.....

(Original Signature of Member)

118TH CONGRESS
1ST SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Food and Agriculture Industry Cybersecurity Support Act''.

SEC. 2. NTIA FOOD AND AGRICULTURE CYBERSECURITY CLEARINGHOUSE.

(a) NTIA FOOD AND AGRICULTURE CYBERSECURITY CLEARINGHOUSE.—

(1) ESTABLISHMENT.—

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

(B) REQUIREMENTS.—The clearinghouse shall—

(i) be publicly available online;

(ii) contain current, relevant, and publicly available food and agriculture industry focused cybersecurity resources, including the recommendations described in paragraph (2), and any other appropriate materials for reference by entities that develop products with potential security vulnerabilities for the food and agriculture industry;

(iii) contain a mechanism for individuals or entities in the food and agriculture industry to request in-person or virtual

support from the NTIA or, if appropriate, a cooperating agency for cybersecurity related issues;

(iv) contain a Frequently Asked Questions (FAQ) section, updated at least annually, with answers to the top 20 most frequently asked questions relevant to the cybersecurity of the food and agriculture industry; and

(v) include materials specifically aimed at assisting small business concerns and non-technical users in the food and agriculture industry with critical cybersecurity protections related to the food and agriculture industry, including recommendations on how to respond to a ransomware attack and resources for additional information, including the ''Stop Ransomware'' site hosted by the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(C) EXISTING PLATFORM OR WEBSITE.—The Assistant Secretary may establish the clearinghouse on an online platform or a

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

(2) CONSOLIDATION OF FOOD AND AGRICULTURE INDUSTRY CYBERSECURITY RECOMMENDATIONS.—

(A) IN GENERAL.—The Assistant Secretary, in consultation with the Administrator of the Farm Service Agency of the Department of Agriculture and relevant Sector Risk Management Agencies, shall consolidate public and private sector best practices to produce a set of voluntary cybersecurity recommendations relating to the development, maintenance, and operation of the food and agriculture industry.

(B) REQUIREMENTS.—The recommendations consolidated under subparagraph (A) shall include, to the greatest extent practicable, materials addressing the following:

(i) Risk-based, cybersecurity-informed engineering, including continuous monitoring and resiliency.

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

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

(iv) Cybersecurity against threats to products of the food and agriculture industry throughout the lifetimes of such products.

(v) How businesses in the food and agriculture industry should respond to ransomware attacks, including details on the legal obligations of such businesses in the event of such an attack, including reporting requirements and Federal resources for support.

(vi) Any other recommendations to ensure the confidentiality, availability, and integrity of data residing on or in transit through systems in the food and agriculture industry.

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

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

(B) consult with non-Federal entities developing equipment and systems utilized in the

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

(C) consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security;

(D) consult with food and agriculture industry trade groups;

(E) consult with relevant Sector Risk Management Agencies;

(F) consult with civil society organizations;

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

(H) consider the development of an advisory board to advise the Assistant Secretary on implementing this subsection, including the collection of data through the clearinghouse and the disclosure of such data.

(b) STUDY.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a study on the actions the Federal Government has taken or may take to improve the cybersecurity of the food and agriculture industry.

(2) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the study conducted under paragraph (1), which shall include information on the following:

(A) The effectiveness of efforts of the Federal Government to improve the cybersecurity of the food and agriculture industry.

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

(C) The extent to which Federal agencies coordinate or duplicate authorities and take other actions for the improvement of the cybersecurity of the food and agriculture industry.

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

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

Information Sharing and Analysis Center (ISAC), including required actions by the Federal Government and expected costs to the Federal Government to create such an organization and potential industry and civil society partners who could operate such an organization.

(F) The advantages and disadvantages of the creation by the Assistant Secretary of a database containing a software bill of materials (SBOM) for the most common internet-connected hardware and software applications used in the food and agriculture industry and recommendations for how the Assistant Secretary can maintain and update such database.

(3) COORDINATION.—In carrying out paragraphs (1) and (2), the Comptroller General of the United States shall coordinate with appropriate Federal agencies, including the following:

(A) The Department of Health and Human Services.

(B) The Department of Commerce.

(C) The Department of Agriculture.

(D) The Federal Communications Commission.

(E) The Department of Energy.

(F) The Small Business Administration.

(4) PROCESS FOR STUDYING CREATION OF ISAC.—In studying the advantages and disadvantages of creating a food and agriculture industry specific Information Sharing and Analysis Center for purposes of including in the report required by paragraph (2) the information required by subparagraph (E) of such paragraph, the Comptroller General shall convene stakeholders that include civil society organizations, individual food and agriculture producers, and the Federal agencies described in paragraph (3).

(5) BRIEFING.—Not later than 90 days after the date on which the Comptroller General of the United States submits the report under paragraph (2), the Comptroller General shall provide to Congress a briefing regarding such report.

(6) CLASSIFICATION.—The report under paragraph (2) shall be unclassified but may include a classified annex.

(c) DEFINITIONS.—In this section:

(1) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary of Commerce for Communications and Information.

(2) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(3) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(4) FOOD AND AGRICULTURE INDUSTRY.—The term ''food and agriculture industry'' means—

(A) equipment and systems utilized in the food and agriculture supply chain, such as computer vision algorithms for precision agriculture, grain silos, and related food and agriculture storage infrastructure;

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

(C) information technology systems of businesses engaged in farming, ranching, planting, harvesting, food and agriculture product storage, food or animal genetic modification, the design or production of agrochemicals, or the design or production of food and agriculture tools.

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

(6) NTIA.—The term ''NTIA'' means the National Telecommunications and Information Administration.

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

(8) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

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

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

(d) SUNSET.—This section shall have no force or effect after the date that is 7 years after the date of the enactment of this Act.