide such in-  
20 formation to another department or agency of  
21 the Federal Government.

22 “(3) USE AND PROTECTION OF INFORMA-  
23 TION.—Cyber threat information shared in accord-  
24 ance with 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 minimiza-  
6 tion of such information;

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

12           “(C) if shared with the Federal Govern-  
13 ment—

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

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;

24           “(iv) shall not be provided by the de-  
25 partment or agency of the Federal Govern-

1           ment receiving such cyber threat informa-  
2           tion to another department or agency of  
3           the Federal Government under paragraph  
4           (2)(A) if—

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

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

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

22                   “(D) shall be exempt from disclosure  
23                   under a State, local, or tribal law or regulation  
24                   that requires public disclosure of information by  
25                   a public or quasi-public entity.

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

8           “(A) for using cybersecurity systems to  
9 identify or obtain cyber threat information or  
10 for sharing such information in accordance with  
11 this section; or

12           “(B) for decisions made based on cyber  
13 threat information identified, obtained, or  
14 shared under this section.

15           “(5) RELATIONSHIP TO OTHER LAWS REQUIR-  
16 ING THE DISCLOSURE OF INFORMATION.—The sub-  
17 mission of information under this subsection to the  
18 Federal Government shall not satisfy or affect—

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

22           “(B) the applicability of other provisions of  
23 law, including section 552 of title 5, United  
24 States Code (commonly known as the ‘Freedom  
25 of Information Act’), with respect to informa-

1           tion required to be provided to the Federal Gov-  
2           ernment under such other provision of law.

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;

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 such minor, including kidnapping and  
21           trafficking and the investigation and prosecu-  
22           tion of crimes involving child pornography, any  
23           risk of sexual exploitation, and serious threats  
24           to the physical safety of minors, including kid-  
25           napping and trafficking, and any crime referred

1 to in 2258A(a)(2) of title 18, United States  
2 Code; or

3 “(E) to protect the national security of the  
4 United States.

5 “(2) AFFIRMATIVE SEARCH RESTRICTION.—  
6 The Federal Government may not affirmatively  
7 search cyber threat information shared with the  
8 Federal Government under subsection (b) for a pur-  
9 pose other than a purpose referred to in paragraph  
10 (1)(B).

11 “(3) ANTI-TASKING RESTRICTION.—Nothing in  
12 this section shall be construed to permit the Federal  
13 Government to—

14 “(A) require a private-sector entity to  
15 share information with the Federal Govern-  
16 ment; or

17 “(B) condition the sharing of cyber threat  
18 intelligence with a private-sector entity on the  
19 provision of cyber threat information to the  
20 Federal Government.

21 “(4) PROTECTION OF SENSITIVE PERSONAL  
22 DOCUMENTS.—The Federal Government may not  
23 use the following information, containing informa-  
24 tion that identifies a person, shared with the Federal  
25 Government in accordance with subsection (b):

1 “(A) Library circulation records.

2 “(B) Library patron lists.

3 “(C) Book sales records.

4 “(D) Book customer lists.

5 “(E) Firearms sales records.

6 “(F) Tax return records.

7 “(G) Educational records.

8 “(H) Medical records.

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

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

21 “(7) PROTECTION OF INDIVIDUAL INFORMA-  
22 TION.—The Federal Government may, consistent  
23 with the need to protect Federal systems and critical  
24 information infrastructure from cybersecurity  
25 threats and to mitigate such threats, undertake rea-

1 sonable efforts to limit the impact on privacy and  
2 civil liberties of the sharing of cyber threat informa-  
3 tion with the Federal Government pursuant to this  
4 subsection.

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

8 “(1) IN GENERAL.—If a department or agency  
9 of the Federal Government intentionally or willfully  
10 violates subsection (b)(3)(C) or subsection (c) with  
11 respect to the disclosure, use, or protection of volun-  
12 tarily shared cyber threat information shared under  
13 this section, the United States shall be liable to a  
14 person adversely affected by such violation in an  
15 amount equal to the sum of—

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

19 “(B) the costs of the action together with  
20 reasonable attorney fees as determined by the  
21 court.

