

1     **DIVISION N—CYBERSECURITY**  
2                     **ACT OF 2015**

3     **SEC. 1. SHORT TITLE; TABLE OF CONTENTS.**

4             (a) SHORT TITLE.—This division may be cited as the  
5     “Cybersecurity Act of 2015”.

6             (b) TABLE OF CONTENTS.—The table of contents for  
7     this division is as follows:

Sec. 1. Short title; table of contents.

**TITLE I—CYBERSECURITY INFORMATION SHARING**

Sec. 101. Short title.

Sec. 102. Definitions.

Sec. 103. Sharing of information by the Federal Government.

Sec. 104. Authorizations for preventing, detecting, analyzing, and mitigating  
cybersecurity threats.

Sec. 105. Sharing of cyber threat indicators and defensive measures with the  
Federal Government.

Sec. 106. Protection from liability.

Sec. 107. Oversight of Government activities.

Sec. 108. Construction and preemption.

Sec. 109. Report on cybersecurity threats.

Sec. 110. Exception to limitation on authority of Secretary of Defense to dis-  
seminate certain information.

Sec. 111. Effective period.

**TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT**

**Subtitle A—National Cybersecurity and Communications Integration Center**

Sec. 201. Short title.

Sec. 202. Definitions.

Sec. 203. Information sharing structure and processes.

Sec. 204. Information sharing and analysis organizations.

Sec. 205. National response framework.

Sec. 206. Report on reducing cybersecurity risks in DHS data centers.

Sec. 207. Assessment.

Sec. 208. Multiple simultaneous cyber incidents at critical infrastructure.

Sec. 209. Report on cybersecurity vulnerabilities of United States ports.

Sec. 210. Prohibition on new regulatory authority.

Sec. 211. Termination of reporting requirements.

**Subtitle B—Federal Cybersecurity Enhancement**

Sec. 221. Short title.

Sec. 222. Definitions.

Sec. 223. Improved Federal network security.

Sec. 224. Advanced internal defenses.

- Sec. 225. Federal cybersecurity requirements.
- Sec. 226. Assessment; reports.
- Sec. 227. Termination.
- Sec. 228. Identification of information systems relating to national security.
- Sec. 229. Direction to agencies.

#### TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

- Sec. 301. Short title.
- Sec. 302. Definitions.
- Sec. 303. National cybersecurity workforce measurement initiative.
- Sec. 304. Identification of cyber-related work roles of critical need.
- Sec. 305. Government Accountability Office status reports.

#### TITLE IV—OTHER CYBER MATTERS

- Sec. 401. Study on mobile device security.
- Sec. 402. Department of State international cyberspace policy strategy.
- Sec. 403. Apprehension and prosecution of international cyber criminals.
- Sec. 404. Enhancement of emergency services.
- Sec. 405. Improving cybersecurity in the health care industry.
- Sec. 406. Federal computer security.
- Sec. 407. Stopping the fraudulent sale of financial information of people of the United States.

## 1           **TITLE I—CYBERSECURITY** 2           **INFORMATION SHARING**

### 3   **SEC. 101. SHORT TITLE.**

4           This title may be cited as the “Cybersecurity Infor-  
5   mation Sharing Act of 2015”.

### 6   **SEC. 102. DEFINITIONS.**

7           In this title:

8                   (1) **AGENCY.**—The term “agency” has the  
9           meaning given the term in section 3502 of title 44,  
10          United States Code.

11                   (2) **ANTITRUST LAWS.**—The term “antitrust  
12          laws”—

13                           (A) has the meaning given the term in the  
14           first section of the Clayton Act (15 U.S.C. 12);

1 (B) includes section 5 of the Federal  
2 Trade Commission Act (15 U.S.C. 45) to the  
3 extent that section 5 of that Act applies to un-  
4 fair methods of competition; and

5 (C) includes any State antitrust law, but  
6 only to the extent that such law is consistent  
7 with the law referred to in subparagraph (A) or  
8 the law referred to in subparagraph (B).

