119TH CONGRESS
1ST SESSION

S. 2866

To amend the National Agricultural Research, Extension, and Teaching Policy Act of 1977 to direct the Secretary of Agriculture to establish a program providing for the establishment of Agriculture Cybersecurity Centers, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 18 (legislative day, SEPTEMBER 16), 2025

Mr. BUDD (for himself and Ms. CORTEZ MASTO) introduced the following bill; which was read twice and referred to the Committee on Agriculture, Nutrition, and Forestry

---

A BILL

To amend the National Agricultural Research, Extension, and Teaching Policy Act of 1977 to direct the Secretary of Agriculture to establish a program providing for the establishment of Agriculture Cybersecurity Centers, 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 ''Cybersecurity in Agriculture Act of 2025''.

SEC. 2. AGRICULTURE CYBERSECURITY CENTERS.

Subtitle K of the National Agricultural Research, Extension, and Teaching Policy Act of 1977 (7 U.S.C. 3310 et seq.) is amended by adding at the end the following:

"SEC. 1473I. AGRICULTURE CYBERSECURITY CENTERS.

"(a) IN GENERAL.—The Secretary, acting through the Director of the National Institute of Food and Agriculture, and in consultation with the Secretary of Homeland Security, shall establish a program under which the Secretary shall—

"(1) on a competitive basis, award grants to, or enter into cooperative agreements with, eligible entities to establish 5 Regional Agriculture Cybersecurity Centers to carry out research, development, and education on agriculture cybersecurity, with respect to seed agriculture, horticulture, animal agriculture, and the agriculture supply chain;

"(2) establish a national network of such Regional Agriculture Cybersecurity Centers; and

"(3) designate one eligible entity to coordinate the activities of such national network.

"(b) DUTIES.—A Regional Agriculture Cybersecurity Center shall—

"(1) conduct research on cybersecurity systems for the agriculture sector, including developing cy-

bersecurity situational awareness systems to monitor cybersecurity threats, intrusions, and anomalies;

''(2) develop a security operations center for the agriculture sector—

''(A) to analyze cybersecurity threats, intrusions, and anomalies; and

''(B) to recommend mitigation actions;

''(3) develop cybersecurity technologies and tools for the agriculture sector, including—

''(A) domain-specific intrusion and anomaly detection systems;

''(B) domain-specific intrusion prevention systems;

''(C) domain-specific role-based access control and user authentication systems;

''(D) lightweight device authentication protocols; and

''(E) secure network architectures;

''(4) build live cybersecurity testbeds to assess and refine cybersecurity technologies, tools, and systems developed for the agriculture sector;

''(5) conduct attack/defense exercises to validate and evaluate cybersecurity solutions for field deployment and agriculture industry adoption;

''(6) develop cybersecurity education and training programs for agricultural stakeholders;

''(7) conduct cybersecurity training using the testbeds referred to in paragraph (4);

''(8) build a regional research and development collaboration network; and

''(9) ensure that the research described in paragraph (1), the technologies and tools described in paragraph (3), and the attack/defense exercises described in paragraph (5) are specifically designed to prevent cyberattacks from—

''(A) the People's Republic of China;

''(B) the Democratic People's Republic of Korea;

''(C) the Russian Federation;

''(D) the Islamic Republic of Iran; and

''(E) such other countries as the Secretary, in consultation with the Secretary of Homeland Security, determines to be appropriate.

''(c) DEFINITION OF ELIGIBLE ENTITY.—In this section, the term 'eligible entity' means a land-grant college or university that—

''(1) has programs in the food and agricultural sciences and cybersecurity; and

''(2) coordinates regional industry partners, cooperatives, government authorities, and other stakeholders—

''(A) to strengthen the security, privacy, and resiliency of agricultural systems;

''(B) to bolster the resiliency of cybersecurity infrastructure used by independent, noncentralized, locally owned and operated agricultural networks; and

''(C) to develop a skilled workforce equipped to manage and protect agricultural systems from cyberattacks.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $25,000,000 for each of fiscal years 2026 through 2030.''.

○