

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 3523**

OFFERED BY M__ . _____

Strike all after the enacting clause and insert the
following:

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
6 cybersecurity provider, with the express consent
7 of a protected entity for which such
8 cybersecurity provider is providing goods or
9 services for cybersecurity purposes, may, for
10 cybersecurity 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
18 Cybersecurity and Communications Integration
19 Center of the Department of Homeland Secu-
20 rity.

21 “(B) REQUEST TO SHARE WITH ANOTHER
22 DEPARTMENT OR AGENCY OF THE FEDERAL
23 GOVERNMENT.—An entity sharing cyber threat
24 information that is provided to the National
25 Cybersecurity and Communications Integration

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

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

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

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

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

23 “(i) shall be exempt from disclosure
24 under section 552 of title 5, United States
25 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 the entity providing such infor-
14 mation or the head of the department or
15 agency of the Federal Government receiv-
16 ing such cyber threat information deter-
17 mine that the provision of such informa-
18 tion will undermine the purpose for which
19 such information is shared; and

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

24 “(D) shall be exempt from disclosure
25 under a State, local, or tribal law or regulation

1 that requires public disclosure of information by
2 a public or quasi-public entity.

3 “(4) LIMITATION ON LIABILITY.—

4 “(A) LIMITATION.—No cause of action
5 shall lie in any court against a covered entity
6 that uses a cybersecurity system or shares
7 cyber threat information in accordance with this
8 section for the use of such cybersecurity system,
9 the sharing of cyber threat information, or deci-
10 sions made based on cyber threat information
11 identified, obtained, or shared under this sec-
12 tion, unless such covered entity engages in will-
13 ful misconduct in the sharing of such informa-
14 tion and such willful misconduct proximately
15 causes injury.

16 “(B) PROOF OF WILLFUL MISCONDUCT.—

17 In an action against a covered entity alleging
18 willful misconduct in the sharing of cyber threat
19 information, the plaintiff shall have the burden
20 of proving by clear and convincing evidence the
21 willful misconduct by such covered entity and
22 that such willful misconduct proximately caused
23 injury.

24 “(C) NO NEW CAUSE OF ACTION.—Noth-
25 ing in this section shall be construed to create

1 a cause of action not otherwise existing under
2 law.

3 “(D) DEFINITIONS.—In this paragraph:

4 “(i) COVERED ENTITY.—The term
5 ‘covered entity’ means a protected entity,
6 self-protected entity, or cybersecurity pro-
7 vider, or an officer, employee, or agent of
8 a protected entity, self-protected entity, or
9 cybersecurity provider.

10 “(ii) WILLFUL MISCONDUCT.—The
11 term ‘willful misconduct’ means an act or
12 omission that is made—

13 “(I) intentionally to achieve a
14 wrongful purpose;

15 “(II) knowingly without legal or
16 factual justification; and

17 “(III) in disregard of a known or
18 obvious risk that is so great as to
19 make it highly probable that the harm
20 of the act or omission will outweigh
21 the benefit.

22 “(5) RELATIONSHIP TO OTHER LAWS REQUIR-
23 ING THE DISCLOSURE OF INFORMATION.—The sub-
24 mission of information under this subsection to the
25 Federal Government shall not satisfy or affect any

1 requirement under any other provision of law for a
2 person or entity to provide information to the Fed-
3 eral Government.

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

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

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

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

14 “(i) a cybersecurity purpose; or

15 “(ii) the protection of the national se-
16 curity of the United States.

17 “(2) AFFIRMATIVE SEARCH RESTRICTION.—

18 The Federal Government may not affirmatively
19 search cyber threat information shared with the
20 Federal Government under subsection (b) for a pur-
21 pose other than a purpose referred to in paragraph
22 (1)(B).

23 “(3) ANTI-TASKING RESTRICTION.—Nothing in
24 this section shall be construed to permit the Federal
25 Government to—

1 “(A) require a private-sector entity to
2 share information with the Federal Govern-
3 ment; or

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

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

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

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

22 “(B) the costs of the action together with
23 reasonable attorney fees as determined by the
24 court.

