I

118TH CONGRESS
2D SESSION

H. R. 7062

To direct the Secretary of Agriculture to periodically assess cybersecurity threats to, and vulnerabilities in, the agriculture and food critical infrastructure sector and to provide recommendations to enhance their security and resilience, to require the Secretary of Agriculture to conduct an annual cross-sector simulation exercise relating to a food-related emergency or disruption, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 22, 2024

Mr. FINSTAD (for himself, Ms. SLOTKIN, Mr. KELLY of Mississippi, Ms. TOKUDA, Mr. BACON, Ms. CARAVEO, Mrs. HINSON, Mr. SOTO, Mr. MOOLENAAR, Mr. JACKSON of Texas, Mr. AUSTIN SCOTT of Georgia, Mr. NUNN of Iowa, Mr. ALFORD, and Mr. SMUCKER) introduced the following bill; which was referred to the Committee on Agriculture

---

A BILL

To direct the Secretary of Agriculture to periodically assess cybersecurity threats to, and vulnerabilities in, the agriculture and food critical infrastructure sector and to provide recommendations to enhance their security and resilience, to require the Secretary of Agriculture to conduct an annual cross-sector simulation exercise relating to a food-related emergency or disruption, 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 ''Farm and Food Cybersecurity Act of 2024''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGRICULTURE AND FOOD CRITICAL INFRASTRUCTURE SECTOR.—The term ''agriculture and food critical infrastructure sector'' means—

(A) any activity relating to the production, processing, distribution, storage, transportation, consumption, or disposal of agricultural or food products; and

(B) any entity involved in an activity described in subparagraph (A), including a farmer, rancher, processor, manufacturer, distributor, retailer, consumer, and regulator.

(2) CYBERSECURITY THREAT; DEFENSIVE MEASURE; INCIDENT; SECURITY VULNERABILITY.—The terms ''cybersecurity threat'', ''defensive measure'', ''incident'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(3) SECRETARY.—The term ''Secretary'' means the Secretary of Agriculture.

SEC. 3. ASSESSMENT OF CYBERSECURITY THREATS AND SECURITY VULNERABILITIES IN THE AGRICULTURE AND FOOD CRITICAL INFRASTRUCTURE SECTOR.

(a) STUDY.—The Secretary shall conduct a study, on a biennial basis, on the cybersecurity threats to, and security vulnerabilities in, the agriculture and food critical infrastructure sector, including—

(1) the nature and extent of cyberattacks and incidents that affect the agriculture and food critical infrastructure sector;

(2) the potential impacts of a cyberattack or incident on the safety, security, and availability of food products, as well as on the economy, public health, and national security of the United States;

(3) the current capability and readiness of the Federal Government, State and local governments, and private sector entities to prevent, detect, respond to, and recover from cyberattacks and incidents described in paragraph (2);

(4) the existing policies, standards, guidelines, best practices, and initiatives applicable to the agriculture and food critical infrastructure sector to enhance defensive measures in that sector;

(5) the gaps, challenges, barriers, or opportunities for improving defensive measures in the agriculture and food critical infrastructure sector; and

(6) any recommendations for Federal legislative or administrative actions to address the cybersecurity threats to, and security vulnerabilities in, the agriculture and food critical infrastructure sector.

(b) BIENNIAL REPORT.—Not later than 1 year after the date of enactment of this Act, and every 2 years thereafter, the Secretary shall submit a report on each study conducted under subsection (a) to—

(1) the Committee on Agriculture, Nutrition, and Forestry of the Senate;

(2) the Committee on Homeland Security and Governmental Affairs of the Senate;

(3) the Committee on Agriculture of the House of Representatives; and

(4) the Committee on Homeland Security of the House of Representatives.

SEC. 4. FOOD SECURITY AND CYBER RESILIENCE SIMULATION EXERCISE.

(a) ESTABLISHMENT.—The Secretary, in coordination with the Secretary of Homeland Security, the Secretary of Health and Human Services, the Director of National Intelligence, and the heads of other relevant Federal

agencies, shall conduct, over a 5-year period, an annual cross-sector crisis simulation exercise relating to a food-related emergency or disruption (referred to in this section as an ''exercise'').

(b) PURPOSES.—The purposes of each exercise are—

(1) to assess the preparedness and response capabilities of Federal, State, Tribal, local, and territorial governments and private sector entities in the event of a food-related emergency or disruption;

(2) to identify and address gaps and vulnerabilities in the food supply chain and critical infrastructure;

(3) to enhance coordination and information sharing among stakeholders involved in food production, processing, distribution, and consumption;

(4) to evaluate the effectiveness and efficiency of existing policies, programs, and resources relating to food security and resilience;

(5) to develop and disseminate best practices and recommendations for improving food security and resilience; and

(6) to identify key stakeholders and categories that were missing from the exercise to ensure the inclusion of those stakeholders and categories in future exercises.

(c) DESIGN.—Each exercise shall—

(1) involve a realistic and plausible scenario that simulates a food-related emergency or disruption affecting multiple sectors and jurisdictions;

(2) incorporate input from experts and stakeholders from various disciplines and sectors, including agriculture, public health, nutrition, emergency management, transportation, energy, water, communications, related equipment suppliers and manufacturers, and cybersecurity, including related academia and private sector information security researchers and practitioners;

(3) use a variety of methods and tools, such as tabletop exercises, workshops, seminars, games, drills, or full-scale exercises; and

(4) include participants from Federal, State, Tribal, local, and territorial governments and private sector entities that have roles and responsibilities relating to food security and resilience.

(d) FEEDBACK; REPORT.—After each exercise, the Secretary, in consultation with the heads of the Federal agencies described in subsection (a), shall—

(1) provide feedback to, and an evaluation of, the participants in that exercise on their performance and outcomes; and

(2) produce, and submit to Congress, a report that summarizes, with respect to that exercise, the findings of that exercise, lessons learned from that exercise, and recommendations to enhance the cybersecurity and resilience of the agriculture and food critical infrastructure sector.

(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $1,000,000 for each of fiscal years 2024 through 2028.

○