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

1           “(A) the district in which the complainant  
2 resides;

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

5           “(C) the district in which the department  
6 or agency of the Federal Government that dis-  
7 closed the information is located; or

8           “(D) the District of Columbia.

9           “(3) STATUTE OF LIMITATIONS.—No action  
10 shall lie under this subsection unless such action is  
11 commenced not later than two years after the date  
12 of the violation of subsection (b)(3)(C) or subsection  
13 (c) that is the basis for the action.

14           “(4) EXCLUSIVE CAUSE OF ACTION.—A cause  
15 of action under this subsection shall be the exclusive  
16 means available to a complainant seeking a remedy  
17 for a violation of subsection (b)(3)(C) or subsection  
18 (c).

19           “(e) REPORT ON INFORMATION SHARING.—

20           “(1) REPORT.—The Inspector General of the  
21 Intelligence Community shall annually submit to the  
22 congressional intelligence committees a report con-  
23 taining a review of the use of information shared  
24 with the Federal Government under this section, in-  
25 cluding—

1           “(A) a review of the use by the Federal  
2 Government of such information for a purpose  
3 other than a cybersecurity purpose;

4           “(B) a review of the type of information  
5 shared with the Federal Government under this  
6 section;

7           “(C) a review of the actions taken by the  
8 Federal Government based on such information;

9           “(D) appropriate metrics to determine the  
10 impact of the sharing of such information with  
11 the Federal Government on privacy and civil  
12 liberties, if any;

13           “(E) a list of the department or agency re-  
14 ceiving such information;

15           “(F) a review of the sharing of such infor-  
16 mation within the Federal Government to iden-  
17 tify inappropriate stovepiping of shared infor-  
18 mation; and

19           “(G) any recommendations of the Inspec-  
20 tor General for improvements or modifications  
21 to the authorities under this section.

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

1       “(f) FEDERAL PREEMPTION.—This section super-  
2 sedes any statute of a State or political subdivision of a  
3 State that restricts or otherwise expressly regulates an ac-  
4 tivity authorized under subsection (b).

5       “(g) SAVINGS CLAUSES.—

6           “(1) EXISTING AUTHORITIES.—Nothing in this  
7 section shall be construed to limit any other author-  
8 ity to use a cybersecurity system or to identify, ob-  
9 tain, or share cyber threat intelligence or cyber  
10 threat information.

11           “(2) LIMITATION ON MILITARY AND INTEL-  
12 LIGENCE COMMUNITY INVOLVEMENT IN PRIVATE  
13 AND PUBLIC SECTOR CYBERSECURITY EFFORTS.—  
14 Nothing in this section shall be construed to provide  
15 additional authority to, or modify an existing au-  
16 thority of, the Department of Defense or the Na-  
17 tional Security Agency or any other element of the  
18 intelligence community to control, modify, require,  
19 or otherwise direct the cybersecurity efforts of a pri-  
20 vate-sector entity or a component of the Federal  
21 Government or a State, local, or tribal government.

22           “(3) INFORMATION SHARING RELATIONSHIPS.—  
23 Nothing in this section shall be construed to—

24           “(A) limit or modify an existing informa-  
25 tion sharing relationship;

1           “(B) prohibit a new information sharing  
2 relationship;

3           “(C) require a new information sharing re-  
4 lationship between the Federal Government and  
5 a private-sector entity; or

6           “(D) modify the authority of a department  
7 or agency of the Federal Government to protect  
8 sources and methods and the national security  
9 of the United States.

10          “(4) LIMITATION ON FEDERAL GOVERNMENT  
11 USE OF CYBERSECURITY SYSTEMS.—Nothing in this  
12 section shall be construed to provide additional au-  
13 thority to, or modify an existing authority of, any  
14 entity to use a cybersecurity system owned or con-  
15 trolled by the Federal Government on a private-sec-  
16 tor system or network to protect such private-sector  
17 system or network.

18          “(5) NO LIABILITY FOR NON-PARTICIPATION.—  
19 Nothing in this section shall be construed to subject  
20 a protected entity, self-protected entity, cyber secu-  
21 rity provider, or an officer, employee, or agent of a  
22 protected entity, self-protected entity, or cybersecu-  
23 rity provider, to liability for choosing not to engage  
24 in the voluntary activities authorized under this sec-  
25 tion.