9 (3) APPROPRIATE FEDERAL ENTITIES.—The  
10 term “appropriate Federal entities” means the fol-  
11 lowing:

12 (A) The Department of Commerce.

13 (B) The Department of Defense.

14 (C) The Department of Energy.

15 (D) The Department of Homeland Secu-  
16 rity.

17 (E) The Department of Justice.

18 (F) The Department of the Treasury.

19 (G) The Office of the Director of National  
20 Intelligence.

21 (4) CYBERSECURITY PURPOSE.—The term  
22 “cybersecurity purpose” means the purpose of pro-  
23 tecting an information system or information that is  
24 stored on, processed by, or transiting an information

1 system from a cybersecurity threat or security vul-  
2 nerability.

3 (5) CYBERSECURITY THREAT.—

4 (A) IN GENERAL.—Except as provided in  
5 subparagraph (B), the term “cybersecurity  
6 threat” means an action, not protected by the  
7 First Amendment to the Constitution of the  
8 United States, on or through an information  
9 system that may result in an unauthorized ef-  
10 fort to adversely impact the security, avail-  
11 ability, confidentiality, or integrity of an infor-  
12 mation system or information that is stored on,  
13 processed by, or transiting an information sys-  
14 tem.

15 (B) EXCLUSION.—The term “cybersecurity  
16 threat” does not include any action that solely  
17 involves a violation of a consumer term of serv-  
18 ice or a consumer licensing agreement.

19 (6) CYBER THREAT INDICATOR.—The term  
20 “cyber threat indicator” means information that is  
21 necessary to describe or identify—

22 (A) malicious reconnaissance, including  
23 anomalous patterns of communications that ap-  
24 pear to be transmitted for the purpose of gath-

1           ering technical information related to a  
2           cybersecurity threat or security vulnerability;

3           (B) a method of defeating a security con-  
4           trol or exploitation of a security vulnerability;

5           (C) a security vulnerability, including  
6           anomalous activity that appears to indicate the  
7           existence of a security vulnerability;

8           (D) a method of causing a user with legiti-  
9           mate access to an information system or infor-  
10          mation that is stored on, processed by, or  
11          transiting an information system to unwittingly  
12          enable the defeat of a security control or exploi-  
13          tation of a security vulnerability;

14          (E) malicious cyber command and control;

15          (F) the actual or potential harm caused by  
16          an incident, including a description of the infor-  
17          mation exfiltrated as a result of a particular  
18          cybersecurity threat;

19          (G) any other attribute of a cybersecurity  
20          threat, if disclosure of such attribute is not oth-  
21          erwise prohibited by law; or

22          (H) any combination thereof.

23       (7) DEFENSIVE MEASURE.—

24           (A) IN GENERAL.—Except as provided in  
25          subparagraph (B), the term “defensive meas-

1           ure” means an action, device, procedure, signa-  
2           ture, technique, or other measure applied to an  
3           information system or information that is  
4           stored on, processed by, or transiting an infor-  
5           mation system that detects, prevents, or miti-  
6           gates a known or suspected cybersecurity threat  
7           or security vulnerability.

8           (B) EXCLUSION.—The term “defensive  
9           measure” does not include a measure that de-  
10          stroys, renders unusable, provides unauthorized  
11          access to, or substantially harms an information  
12          system or information stored on, processed by,  
13          or transiting such information system not  
14          owned by—

15               (i) the private entity operating the  
16               measure; or

17               (ii) another entity or Federal entity  
18               that is authorized to provide consent and  
19               has provided consent to that private entity  
20               for operation of such measure.

21          (8) FEDERAL ENTITY.—The term “Federal en-  
22          tity” means a department or agency of the United  
23          States or any component of such department or  
24          agency.

1           (9) INFORMATION SYSTEM.—The term “infor-  
2           mation system”—

3                   (A) has the meaning given the term in sec-  
4                   tion 3502 of title 44, United States Code; and

5                   (B) includes industrial control systems,  
6                   such as supervisory control and data acquisition  
7                   systems, distributed control systems, and pro-  
8                   grammable logic controllers.

