

[DISCUSSION DRAFT]112TH CONGRESS
1ST SESSION**H. R.** _____

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

M____. _____ introduced the following bill; which was referred to the
Committee on _____

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
5 Sharing and Protection Act of 2011”.

1 **SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION**
2 **SHARING.**

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

6 “CYBER THREAT INTELLIGENCE AND INFORMATION
7 SHARING

8 “SEC. 1104. (a) INTELLIGENCE COMMUNITY SHAR-
9 ING OF CYBER THREAT INTELLIGENCE WITH PRIVATE
10 SECTOR.—

11 “(1) IN GENERAL.—The Director of National
12 Intelligence shall establish procedures to allow ele-
13 ments of the intelligence community to share cyber
14 threat intelligence with private-sector entities and to
15 encourage the sharing of such intelligence.

16 “(2) SHARING AND USE OF CLASSIFIED INTEL-
17 LIGENCE.—The procedures established under para-
18 graph (1) shall provide that classified cyber threat
19 intelligence may only be—

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

22 “(i) certified entities; or

23 “(ii) a person with an appropriate se-
24 curity clearance to receive such cyber
25 threat intelligence;

1 “(B) shared consistent with the need to
2 protect the national security of the United
3 States; and

4 “(C) used by a certified entity in a manner
5 which protects such cyber threat intelligence
6 from unauthorized disclosure.

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

13 “(A) grant a security clearance on a tem-
14 porary or permanent basis to an employee or
15 officer of a certified entity;

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

19 “(C) expedite the security clearance proc-
20 ess for a person or entity as the head of such
21 element considers necessary, consistent with the
22 need to protect the national security of the
23 United States.

24 “(4) NO RIGHT OR BENEFIT.—The provision of
25 information to a private-sector entity under this sub-

1 section shall not create a right or benefit to similar
2 information by such entity or any other private-sec-
3 tor entity.

4 “(b) PRIVATE SECTOR USE OF CYBERSECURITY SYS-
5 TEMS AND SHARING OF CYBER THREAT INFORMATION.—

6 “(1) IN GENERAL.—

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

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

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

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

1 “(i) use cybersecurity systems to iden-
2 tify and obtain cyber threat information to
3 protect the rights and property of such
4 self-protected entity; and

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

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

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

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

23 “(C) if shared with the Federal Govern-
24 ment—

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

4 “(ii) shall be considered proprietary
5 information and shall not be disclosed to
6 an entity outside of the Federal Govern-
7 ment except as authorized by the entity
8 sharing such information; and

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

11 “(3) 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 not acting on information ob-
22 tained or shared in accordance with this sec-
23 tion.

24 “(4) 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) REPORT ON INFORMATION SHARING.—The Pri-
7 vacy and Civil Liberties Oversight Board established
8 under section 1061 of the Intelligence Reform and Ter-
9 rorism Prevention Act of 2004 (5 U.S.C. 601 note) shall
10 annually submit to Congress a report in unclassified form
11 containing—

12 “(1) a review of the sharing and use of infor-
13 mation by the Federal Government under this sec-
14 tion and the procedures and guidelines established
15 or issued by the Director of National Intelligence
16 under subsection (a); and

17 “(2) any recommendations of the Board for im-
18 provements or modifications to such authorities to
19 address privacy and civil liberties concerns.

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

24 “(e) SAVINGS CLAUSE.—Nothing in this section shall
25 be construed to limit any other authority to use a cyberse-

1 curity system or to identify, obtain, or share cyber threat
2 intelligence or cyber threat information.

3 “(f) DEFINITIONS.—In this section:

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

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

10 “(B) is able to demonstrate to the Director
11 of National Intelligence that such provider or
12 such entity can appropriately protect classified
13 cyber threat intelligence.

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

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

23 “(B) theft or misappropriation of private
24 or government information, intellectual prop-
25 erty, or personally identifiable information.

1 “(3) 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 “(4) 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) theft or misappropriation of private
13 or government information, intellectual prop-
14 erty, or personally identifiable information.

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

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

22 “(B) theft or misappropriation of private
23 or government information, intellectual prop-
24 erty, or personally identifiable information.

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

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

9 “(B) theft or misappropriation of private
10 or government information, intellectual prop-
11 erty, or personally identifiable information.

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

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

21 (b) PROCEDURES AND GUIDELINES.—The Director
22 of National Intelligence shall—

23 (1) not later than 60 days after the date of the
24 enactment of this Act, establish procedures under
25 paragraph (1) of section 1104(a) of the National Se-

1 security Act of 1947, as added by subsection (a) of
2 this section, and issue guidelines under paragraph
3 (3) of such section 1104(a); and

4 (2) following the establishment of such proce-
5 dures and the issuance of such guidelines, expedi-
6 tiously distribute such procedures and such guide-
7 lines to appropriate Federal Government and pri-
8 vate-sector entities;

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

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

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