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

4 “(A) the district in which the complainant
5 resides;

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

8 “(C) the district in which the department
9 or agency of the Federal Government that dis-
10 closed the information is located; or

11 “(D) the District of Columbia.

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

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

22 “(e) REPORT ON INFORMATION SHARING.—

23 “(1) REPORT.—The Inspector General of the
24 Intelligence Community shall annually submit to the
25 congressional intelligence committees a report con-

1 taining a review of the use of information shared
2 with the Federal Government under this section, in-
3 cluding—

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

7 “(B) a review of the type of information
8 shared with the Federal Government under this
9 section;

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

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

16 “(E) any recommendations of the Inspec-
17 tor General for improvements or modifications
18 to the authorities under this section.

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

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

1 “(g) SAVINGS CLAUSES.—

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

7 “(2) LIMITATION ON MILITARY AND INTEL-
8 LIGENCE COMMUNITY INVOLVEMENT IN PRIVATE
9 AND PUBLIC SECTOR CYBERSECURITY EFFORTS.—

10 Nothing in this section shall be construed to provide
11 additional authority to, or modify an existing au-
12 thority of, the Department of Defense or the Na-
13 tional Security Agency or any other element of the
14 intelligence community to control, modify, require,
15 or otherwise direct the cybersecurity efforts of a pri-
16 vate-sector entity or a component of the Federal
17 Government or a State, local, or tribal government.

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

20 “(A) limit or modify an existing informa-
21 tion sharing relationship;

22 “(B) prohibit a new information sharing
23 relationship;

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

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

8 “(h) DEFINITIONS.—In this section:

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

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

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

19 “(2) CYBER THREAT INFORMATION.—The term
20 ‘cyber threat information’ means information di-
21 rectly pertaining to a vulnerability of, or threat to,
22 a system or network of a government or private enti-
23 ty, including information pertaining to the protection
24 of a system or network from—

1 “(A) efforts to degrade, disrupt, or destroy
2 such system or network; or

3 “(B) efforts to gain unauthorized access to
4 a system or network, including efforts to gain
5 such unauthorized access to steal or misappro-
6 priate private or government information.

7 “(3) CYBER THREAT INTELLIGENCE.—The
8 term ‘cyber threat intelligence’ means information in
9 the possession of an element of the intelligence com-
10 munity directly pertaining to a vulnerability of, or
11 threat to, a system or network of a government or
12 private entity, including information pertaining to
13 the protection of a system or network from—

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

16 “(B) efforts to gain unauthorized access to
17 a system or network, including efforts to gain
18 such unauthorized access to steal or misappro-
19 priate private or government information.

20 “(4) CYBERSECURITY PROVIDER.—The term
21 ‘cybersecurity provider’ means a non-governmental
22 entity that provides goods or services intended to be
23 used for cybersecurity purposes.

24 “(5) CYBERSECURITY PURPOSE.—The term
25 ‘cybersecurity purpose’ means the purpose of ensur-

1 ing the integrity, confidentiality, or availability of, or
2 safeguarding, a system or network, including pro-
3 tecting a system or network from—

4 “(A) efforts to degrade, disrupt, or destroy
5 such system or network; or

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

10 “(6) CYBERSECURITY SYSTEM.—The term
11 ‘cybersecurity system’ means a system designed or
12 employed to ensure the integrity, confidentiality, or
13 availability of, or safeguard, a system or network,
14 including protecting a system or network from—

15 “(A) efforts to degrade, disrupt, or destroy
16 such system or network; or

17 “(B) efforts to gain unauthorized access to
18 a system or network, including efforts to gain
19 such unauthorized access to steal or misappro-
20 priate private or government information.

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

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

5 “(9) UTILITY.—The term ‘utility’ means an en-
6 tity providing essential services (other than law en-
7 forcement 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 one 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.”.

