

118TH CONGRESS
1ST SESSION

H. R. 1219

To establish a food and agriculture cybersecurity clearinghouse in the National Telecommunications and Information Administration, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 27, 2023

Mr. PFLUGER (for himself, Mr. VEASEY, Mr. CURTIS, and Ms. MATSUI) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Agriculture, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To establish a food and agriculture cybersecurity clearinghouse in the National Telecommunications and Information Administration, 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 “Food and Agriculture
5 Industry Cybersecurity Support Act”.

1 **SEC. 2. NTIA FOOD AND AGRICULTURE CYBERSECURITY**
2 **CLEARINGHOUSE.**

3 (a) NTIA FOOD AND AGRICULTURE CYBERSECURITY
4 CLEARINGHOUSE.—

5 (1) ESTABLISHMENT.—

6 (A) IN GENERAL.—Not later than 180
7 days after the date of the enactment of this
8 Act, the Assistant Secretary shall establish in
9 the NTIA a food and agriculture cybersecurity
10 clearinghouse (in this section referred to as the
11 “clearinghouse”).

12 (B) REQUIREMENTS.—The clearinghouse
13 shall—

14 (i) be publicly available online;

15 (ii) contain current, relevant, and
16 publicly available food and agriculture in-
17 dustry focused cybersecurity resources, in-
18 cluding the recommendations described in
19 paragraph (2), and any other appropriate
20 materials for reference by entities that de-
21 velop products with potential security
22 vulnerabilities for the food and agriculture
23 industry;

24 (iii) contain a mechanism for individ-
25 uals or entities in the food and agriculture
26 industry to request in-person or virtual

1 support from the NTIA or, if appropriate,
2 a cooperating agency for cybersecurity re-
3 lated issues;

4 (iv) contain a Frequently Asked Ques-
5 tions (FAQ) section, updated at least an-
6 nually, with answers to the top 20 most
7 frequently asked questions relevant to the
8 cybersecurity of the food and agriculture
9 industry; and

10 (v) include materials specifically
11 aimed at assisting small business concerns
12 and non-technical users in the food and ag-
13 riculture industry with critical cybersecu-
14 rity protections related to the food and ag-
15 riculture industry, including recommenda-
16 tions on how to respond to a ransomware
17 attack and resources for additional infor-
18 mation, including the “Stop Ransomware”
19 site hosted by the Cybersecurity and Infra-
20 structure Security Agency of the Depart-
21 ment of Homeland Security.

22 (C) EXISTING PLATFORM OR WEBSITE.—

23 The Assistant Secretary may establish the
24 clearinghouse on an online platform or a

1 website that is in existence as of the date of the
2 enactment of this Act.

3 (2) CONSOLIDATION OF FOOD AND AGRI-
4 CULTURE INDUSTRY CYBERSECURITY RECOMMENDA-
5 TIONS.—

6 (A) IN GENERAL.—The Assistant Sec-
7 retary, in consultation with the Administrator
8 of the Farm Service Agency of the Department
9 of Agriculture and relevant Sector Risk Man-
10 agement Agencies, shall consolidate public and
11 private sector best practices to produce a set of
12 voluntary cybersecurity recommendations relat-
13 ing to the development, maintenance, and oper-
14 ation of the food and agriculture industry.

15 (B) REQUIREMENTS.—The recommenda-
16 tions consolidated under subparagraph (A) shall
17 include, to the greatest extent practicable, ma-
18 terials addressing the following:

19 (i) Risk-based, cybersecurity-informed
20 engineering, including continuous moni-
21 toring and resiliency.

22 (ii) Planning for retention or recovery
23 of positive control of systems in the food
24 and agriculture industry in the event of a
25 cybersecurity incident.

1 (iii) Protection against unauthorized
2 access to critical functions of the food and
3 agriculture industry.

4 (iv) Cybersecurity against threats to
5 products of the food and agriculture indus-
6 try throughout the lifetimes of such prod-
7 ucts.

8 (v) How businesses in the food and
9 agriculture industry should respond to
10 ransomware attacks, including details on
11 the legal obligations of such businesses in
12 the event of such an attack, including re-
13 porting requirements and Federal re-
14 sources for support.

15 (vi) Any other recommendations to
16 ensure the confidentiality, availability, and
17 integrity of data residing on or in transit
18 through systems in the food and agri-
19 culture industry.

20 (3) IMPLEMENTATION.—In implementing this
21 subsection, the Assistant Secretary shall—

22 (A) to the extent practicable, consult with
23 the private sector;

24 (B) consult with non-Federal entities de-
25 veloping equipment and systems utilized in the

1 food and agriculture industry, including private,
2 consensus organizations that develop relevant
3 standards;

4 (C) consult with the Director of the Cyber-
5 security and Infrastructure Security Agency of
6 the Department of Homeland Security;

7 (D) consult with food and agriculture in-
8 dustry trade groups;

9 (E) consult with relevant Sector Risk Man-
10 agement Agencies;

11 (F) consult with civil society organizations;

12 (G) consult with the Administrator of the
13 Small Business Administration; and

14 (H) consider the development of an advi-
15 sory board to advise the Assistant Secretary on
16 implementing this subsection, including the col-
17 lection of data through the clearinghouse and
18 the disclosure of such data.

19 (b) STUDY.—

20 (1) IN GENERAL.—The Comptroller General of
21 the United States shall conduct a study on the ac-
22 tions the Federal Government has taken or may
23 take to improve the cybersecurity of the food and
24 agriculture industry.