9           (10) LOCAL GOVERNMENT.—The term “local  
10           government” means any borough, city, county, par-  
11           ish, town, township, village, or other political sub-  
12           division of a State.

13           (11) MALICIOUS CYBER COMMAND AND CON-  
14           TROL.—The term “malicious cyber command and  
15           control” means a method for unauthorized remote  
16           identification of, access to, or use of, an information  
17           system or information that is stored on, processed  
18           by, or transiting an information system.

19           (12) MALICIOUS RECONNAISSANCE.—The term  
20           “malicious reconnaissance” means a method for ac-  
21           tively probing or passively monitoring an information  
22           system for the purpose of discerning security  
23           vulnerabilities of the information system, if such  
24           method is associated with a known or suspected  
25           cybersecurity threat.

1           (13) MONITOR.—The term “monitor” means to  
2       acquire, identify, or scan, or to possess, information  
3       that is stored on, processed by, or transiting an in-  
4       formation system.

5           (14) NON-FEDERAL ENTITY.—

6           (A) IN GENERAL.—Except as otherwise  
7       provided in this paragraph, the term “non-Fed-  
8       eral entity” means any private entity, non-Fed-  
9       eral government agency or department, or  
10      State, tribal, or local government (including a  
11      political subdivision, department, or component  
12      thereof).

13          (B) INCLUSIONS.—The term “non-Federal  
14      entity” includes a government agency or depart-  
15      ment of the District of Columbia, the Common-  
16      wealth of Puerto Rico, the United States Virgin  
17      Islands, Guam, American Samoa, the Northern  
18      Mariana Islands, and any other territory or  
19      possession of the United States.

20          (C) EXCLUSION.—The term “non-Federal  
21      entity” does not include a foreign power as de-  
22      fined in section 101 of the Foreign Intelligence  
23      Surveillance Act of 1978 (50 U.S.C. 1801).

24          (15) PRIVATE ENTITY.—



1 (A) IN GENERAL.—Except as otherwise  
2 provided in this paragraph, the term “private  
3 entity” means any person or private group, or-  
4 ganization, proprietorship, partnership, trust,  
5 cooperative, corporation, or other commercial or  
6 nonprofit entity, including an officer, employee,  
7 or agent thereof.

8 (B) INCLUSION.—The term “private enti-  
9 ty” includes a State, tribal, or local government  
10 performing utility services, such as electric, nat-  
11 ural gas, or water services.

12 (C) EXCLUSION.—The term “private enti-  
13 ty” does not include a foreign power as defined  
14 in section 101 of the Foreign Intelligence Sur-  
15 veillance Act of 1978 (50 U.S.C. 1801).

16 (16) SECURITY CONTROL.—The term “security  
17 control” means the management, operational, and  
18 technical controls used to protect against an unau-  
19 thorized effort to adversely affect the confidentiality,  
20 integrity, and availability of an information system  
21 or its information.

22 (17) SECURITY VULNERABILITY.—The term  
23 “security vulnerability” means any attribute of hard-  
24 ware, software, process, or procedure that could en-  
25 able or facilitate the defeat of a security control.

1           (18) TRIBAL.—The term “tribal” has the  
2           meaning given the term “Indian tribe” in section 4  
3           of the Indian Self-Determination and Education As-  
4           sistance Act (25 U.S.C. 450b).

