118TH CONGRESS
2D SESSION

S. 4715

To require the National Cyber Director to submit to Congress a plan to establish an institute within the Federal Government to serve as a centralized resource and training center for Federal cyber workforce development.

IN THE SENATE OF THE UNITED STATES

JULY 11 (legislative day, JULY 10), 2024

Mr. ROUNDS (for himself and Mr. OSSOFF) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To require the National Cyber Director to submit to Congress a plan to establish an institute within the Federal Government to serve as a centralized resource and training center for Federal cyber workforce development.

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 ''Federal Cyber Workforce Training Act of 2024''.

SEC. 2. FEDERAL CYBER WORKFORCE DEVELOPMENT INSTITUTE.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 551 of title 5, United States Code.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services of the Senate;

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

(C) the Committee on Armed Services of the House of Representatives;

(D) the Committee on Homeland Security of the House of Representatives; and

(E) the Committee on Oversight and Accountability of the House of Representatives.

(3) CYBER WORK ROLE.—The term ''cyber work role'' means—

(A) a role indicated in the NICE framework for new hires and personnel seeking transition to mid-career positions; and

(B) a role relating to work involving designing, building, securing, operating, defending, and protecting cyberspace resources.

(4) DIRECTOR.—The term ''Director'' means the National Cyber Director.

(5) FEDERAL INSTITUTE.—The term ''Federal institute'' means the Federal institute described in the plan required under subsection (b)(1).

(6) NICE FRAMEWORK.—The term ''NICE framework'' means Special Publication 800–181 of the National Institute of Standards and Technology entitled ''Workforce Framework for Cybersecurity (NICE Framework)'', or any successor document.

(7) WORK-BASED LEARNING.—The term ''work-based learning'' has the meaning given the term in section 3 of the Carl D. Perkins Career and Technical Education Act of 2006 (20 U.S.C. 2302).

(b) REQUIREMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director, in consultation with the Secretary of Homeland Security, the Secretary of Defense, the Director of the Office of Personnel Management, and the head of any other agency the Director determines necessary, shall submit to Congress and make publicly available

a plan for the establishment of a Federal institute to provide—

(A) training for personnel hired for cyber work roles in the Federal Government, including new hires and personnel seeking transition to mid-career positions, which may include upskilling and reskilling efforts; and

(B) training for personnel with responsibilities for human resource functions relating to cyber personnel.

(2) INSTITUTE FUNCTIONS.—The plan required under paragraph (1) shall provide for the Federal institute to—

(A) provide modularized cyber work role-specific training, including hands-on learning and skill-based assessments, to prepare newly hired Federal personnel from a wide variety of academic and professional backgrounds to perform effectively in Federal cyber work roles;

(B) coordinate with the Secretary of Homeland Security, the Secretary of Defense, and the heads of other agencies determined necessary by the Director to develop a cyber work role-specific curriculum for the training provided under subparagraph (A)—

(i) in accordance with the NICE framework; and

(ii) in consideration of other Federal cyber training programs;

(C) prioritize entry-level positions in the provision of curriculum development and training;

(D) address the training needs of—

(i) personnel seeking transition to mid-career positions; and

(ii) personnel with responsibilities for human resources functions relating to cyber personnel;

(E) include curriculum development and training for Federal cyber workers seeking transition to mid-career positions, which may include upskilling and reskilling efforts;

(F) consider developing a specific module to familiarize and train appropriate Federal Government hiring managers and human resources staff in the unique challenges in recruiting and hiring personnel for Federal cyber work force roles;

(G) incorporate work-based learning in personnel training;

(H) develop a badging system to communicate qualification and proficiency for individuals who successfully complete training through the Federal institute with consideration of systems used by the intelligence community;

(I) offer in-person and virtual options to accommodate various learning environments for individuals; and

(J) provide training to individuals irrespective of whether an individual has a college degree or a college degree in a cyber-related discipline.

(3) PLAN ELEMENTS.—The plan required under paragraph (1) shall—

(A) recommend an organizational placement for the Federal institute, which may include a single agency or a combination of agencies;

(B) to the greatest extent practicable, align training and tools, including cyber work roles and competencies and the associated tasks, knowledge, and skills from—

(i) the Special Publication of the National Institute of Standards and Technology 800–181, Revision 1, entitled ''Na-

tional Initiative for Cybersecurity Education Workforce Framework for Cybersecurity'', or any successor special publication; or

(ii) other applicable publications, studies, or guidance of the Federal Government;

(C) identify—

(i) elements of the Federal institute and its functions that could use existing facilities, resources, and programs of the Federal Government; and

(ii) elements of the Federal institute and its functions that would require new facilities, resources, and programs of the Federal Government in order to implement the plan required under paragraph (1);

(D) recommend a course curriculum, delivery method, and length of curriculum for the training provided under paragraph (1)(A) using Federal Government cyber training programs as models, including the Joint Cyber Analysis Course of the Department of Defense and the Federal Cyber Defense Skilling Academy of the

Cybersecurity and Infrastructure Security Agency;

(E) recommend a policy for individuals who do not complete required training;

(F) describe a security clearance process to complete some level of security clearance for appropriate individuals while individuals are enrolled in training;

(G) recommend a governance structure for the Federal institute that would ensure ongoing interagency coordination in the development of a curriculum, the provision of training, and other considerations the Director determines appropriate;

(H) provide an estimate of the funding and new authorities required to establish and operate the Federal institute;

(I) describe any requirements for the Federal institute to conduct work in a classified setting;

(J) identify how the Federal institute would—

(i) provide some or all of the training required by paragraph (1)(A) through 5

academic institutions from among academic institutions that—

(I) are designated by the National Security Agency as a National Center of Academic Excellence in cybersecurity for cyber defense, cyber research, and cyber operations; and

(II) have an operational sensitive compartmented information facility; and

(ii) select the 5 academic institutions under clause (i);

(K) identify how the instructors of the Federal institute will remain current with respect to cybersecurity knowledge, skills and abilities through scholarship or other means; and

(L) identify how the Federal institute will maintain the quality and longevity of instructors.

(4) CONSULTATION.—In developing a plan for the Federal institute, the Director shall consult with the Director of the Office of Personnel Management, the Chief Human Capital Officers Council, the Chief Information Officers Council, and the Chief Learn-

ing Officers Council to establish tools for human resources professionals of the Federal Government to develop the knowledge, skills and abilities required to manage the career life cycle of cyber professionals from recruitment to retirement.

(c) BRIEFING.—Not later than 270 days after the date of enactment of this Act, the Director shall provide to the appropriate congressional committees a briefing on the plan required under subsection (b)(1), including an estimate of the funding and the authorities necessary to implement the plan.

(d) NO ADDITIONAL FUNDS.—No additional funds are authorized to be appropriated for the purpose of carrying out this Act.

○