1 (2) REPORT.—Not later than 90 days after the
2 date of the enactment of this Act, the Comptroller
3 General of the United States shall submit to Con-
4 gress a report on the study conducted under para-
5 graph (1), which shall include information on the
6 following:

7 (A) The effectiveness of efforts of the Fed-
8 eral Government to improve the cybersecurity of
9 the food and agriculture industry.

10 (B) The resources made available to the
11 public, as of the date of such submission, by
12 Federal agencies to improve the cybersecurity
13 of the food and agriculture industry, including
14 to address cybersecurity risks and cybersecurity
15 threats to the food and agriculture industry.

16 (C) The extent to which Federal agencies
17 coordinate or duplicate authorities and take
18 other actions for the improvement of the cyber-
19 security of the food and agriculture industry.

20 (D) Whether there is an appropriate plan
21 in place to prevent or adequately mitigate the
22 risks of a coordinated attack on the food and
23 agriculture industry.

24 (E) The advantages and disadvantages of
25 creating a food and agriculture industry specific

1 Information Sharing and Analysis Center
2 (ISAC), including required actions by the Fed-
3 eral Government and expected costs to the Fed-
4 eral Government to create such an organization
5 and potential industry and civil society partners
6 who could operate such an organization.

7 (F) The advantages and disadvantages of
8 the creation by the Assistant Secretary of a
9 database containing a software bill of materials
10 (SBOM) for the most common internet-con-
11 nected hardware and software applications used
12 in the food and agriculture industry and rec-
13 ommendations for how the Assistant Secretary
14 can maintain and update such database.

15 (3) COORDINATION.—In carrying out para-
16 graphs (1) and (2), the Comptroller General of the
17 United States shall coordinate with appropriate Fed-
18 eral agencies, including the following:

19 (A) The Department of Health and
20 Human Services.

21 (B) The Department of Commerce.

22 (C) The Department of Agriculture.

23 (D) The Federal Communications Commis-
24 sion.

25 (E) The Department of Energy.

1 (F) The Small Business Administration.

2 (4) PROCESS FOR STUDYING CREATION OF
3 ISAC.—In studying the advantages and disadvan-
4 tages of creating a food and agriculture industry
5 specific Information Sharing and Analysis Center for
6 purposes of including in the report required by para-
7 graph (2) the information required by subparagraph
8 (E) of such paragraph, the Comptroller General
9 shall convene stakeholders that include civil society
10 organizations, individual food and agriculture pro-
11 ducers, and the Federal agencies described in para-
12 graph (3).

13 (5) BRIEFING.—Not later than 90 days after
14 the date on which the Comptroller General of the
15 United States submits the report under paragraph
16 (2), the Comptroller General shall provide to Con-
17 gress a briefing regarding such report.

18 (6) CLASSIFICATION.—The report under para-
19 graph (2) shall be unclassified but may include a
20 classified annex.

21 (c) DEFINITIONS.—In this section:

22 (1) ASSISTANT SECRETARY.—The term “Assist-
23 ant Secretary” means the Assistant Secretary of
24 Commerce for Communications and Information.

1 (2) CYBERSECURITY RISK.—The term “cyberse-
2 curity risk” has the meaning given such term in sec-
3 tion 2200 of the Homeland Security Act of 2002 (6
4 U.S.C. 650).

5 (3) CYBERSECURITY THREAT.—The term “cy-
6 bersecurity threat” has the meaning given such term
7 in section 2200 of the Homeland Security Act of
8 2002 (6 U.S.C. 650).

9 (4) FOOD AND AGRICULTURE INDUSTRY.—The
10 term “food and agriculture industry” means—

11 (A) equipment and systems utilized in the
12 food and agriculture supply chain, such as com-
13 puter vision algorithms for precision agri-
14 culture, grain silos, and related food and agri-
15 culture storage infrastructure;

16 (B) food and agriculture goods processors,
17 growers, and distributors; and

18 (C) information technology systems of
19 businesses engaged in farming, ranching, plant-
20 ing, harvesting, food and agriculture product
21 storage, food or animal genetic modification,
22 the design or production of agrochemicals, or
23 the design or production of food and agriculture
24 tools.

1 (5) INCIDENT.—The term “incident” has the
2 meaning given such term in section 2200 of the
3 Homeland Security Act of 2002 (6 U.S.C. 650).

4 (6) NTIA.—The term “NTIA” means the Na-
5 tional Telecommunications and Information Admin-
6 istration.

7 (7) SECTOR RISK MANAGEMENT AGENCY.—The
8 term “Sector Risk Management Agency” has the
9 meaning given such term in section 2200 of the
10 Homeland Security Act of 2002 (6 U.S.C. 650).

11 (8) SECURITY VULNERABILITY.—The term “se-
12 curity vulnerability” has the meaning given such
13 term in section 2200 of the Homeland Security Act
14 of 2002 (6 U.S.C. 650).

15 (9) SMALL BUSINESS CONCERN.—The term
16 “small business concern” means a small business
17 concern described in section 3 of the Small Business
18 Act (15 U.S.C. 632).

19 (10) SOFTWARE BILL OF MATERIALS.—The
20 term “software bill of materials” has the meaning
21 given such term in section 10 of Executive Order
22 14028 (86 Fed. Reg. 26633; relating to improving
23 the Nation’s cybersecurity).

1 (d) SUNSET.—This section shall have no force or ef-
2 fect after the date that is 7 years after the date of the
3 enactment of this Act.

○