

APRIL 19, 2012

RULES COMMITTEE PRINT 112-20
TEXT OF H.R. 3523, THE CYBER INTELLIGENCE
SHARING AND PROTECTION ACT

**[Showing the text of H.R. 3523 as reported with additional
changes recommended by the Chair and Ranking Minority
Member of the Permanent Select Committee on Intelligence]**

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

1 utilities and to encourage the sharing of such intel-
2 ligence.

3 “(2) SHARING AND USE OF CLASSIFIED INTEL-
4 LIGENCE.—The procedures established under para-
5 graph (1) shall provide that classified cyber threat
6 intelligence may only be—

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

9 “(i) certified entities; or

10 “(ii) a person with an appropriate se-
11 curity clearance to receive such cyber
12 threat intelligence;

13 “(B) shared consistent with the need to
14 protect the national security of the United
15 States; and

16 “(C) used by a certified entity in a manner
17 which protects such cyber threat intelligence
18 from unauthorized disclosure.

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

1 “(A) grant a security clearance on a tem-
2 porary or permanent basis to an employee or
3 officer of a certified entity;

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

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

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

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

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

3 “(1) IN GENERAL.—

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

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

15 “(ii) share such cyber threat informa-
16 tion with any other entity designated by
17 such protected entity, including, if specifi-
18 cally designated, the Federal Government.

19 “(B) SELF-PROTECTED ENTITIES.—Not-
20 withstanding any other provision of law, a self-
21 protected entity may, for cybersecurity pur-
22 poses—

23 “(i) use cybersecurity systems to iden-
24 tify and obtain cyber threat information to

1 protect the rights and property of such
2 self-protected entity; and

3 “(ii) share such cyber threat informa-
4 tion with any other entity, including the
5 Federal Government.

6 “(2) SHARING WITH THE FEDERAL GOVERN-
7 MENT.—

8 “(A) INFORMATION SHARED WITH THE
9 NATIONAL CYBERSECURITY AND COMMUNICA-
10 TIONS INTEGRATION CENTER OF THE DEPART-
11 MENT OF HOMELAND SECURITY.—Subject to
12 the use and protection of information require-
13 ments under paragraph (3), the head of a de-
14 partment or agency of the Federal Government
15 receiving cyber threat information in accordance
16 with paragraph (1) shall provide such cyber
17 threat information to the National Cybersecu-
18 rity and Communications Integration Center of
19 the Department of Homeland Security.

20 “(B) REQUEST TO SHARE WITH ANOTHER
21 DEPARTMENT OR AGENCY OF THE FEDERAL
22 GOVERNMENT.—An entity sharing cyber threat
23 information that is provided to the National Cy-
24 bersecurity and Communications Integration
25 Center of the Department of Homeland Secu-

1 rity under subparagraph (A) or paragraph (1)
2 may request the head of such Center to, and
3 the head of such Center may, provide such in-
4 formation to another department or agency of
5 the Federal Government.

6 “(3) USE AND PROTECTION OF INFORMA-
7 TION.—Cyber threat information shared in accord-
8 ance with paragraph (1)—

9 “(A) shall only be shared in accordance
10 with any restrictions placed on the sharing of
11 such information by the protected entity or self-
12 protected entity authorizing such sharing, in-
13 cluding appropriate anonymization or minimiza-
14 tion of such information;

15 “(B) may not be used by an entity to gain
16 an unfair competitive advantage to the det-
17 riment of the protected entity or the self-pro-
18 tected entity authorizing the sharing of infor-
19 mation;

20 “(C) if shared with the Federal Govern-
21 ment—

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

1 “(ii) shall be considered proprietary
2 information and shall not be disclosed to
3 an entity outside of the Federal Govern-
4 ment except as authorized by the entity
5 sharing 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
12 the 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 in-
18 formation is shared; or

19 “(II) unless otherwise directed by
20 the President, the head of the depart-
21 ment or agency of the Federal Gov-
22 ernment receiving such cyber threat
23 information determines that the provi-
24 sion of such information will under-

1 mine the purpose for which such in-
2 formation is shared; and

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

7 “(D) shall be exempt from disclosure
8 under a State, local, or tribal law or regulation
9 that requires public disclosure of information by
10 a public or quasi-public entity.

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

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

21 “(B) for decisions made based on cyber
22 threat information identified, obtained, or
23 shared under this section.

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

1 mission of information under this subsection to the
2 Federal Government shall not satisfy or affect any
3 requirement under any other provision of law for a
4 person or entity to provide information to the Fed-
5 eral Government.

6 “(c) FEDERAL GOVERNMENT USE OF INFORMA-
7 TION.—

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

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

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

16 “(i) a cybersecurity purpose; or

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

19 “(2) AFFIRMATIVE SEARCH RESTRICTION.—
20 The Federal Government may not affirmatively
21 search cyber threat information shared with the
22 Federal Government under subsection (b) for a pur-
23 pose other than a purpose referred to in paragraph
24 (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
5 share information with the Federal Govern-
6 ment; or

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

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

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

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

1 “(B) the costs of the action together with
2 reasonable attorney fees as determined by the
3 court.

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

7 “(A) the district in which the complainant
8 resides;

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

11 “(C) the district in which the department
12 or agency of the Federal Government that dis-
13 closed the information is located; or

14 “(D) the District of Columbia.

15 “(3) STATUTE OF LIMITATIONS.—No action
16 shall lie under this subsection unless such action is
17 commenced not later than two years after the date
18 of the violation of subsection (b)(3)(C) or subsection
19 (c) that is the basis for the action.