5   **SEC. 103. SHARING OF INFORMATION BY THE FEDERAL**  
6                           **GOVERNMENT.**

7           (a) IN GENERAL.—Consistent with the protection of  
8           classified information, intelligence sources and methods,  
9           and privacy and civil liberties, the Director of National  
10          Intelligence, the Secretary of Homeland Security, the Sec-  
11          retary of Defense, and the Attorney General, in consulta-  
12          tion with the heads of the appropriate Federal entities,  
13          shall jointly develop and issue procedures to facilitate and  
14          promote—

15               (1) the timely sharing of classified cyber threat  
16               indicators and defensive measures in the possession  
17               of the Federal Government with representatives of  
18               relevant Federal entities and non-Federal entities  
19               that have appropriate security clearances;

20               (2) the timely sharing with relevant Federal en-  
21               tities and non-Federal entities of cyber threat indica-  
22               tors, defensive measures, and information relating to  
23               cybersecurity threats or authorized uses under this  
24               title, in the possession of the Federal Government

1       that may be declassified and shared at an unclassi-  
2       fied level;

3           (3) the timely sharing with relevant Federal en-  
4       tities and non-Federal entities, or the public if ap-  
5       propriate, of unclassified, including controlled un-  
6       classified, cyber threat indicators and defensive  
7       measures in the possession of the Federal Govern-  
8       ment;

9           (4) the timely sharing with Federal entities and  
10      non-Federal entities, if appropriate, of information  
11      relating to cybersecurity threats or authorized uses  
12      under this title, in the possession of the Federal  
13      Government about cybersecurity threats to such en-  
14      tities to prevent or mitigate adverse effects from  
15      such cybersecurity threats; and

16          (5) the periodic sharing, through publication  
17      and targeted outreach, of cybersecurity best prac-  
18      tices that are developed based on ongoing analyses  
19      of cyber threat indicators, defensive measures, and  
20      information relating to cybersecurity threats or au-  
21      thorized uses under this title, in the possession of  
22      the Federal Government, with attention to accessi-  
23      bility and implementation challenges faced by small  
24      business concerns (as defined in section 3 of the  
25      Small Business Act (15 U.S.C. 632)).

1 (b) DEVELOPMENT OF PROCEDURES.—

2 (1) IN GENERAL.—The procedures developed  
3 under subsection (a) shall—

4 (A) ensure the Federal Government has  
5 and maintains the capability to share cyber  
6 threat indicators and defensive measures in real  
7 time consistent with the protection of classified  
8 information;

9 (B) incorporate, to the greatest extent  
10 practicable, existing processes and existing roles  
11 and responsibilities of Federal entities and non-  
12 Federal entities for information sharing by the  
13 Federal Government, including sector specific  
14 information sharing and analysis centers;

15 (C) include procedures for notifying, in a  
16 timely manner, Federal entities and non-Fed-  
17 eral entities that have received a cyber threat  
18 indicator or defensive measure from a Federal  
19 entity under this title that is known or deter-  
20 mined to be in error or in contravention of the  
21 requirements of this title or another provision  
22 of Federal law or policy of such error or con-  
23 travention;

24 (D) include requirements for Federal enti-  
25 ties sharing cyber threat indicators or defensive

1 measures to implement and utilize security con-  
2 trols to protect against unauthorized access to  
3 or acquisition of such cyber threat indicators or  
4 defensive measures;

5 (E) include procedures that require a Fed-  
6 eral entity, prior to the sharing of a cyber  
7 threat indicator—

8 (i) to review such cyber threat indi-  
9 cator to assess whether such cyber threat  
10 indicator contains any information not di-  
11 rectly related to a cybersecurity threat that  
12 such Federal entity knows at the time of  
13 sharing to be personal information of a  
14 specific individual or information that  
15 identifies a specific individual and remove  
16 such information; or

17 (ii) to implement and utilize a tech-  
18 nical capability configured to remove any  
19 information not directly related to a  
20 cybersecurity threat that the Federal entity  
21 knows at the time of sharing to be per-  
22 sonal information of a specific individual or  
23 information that identifies a specific indi-  
24 vidual; and

1           (F) include procedures for notifying, in a  
2           timely manner, any United States person whose  
3           personal information is known or determined to  
4           have been shared by a Federal entity in viola-  
5           tion of this title.

