

117TH CONGRESS
1ST SESSION

S. _____

To amend the Cybersecurity Information Sharing Act of 2015 to include voluntary information sharing of cyber threat indicators among cryptocurrency companies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mrs. BLACKBURN (for herself and Ms. LUMMIS) introduced the following bill;
which was read twice and referred to the Committee on

A BILL

To amend the Cybersecurity Information Sharing Act of 2015 to include voluntary information sharing of cyber threat indicators among cryptocurrency companies, 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 “Cryptocurrency Cyber-
5 security Information Sharing Act”.

1 **SEC. 2. SHARING OF CYBER THREAT INDICATORS BY COV-**
2 **ERED COMPANIES.**

3 (a) IN GENERAL.—The Cybersecurity Information
4 Sharing Act of 2015 (6 U.S.C. 1501 et seq.) is amended—

5 (1) in section 102(15)(A) (6 U.S.C.
6 1501(15)(A)) by inserting “covered company (as de-
7 fined in section 110),” after “cooperative,”;

8 (2) by redesignating sections 110 and 111 (6
9 U.S.C. 1509, 1510) as sections 111 and 112, respec-
10 tively; and

11 (3) by inserting after section 109 (6 U.S.C.
12 1508) the following:

13 **“SEC. 110. SHARING OF CYBER THREAT INDICATORS BY**
14 **COVERED COMPANIES.**

15 “(a) DEFINITIONS.—In this section:

16 “(1) COVERED COMPANY.—

17 “(A) IN GENERAL.—Subject to subpara-
18 graph (B), the term ‘covered company’ means
19 an entity—

20 “(i) that is—

21 “(I) engaged in the business of
22 validating distributed ledger tech-
23 nology transactions;

24 “(II) engaged in the business of
25 developing digital assets or the cor-

1 responding protocols for use of digital
2 assets by other persons;

3 “(III) an association of entities
4 that manage digital assets or distrib-
5 uted ledger technologies; or

6 “(IV) a commercial general liabil-
7 ity insurance provider or property in-
8 surance provider offering products de-
9 signed to mitigate losses from a vari-
10 ety of cyber incidents, including—

11 “(aa) data breaches;

12 “(bb) ransomware attacks;

13 “(cc) business interruption;

14 and

15 “(dd) network damage; and

16 “(ii) that shares or receives informa-
17 tion under this section.

18 “(B) MONEY SERVICES BUSINESSES AND
19 FINANCIAL INSTITUTIONS.—For purposes of
20 paragraphs (1), (2), and (3) of subsection (b),
21 the term ‘covered company’ includes an entity
22 that is a money services business, or that other-
23 wise is a financial institution, as defined in sec-
24 tion 5312 of title 31, United States Code, for

1 purposes of digital asset activity engaged in by
2 the entity.

3 “(2) DIGITAL ASSET.—The term ‘digital asset’
4 means a natively electronic asset that—

5 “(A) confers economic, proprietary, or ac-
6 cess rights or powers; and

7 “(B) is recorded using cryptographically
8 secured distributed ledger technology, or any
9 similar analogue.

10 “(3) DISTRIBUTED LEDGER TECHNOLOGY.—
11 The term ‘distributed ledger technology’ means tech-
12 nology that enables the operation and use of a ledger
13 that—

14 “(A) is shared across a set of distributed
15 nodes that participate in a network and store a
16 complete or partial replica of the ledger;

17 “(B) is synchronized between the nodes;

18 “(C) has data appended to the ledger by
19 following the specified consensus mechanism of
20 the ledger;

21 “(D) may be accessible to anyone or re-
22 stricted to a subset of participants; and

23 “(E) may require participants to have au-
24 thorization to perform certain actions or require
25 no authorization.

1 “(b) VOLUNTARY INFORMATION SHARING AMONG
2 COVERED COMPANIES.—

3 “(1) IN GENERAL.—Subject to paragraphs (2),
4 (3), and (4), a covered company may, under the pro-
5 tection of the safe harbor from liability described in
6 subsection (d), transmit, receive, or otherwise share
7 information with any other covered company regard-
8 ing individuals, entities, organizations, and countries
9 for purposes of identifying and, as appropriate, re-
10 porting activities that the covered company suspects
11 may involve possible cyber threat indicators.