20 “(4) EXCLUSIVE CAUSE OF ACTION.—A cause
21 of action under this subsection shall be the exclusive
22 means available to a complainant seeking a remedy
23 for a violation of subsection (b)(3)(C) or subsection
24 (c).

25 “(e) REPORT ON INFORMATION SHARING.—

1 “(1) REPORT.—The Inspector General of the
2 Intelligence Community shall annually submit to the
3 congressional intelligence committees a report con-
4 taining a review of the use of information shared
5 with the Federal Government under this section, in-
6 cluding—

7 “(A) a review of the use by the Federal
8 Government of such information for a purpose
9 other than a cybersecurity purpose;

10 “(B) a review of the type of information
11 shared with the Federal Government under this
12 section;

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

15 “(D) appropriate metrics to determine the
16 impact of the sharing of such information with
17 the Federal Government on privacy and civil
18 liberties, if any;

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

23 “(F) any recommendations of the Inspec-
24 tor General for improvements or modifications
25 to the authorities under this section.

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

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

8 “(g) SAVINGS CLAUSES.—

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

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

1 “(3) INFORMATION SHARING RELATIONSHIPS.—

2 Nothing in this section shall be construed to—

3 “(A) limit or modify an existing informa-
4 tion sharing relationship;

5 “(B) prohibit a new information sharing
6 relationship;

7 “(C) require a new information sharing re-
8 lationship between the Federal Government and
9 a private-sector entity; or

10 “(D) modify the authority of a department
11 or agency of the Federal Government to protect
12 sources and methods and the national security
13 of the United States.

14 “(h) DEFINITIONS.—In this section:

15 “(1) CERTIFIED ENTITY.—The term ‘certified
16 entity’ means a protected entity, self-protected enti-
17 ty, or cybersecurity provider that—

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

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

1 “(2) CYBER THREAT INFORMATION.—The term
2 ‘cyber threat information’ means information di-
3 rectly pertaining to a vulnerability of, or threat to,
4 a system or network of a government or private enti-
5 ty, including information pertaining to the protection
6 of a system or network from—

7 “(A) efforts to degrade, disrupt, or destroy
8 such system or network; or

9 “(B) efforts to gain unauthorized access to
10 a system or network, including efforts to gain
11 such unauthorized access to steal or misappro-
12 priate private or government information.

13 “(3) CYBER THREAT INTELLIGENCE.—The
14 term ‘cyber threat intelligence’ means information in
15 the possession of an element of the intelligence com-
16 munity directly pertaining to a vulnerability of, or
17 threat to, a system or network of a government or
18 private entity, including information pertaining to
19 the protection of a system or network from—

20 “(A) efforts to degrade, disrupt, or destroy
21 such system or network; or

22 “(B) efforts to gain unauthorized access to
23 a system or network, including efforts to gain
24 such unauthorized access to steal or misappro-
25 priate private or government information.

1 “(4) 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 “(5) CYBERSECURITY PURPOSE.—The term ‘cy-
6 bersecurity purpose’ means the purpose of ensuring
7 the integrity, confidentiality, or availability of, or
8 safeguarding, a system or network, including pro-
9 tecting a system or network from—

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

12 “(B) efforts to gain unauthorized access to
13 a system or network, including efforts to gain
14 such unauthorized access to steal or misappro-
15 priate private or government information.

16 “(6) CYBERSECURITY SYSTEM.—The term ‘cy-
17 bersecurity system’ means a system designed or em-
18 ployed to ensure the integrity, confidentiality, or
19 availability of, or safeguard, a system or network,
20 including protecting a system or network from—

21 “(A) efforts to degrade, disrupt, or destroy
22 such system or network; or

23 “(B) efforts to gain unauthorized access to
24 a system or network, including efforts to gain

1 such unauthorized access to steal or misappro-
2 priate private or government information.

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

8 “(8) SELF-PROTECTED ENTITY.—The term
9 ‘self-protected entity’ means an entity, other than an
10 individual, that provides goods or services for cyber-
11 security purposes to itself.

12 “(9) UTILITY.—The term ‘utility’ means an en-
13 tity providing essential services (other than law en-
14 forcement or regulatory services), including elec-
15 tricity, natural gas, propane, telecommunications,
16 transportation, water, or wastewater services.”.

17 (b) PROCEDURES AND GUIDELINES.—The Director
18 of National Intelligence shall—

19 (1) not later than 60 days after the date of the
20 enactment of this Act, establish procedures under
21 paragraph (1) of section 1104(a) of the National Se-
22 curity Act of 1947, as added by subsection (a) of
23 this section, and issue guidelines under paragraph
24 (3) of such section 1104(a);

1 (2) in establishing such procedures and issuing
2 such guidelines, consult with the Secretary of Home-
3 land Security to ensure that such procedures and
4 such guidelines permit the owners and operators of
5 critical infrastructure to receive all appropriate cyber
6 threat intelligence (as defined in section 1104(h)(3)
7 of such Act, as added by subsection (a)) in the pos-
8 session of the Federal Government; and

9 (3) following the establishment of such proce-
10 dures and the issuance of such guidelines, expedi-
11 tiously distribute such procedures and such guide-
12 lines to appropriate departments and agencies of the
13 Federal Government, private-sector entities, and
14 utilities (as defined in section 1104(h)(9) of such
15 Act, as added by subsection (a)).

16 (c) INITIAL REPORT.—The first report required to be
17 submitted under subsection (e) of section 1104 of the Na-
18 tional Security Act of 1947, as added by subsection (a)
19 of this section, shall be submitted not later than one year
20 after the date of the enactment of this Act.

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

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