6           (2) CONSULTATION.—In developing the proce-  
7           dures required under this section, the Director of  
8           National Intelligence, the Secretary of Homeland Se-  
9           curity, the Secretary of Defense, and the Attorney  
10          General shall consult with appropriate Federal enti-  
11          ties, including the Small Business Administration  
12          and the National Laboratories (as defined in section  
13          2 of the Energy Policy Act of 2005 (42 U.S.C.  
14          15801)), to ensure that effective protocols are imple-  
15          mented that will facilitate and promote the sharing  
16          of cyber threat indicators by the Federal Govern-  
17          ment in a timely manner.

18          (c) SUBMITTAL TO CONGRESS.—Not later than 60  
19          days after the date of the enactment of this Act, the Direc-  
20          tor of National Intelligence, in consultation with the heads  
21          of the appropriate Federal entities, shall submit to Con-  
22          gress the procedures required by subsection (a).

1 **SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING,**  
2 **ANALYZING, AND MITIGATING**  
3 **CYBERSECURITY THREATS.**

4 (a) AUTHORIZATION FOR MONITORING.—

5 (1) IN GENERAL.—Notwithstanding any other  
6 provision of law, a private entity may, for  
7 cybersecurity purposes, monitor—

8 (A) an information system of such private  
9 entity;

10 (B) an information system of another non-  
11 Federal entity, upon the authorization and writ-  
12 ten consent of such other entity;

13 (C) an information system of a Federal en-  
14 tity, upon the authorization and written consent  
15 of an authorized representative of the Federal  
16 entity; and

17 (D) information that is stored on, proc-  
18 essed by, or transiting an information system  
19 monitored by the private entity under this para-  
20 graph.

21 (2) CONSTRUCTION.—Nothing in this sub-  
22 section shall be construed—

23 (A) to authorize the monitoring of an in-  
24 formation system, or the use of any information  
25 obtained through such monitoring, other than  
26 as provided in this title; or

1 (B) to limit otherwise lawful activity.

2 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE  
3 MEASURES.—

4 (1) IN GENERAL.—Notwithstanding any other  
5 provision of law, a private entity may, for  
6 cybersecurity purposes, operate a defensive measure  
7 that is applied to—

8 (A) an information system of such private  
9 entity in order to protect the rights or property  
10 of the private entity;

11 (B) an information system of another non-  
12 Federal entity upon written consent of such en-  
13 tity for operation of such defensive measure to  
14 protect the rights or property of such entity;  
15 and

16 (C) an information system of a Federal en-  
17 tity upon written consent of an authorized rep-  
18 resentative of such Federal entity for operation  
19 of such defensive measure to protect the rights  
20 or property of the Federal Government.

21 (2) CONSTRUCTION.—Nothing in this sub-  
22 section shall be construed—

23 (A) to authorize the use of a defensive  
24 measure other than as provided in this sub-  
25 section; or



1 (B) to limit otherwise lawful activity.

2 (c) AUTHORIZATION FOR SHARING OR RECEIVING  
3 CYBER THREAT INDICATORS OR DEFENSIVE MEAS-  
4 URES.—

5 (1) IN GENERAL.—Except as provided in para-  
6 graph (2) and notwithstanding any other provision  
7 of law, a non-Federal entity may, for a cybersecurity  
8 purpose and consistent with the protection of classi-  
9 fied information, share with, or receive from, any  
10 other non-Federal entity or the Federal Government  
11 a cyber threat indicator or defensive measure.

12 (2) LAWFUL RESTRICTION.—A non-Federal en-  
13 tity receiving a cyber threat indicator or defensive  
14 measure from another non-Federal entity or a Fed-  
15 eral entity shall comply with otherwise lawful restric-  
16 tions placed on the sharing or use of such cyber  
17 threat indicator or defensive measure by the sharing  
18 non-Federal entity or Federal entity.

19 (3) CONSTRUCTION.—Nothing in this sub-  
20 section shall be construed—

21 (A) to authorize the sharing or receiving of  
22 a cyber threat indicator or defensive measure  
23 other than as provided in this subsection; or

24 (B) to limit otherwise lawful activity.

25 (d) PROTECTION AND USE OF INFORMATION.—