12 “(2) INFORMATION SHARING BETWEEN COV-
13 ERED COMPANIES.—

14 “(A) NOTICE REQUIREMENT.—

15 “(i) IN GENERAL.—A covered com-
16 pany that intends to share information as
17 described in paragraph (1) shall submit a
18 notice of intent to the Financial Crimes
19 Enforcement Network and the Cybersecu-
20 rity and Infrastructure Security Agency,
21 which shall contain, at a minimum, a list
22 of each other company the covered com-
23 pany intends to share information with.

24 “(ii) EFFECTIVE PERIOD.—Each no-
25 tice provided under clause (i) shall be ef-

1 fective for the 1-year period beginning on
2 the date of the notice.

3 “(iii) ADDITIONAL NOTICES.—Upon
4 expiration of the 1-year period described in
5 subclause (ii), a covered company shall
6 submit an additional notice of intent at the
7 beginning of each year during which the
8 covered company intends to share informa-
9 tion as described in paragraph (1).

10 “(iv) LIST OF COVERED COMPANIES
11 THAT HAVE SUBMITTED NOTICE.—The Fi-
12 nancial Crimes Enforcement Network shall
13 periodically make available a list of covered
14 companies that have submitted a notice
15 under this subparagraph.

16 “(B) VERIFICATION REQUIREMENT.—Prior
17 to sharing information as described in para-
18 graph (1), a covered company shall take reason-
19 able steps to verify that the company with
20 which the covered company intends to share in-
21 formation is listed in a notice required under
22 subparagraph (A).

23 “(3) PROTECTION AND USE OF INFORMATION
24 BY COVERED COMPANIES.—

1 “(A) PURPOSE.—Information received by a
2 covered company under this section may not be
3 used for any purpose other than—

4 “(i) identifying and, as appropriate,
5 reporting on cyber threat indicators; or

6 “(ii) assisting the covered company in
7 complying with any requirement of this
8 title.

9 “(B) PROCEDURES FOR PROTECTION OF
10 INFORMATION.—Each covered company that en-
11 gages in the sharing of information under this
12 section shall maintain adequate procedures to
13 protect the security and confidentiality of the
14 information in accordance with the policies and
15 guidelines established under subsection (c).

16 “(4) REPORTING REQUIREMENTS FOR COVERED
17 COMPANIES.—

18 “(A) CYBERSECURITY THREAT INFORMA-
19 TION.—A covered company that identifies cy-
20 bersecurity threat information requiring imme-
21 diate attention, such as suspected terrorist ac-
22 tivity, shall, as soon as practicable but not later
23 than 36 hours after identifying the informa-
24 tion—

1 “(i) notify an appropriate law enforce-
2 ment authority and the Cybersecurity and
3 Infrastructure Security Agency Incident
4 Reporting System; and

5 “(ii) comply with any other Federal
6 requirements for reporting suspicious ac-
7 tivity.

8 “(B) SUSPICIOUS ACTIVITY.—

9 “(i) VOLUNTARY REPORTING TO FED-
10 ERAL AGENCIES.—A covered company may
11 voluntarily report suspicious activity to the
12 Financial Crimes Enforcement Network
13 and the Cybersecurity and Infrastructure
14 Security Agency under this section.

15 “(ii) RULE OF CONSTRUCTION.—
16 Nothing in this subparagraph shall be con-
17 strued to—

18 “(I) modify the requirements for
19 reporting suspicious activity if a cov-
20 ered company is subject to such regu-
21 lations; or

22 “(II) create new suspicious activ-
23 ity reporting requirements for a cov-
24 ered company that is not currently
25 subject to such a regulation.

1 “(C) EXEMPTION FROM DISCLOSURE.—In-
2 formation shared under this paragraph shall be
3 exempt from disclosure under any provision of
4 State, Tribal, or local freedom of information
5 law, open government law, open meetings law,
6 open records law, sunshine law, or similar law
7 requiring disclosure of information or records,
8 in accordance with section 104(d)(4)(B).

9 “(c) INFORMATION SHARING BETWEEN COVERED
10 COMPANIES AND THE FEDERAL GOVERNMENT.—

11 “(1) POLICIES AND PROCEDURES.—

12 “(A) IN GENERAL.—Not later than 180
13 days after the date of enactment of the
14 Cryptocurrency Cybersecurity Information
15 Sharing Act, the Director of the Financial
16 Crimes Enforcement Network and the Director
17 of the Cybersecurity and Infrastructure Secu-
18 rity Agency shall, in consultation with the Na-
19 tional Cyber Director and the heads of the ap-
20 propriate Federal entities, jointly develop and
21 make publicly available policies and procedures
22 relating to the receipt by the Federal Govern-
23 ment of cyber threat indicators shared by cov-
24 ered companies.