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

8           “(h) DEFINITIONS.—In this section:

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

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

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

18           “(B) is able to demonstrate to the Director  
19           of National Intelligence that such provider or  
20           such entity can appropriately protect classified  
21           cyber threat intelligence.

22           “(3) CONFIDENTIALITY.—The term ‘confiden-  
23           tiality’ means preserving authorized restrictions on  
24           access and disclosure, including means for protecting  
25           personal privacy and proprietary information.

1 “(4) CYBER THREAT INFORMATION.—

2 “(A) IN GENERAL.—The term ‘cyber  
3 threat information’ means information directly  
4 pertaining to—

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

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

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

15 “(iv) efforts to gain unauthorized ac-  
16 cess to a system or network of a govern-  
17 ment or private entity, including to gain  
18 such unauthorized access for the purpose  
19 of exfiltrating information stored on, proc-  
20 essed on, or transiting a system or network  
21 of a government or private entity.

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

1            involve violations of consumer terms of service or  
2            consumer licensing agreements and do not oth-  
3            erwise constitute unauthorized access.

4            “(5) CYBER THREAT INTELLIGENCE.—

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

9                          “(i) a vulnerability of a system or net-  
10            work of a government or private entity;

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

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

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

1           “(B) EXCLUSION.— Such term does not  
2 include intelligence pertaining to efforts to gain  
3 unauthorized access to a system or network of  
4 a government or private entity that solely in-  
5 volve violations of consumer terms of service or  
6 consumer licensing agreements and do not oth-  
7 erwise constitute unauthorized access.

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

10           “(A) a crime under a Federal or State law  
11 that involves—

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

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

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

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

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

5           “(8) CYBERSECURITY PURPOSE.—

6           “(A) IN GENERAL.—The term ‘cybersecu-  
7           rity purpose’ means the purpose of ensuring the  
8           integrity, confidentiality, or availability of, or  
9           safeguarding, a system or network, including  
10          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,  
16                  processed on, or transiting such a system  
17                  or network;

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  
2           network.

3           “(B) EXCLUSION.— Such term does not  
4           include the purpose of protecting a system or  
5           network from efforts to gain unauthorized ac-  
6           cess to such system or network that solely in-  
7           volve violations of consumer terms of service or  
8           consumer licensing agreements and do not oth-  
9           erwise constitute unauthorized access.

10          “(9) CYBERSECURITY SYSTEM.—

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

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

19                         “(ii) a threat to the integrity, con-  
20                         fidentiality, or availability of a system or  
21                         network or any information stored on,  
22                         processed on, or transiting such a system  
23                         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  
11          include a system designed or employed to pro-  
12          tect a system or network from efforts to gain  
13          unauthorized access to such system or network  
14          that solely involve violations of consumer terms  
15          of service or consumer licensing agreements and  
16          do not otherwise constitute unauthorized access.

17          “(10) INTEGRITY.—The term ‘integrity’ means  
18          guarding against improper information modification  
19          or destruction, including ensuring information non-  
20          repudiation and authenticity.

21          “(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)(3)  
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)(9) of such  
7           Act, as added by subsection (a)).

8           (c) INITIAL REPORT.—The first report required to be  
9           submitted under subsection (e) of section 1104 of the Na-  
10          tional Security Act of 1947, as added by subsection (a)  
11          of this section, shall be submitted not later than 1 year  
12          after the date of the enactment of this Act.

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

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

17          **SEC. 3. SUNSET.**

18          Effective on the date that is 5 years after the date  
19          of the enactment of this Act—

20                 (1) section 1104 of the National Security Act of  
21                 1947, as added by section 2(a) of this Act, is re-  
22                 pealed; and

23                 (2) the table of contents in the first section of  
24                 the National Security Act of 1947, as amended by  
25                 section 2(d) of this Act, is amended by striking the

1 item relating to section 1104, as added by such sec-  
2 tion 2(d).

Passed the House of Representatives April 26, 2012.

Attest:

*Clerk.*

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

---

---

# H. R. 3523

## 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.