Slotkin 1st Degree #2

AMENDMENT NO._____ Calendar No._____

Purpose: To periodically assess cybersecurity threats to, and vulnerabilities in, the agriculture and food critical infrastructure sector.

IN THE SENATE OF THE UNITED STATES—119th Cong., 2d Sess.

S._____

To provide for the reform and continuation of agricultural and other programs of the Department of Agriculture through fiscal year 2031, and for other purposes.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Ms. SLOTKIN

Viz:

At the end of subtitle B of title XII, add the following:

SEC. 122___. ASSESSMENT OF CYBERSECURITY THREATS AND SECURITY VULNERABILITIES IN THE AGRICULTURE AND FOOD CRITICAL INFRASTRUCTURE SECTOR.

(a) DEFINITIONS.—In this section:

(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) SECTOR-SPECIFIC ISAC.—The term "sector-specific ISAC" means the Food and Agriculture-Information Sharing and Analysis Center.

(b) RISK ASSESSMENT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and on a biennial basis thereafter, the Secretary, in coordination with the Cybersecurity and Infrastructure Security Agency, shall conduct a risk assessment on the cybersecurity threats to, and security vulnerabilities in, the

agriculture and food critical infrastructure sector, including—

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

(B) 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;

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

(D) 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;

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

(F) 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, including intrusive, duplicative, or conflicting regulatory requirements that may divert attention and resources from operational risk management to a compliance regime that impedes security efforts.

(2) PRIVATE SECTOR PARTICIPATION.—In conducting a risk assessment under paragraph (1), the Secretary shall consult with appropriate entities in the private sector, including—

(A) the sector-specific ISAC; and

(B) the appropriate sector coordinating council.

(3) REPORT.—The Secretary shall submit a report on each risk assessment conducted under paragraph (1) to—

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

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

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

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

(c) FOOD SECURITY AND CYBER RESILIENCE SIMULATION EXERCISE.—

(1) ESTABLISHMENT.—Not later than 2 years after the date of enactment of this Act, and on a biennial basis thereafter over a 6-year period, 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 a cross-sector crisis simulation exercise relating to a food-related emergency or disruption (referred to in this subsection as an "exercise").

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

(A) 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;

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

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

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

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

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

(3) DESIGN.—Each exercise shall—

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

(B) 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 cyberse-

curity, including related academia and private sector information security researchers and practitioners, including the sector-specific ISAC;

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

(D) include participants from Federal, State, Tribal, local, and territorial governments and private sector entities, including the sector-specific ISAC and appropriate sector coordinating councils, that have roles and responsibilities relating to food security and resilience.

(4) PRIVATE SECTOR PARTICIPATION.—In conducting an exercise, the Secretary shall consult with appropriate entities in the private sector, including—

(A) the sector-specific ISAC; and

(B) the appropriate sector coordinating councils.

(5) FEEDBACK; REPORT.—After each exercise, the Secretary, in consultation with the heads of the Federal agencies described in paragraph (1), shall—

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

(B) 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.

(6) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this subsection $1,000,000 for each of fiscal years 2027 through 2031.