1 “(B) CONSIDERATIONS.—In developing the
2 policies and procedures required under subpara-
3 graph (A), the Director of the Financial Crimes
4 Enforcement Network and the Director of the
5 Cybersecurity and Infrastructure Security
6 Agency shall take into account the requirements
7 described in subsections (a)(3) and (b)(3) of
8 section 105.

9 “(C) COMPLIANCE WITH SIMILAR PROCE-
10 DURES.—In the case of a covered company that
11 is required to comply with section 501 of the
12 Gramm-Leach-Bliley Act (15 U.S.C. 6801) and
13 the Payment Card Industry Data Security
14 Standard, and applicable regulations issued
15 thereunder, the covered company shall be con-
16 sidered to be acting in compliance with the re-
17 quirements developed under this subsection if
18 the covered company applies the procedures re-
19 quired under such section 501 to information
20 shared under this section.

21 “(2) GUIDELINES.—

22 “(A) IN GENERAL.—Not later than 60
23 days after the date of enactment of the
24 Cryptocurrency Cybersecurity Information
25 Sharing Act, the Director of the Financial

1 Crimes Enforcement Network and the Director
2 of the Cybersecurity and Infrastructure Security
3 Agency shall jointly develop and make publicly
4 available guidance—

5 “(i) to assist covered companies and
6 promote sharing of cyber threat indicators
7 with Federal entities under this section;
8 and

9 “(ii) relating to adequate procedures
10 to protect the security and confidentiality
11 of information shared under this section,
12 as required under subsection (b)(3)(B).

13 “(B) CONTENTS.—The guidelines required
14 under subparagraph (A) shall include guidance
15 relating to the following:

16 “(i) Identification of types of informa-
17 tion that would qualify as a cyber threat
18 indicator under this title and that would be
19 unlikely to include information that—

20 “(I) is not directly related to a
21 cybersecurity threat; and

22 “(II) is personal information of a
23 specific individual or information that
24 identifies a specific individual.

1 “(ii) Identification of types of infor-
2 mation protected under otherwise applica-
3 ble privacy laws that are unlikely to be di-
4 rectly related to a cybersecurity threat.

5 “(iii) Such other matters as the Di-
6 rector of the Financial Crimes Enforce-
7 ment Network and the Director of the Cy-
8 bersecurity and Infrastructure Security
9 Agency consider appropriate for entities
10 sharing cyber threat indicators with Fed-
11 eral entities under this title.

12 “(3) COMPLIANCE WITH THE PAPERWORK RE-
13 DUCTION ACT.—In establishing requirements under
14 this subsection, the Secretary shall ensure that the
15 requirements comply with chapter 35 of title 44,
16 United States Code (commonly known as the “Pa-
17 perwork Reduction Act”).

18 “(d) SAFE HARBOR FROM CERTAIN LIABILITY.—
19 The liability protections in section 106 shall not apply to
20 a covered company to the extent the company fails to com-
21 ply with paragraphs (2), (3), and (4) of subsection (b).

22 “(e) EXEMPTION FROM DISCLOSURE.—In accord-
23 ance with paragraphs (3) and (8) of section 502(e) of the
24 Gramm-Leach-Bliley Act (15 U.S.C. 6802), if a covered
25 company voluntarily shares information pursuant to this

1 section, the covered company shall not be required to pro-
2 vide any affected consumer the notice required under sec-
3 tion 503 of the Gramm-Leach-Bliley Act (15 U.S.C.
4 6803).”.

5 (b) CONFORMING AMENDMENT.—The table of con-
6 tents in section 1(b) of division N of the Consolidated Ap-
7 propriations Act, 2016 (Public Law 114–113; 129 Stat.
8 2935) is amended by striking the items relating to sections
9 110 and 111 and inserting the following:

“Sec. 110. Sharing of cyber threat indicators by covered companies.

“Sec. 111. Exception to limitation on authority of Secretary of Defense to dis-
seminate certain information.

“Sec. 112. Effective period.”.