

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: In the nature of a substitute.

**IN THE SENATE OF THE UNITED STATES—118th Cong., 2d Sess.**

**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.

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended  
to be proposed by Mr. OSSOFF

Viz:

1       Strike all after the enacting clause and insert the fol-  
2       lowing:

3       **SECTION 1. SHORT TITLE.**

4       This Act may be cited as the “Federal Cyber Work-  
5       force Training Act of 2024”.

6       **SEC. 2. FEDERAL CYBER WORKFORCE DEVELOPMENT IN-**  
7       **STITUTE.**

8       (a) DEFINITIONS.—In this section:

9               (1) AGENCY.—The term “agency” has the  
10       meaning given the term in section 551 of title 5,  
11       United States Code.

1           (2) APPROPRIATE CONGRESSIONAL COMMIT-  
2           TEES.—The term “appropriate congressional com-  
3           mittees” means—

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

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

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

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

12                  (E) the Committee on Oversight and Ac-  
13           countability of the House of Representatives.

14           (3) CYBER WORK ROLE.—The term “cyber  
15           work role” means—

16                   (A) a role indicated in the NICE frame-  
17           work for new hires and personnel seeking tran-  
18           sition to mid-career positions; and

19                   (B) a role relating to work involving de-  
20           signing, building, securing, operating, defend-  
21           ing, and protecting cyberspace resources.

22           (4) DIRECTOR.—The term “Director” means  
23           the National Cyber Director.

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

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

9           (7) WORK-BASED LEARNING.—The term “work-  
10 based learning” has the meaning given the term in  
11 section 3 of the Carl D. Perkins Career and Tech-  
12 nical Education Act of 2006 (20 U.S.C. 2302).

13 (b) REQUIREMENT.—

14           (1) IN GENERAL.—Not later than 180 days  
15 after the date of enactment of this Act, the Director,  
16 in consultation with the Secretary of Homeland Se-  
17 curity, the Secretary of Defense, the Director of the  
18 Office of Personnel Management, and the head of  
19 any other agency the Director determines necessary,  
20 shall submit to Congress and make publicly available  
21 a plan for the establishment of a Federal institute  
22 to provide—

23           (A) training for personnel hired for cyber  
24 work roles in the Federal Government, includ-  
25 ing new hires and personnel seeking transition

1 to mid-career positions, which may include  
2 upskilling and reskilling efforts; and

3 (B) training for personnel with responsibil-  
4 ities for human resource functions relating to  
5 cyber personnel.

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

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

15 (B) coordinate with the Secretary of  
16 Homeland Security, the Secretary of Defense,  
17 and the heads of other agencies determined nec-  
18 essary by the Director to develop a cyber work  
19 role-specific curriculum for the training pro-  
20 vided under subparagraph (A)—

21 (i) in accordance with the NICE  
22 framework; and

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

1 (C) prioritize entry-level positions in the  
2 provision of curriculum development and train-  
3 ing;

4 (D) address the training needs of—

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

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

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

14 (F) consider developing a specific module  
15 to familiarize and train appropriate Federal  
16 Government hiring managers and human re-  
17 sources staff in the unique challenges in recruit-  
18 ing and hiring personnel for Federal cyber work  
19 force roles;

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

22 (H) develop a badging system to commu-  
23 nicate qualification and proficiency for individ-  
24 uals who successfully complete training through

1 the Federal institute with consideration of sys-  
2 tems used by the intelligence community;

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

6 (J) provide training to individuals irrespec-  
7 tive of whether an individual has a college de-  
8 gree or a college degree in a cyber-related dis-  
9 cipline.

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

12 (A) recommend an organizational place-  
13 ment for the Federal institute, which may in-  
14 clude a single agency or a combination of agen-  
15 cies;

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

20 (i) the Special Publication of the Na-  
21 tional Institute of Standards and Tech-  
22 nology 800–181, Revision 1, entitled “Na-  
23 tional Initiative for Cybersecurity Edu-  
24 cation Workforce Framework for Cyberse-

1                   curity”, or any successor special publica-  
2                   tion; or

3                   (ii) other applicable publications, stud-  
4                   ies, or guidance of the Federal Govern-  
5                   ment;

6                   (C) identify—

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

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

16                  (D) recommend a course curriculum, deliv-  
17                  ery method, and length of curriculum for the  
18                  training provided under paragraph (1)(A) using  
19                  Federal Government cyber training programs as  
20                  models, including the Joint Cyber Analysis  
21                  Course of the Department of Defense and the  
22                  Federal Cyber Defense Skilling Academy of the  
23                  Cybersecurity and Infrastructure Security  
24                  Agency;

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

3 (F) describe a security clearance process to  
4 complete some level of security clearance for ap-  
5 propriate individuals while individuals are en-  
6 rolled in training;

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

13 (H) provide an estimate of the funding and  
14 new authorities required to establish and oper-  
15 ate the Federal institute;

16 (I) describe any requirements for the Fed-  
17 eral institute to conduct work in a classified  
18 setting;

19 (J) identify how the Federal institute  
20 would—

21 (i) provide some or all of the training  
22 required by paragraph (1)(A) through 5  
23 academic institutions from among aca-  
24 demic institutions that—



1 (I) are designated by the Na-  
2 tional Security Agency as a National  
3 Center of Academic Excellence in cy-  
4 bersecurity for cyber defense, cyber  
5 research, and cyber operations; and

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

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

11 (K) identify how the instructors of the  
12 Federal institute will remain current with re-  
13 spect to cybersecurity knowledge, skills and  
14 abilities through scholarship or other means;  
15 and

16 (L) identify how the Federal institute will  
17 maintain the quality and longevity of instruc-  
18 tors.

19 (4) CONSULTATION.—In developing a plan for  
20 the Federal institute, the Director shall consult with  
21 the Director of the Office of Personnel Management,  
22 the Chief Human Capital Officers Council, the Chief  
23 Information Officers Council, and the Chief Learn-  
24 ing Officers Council to establish tools for human re-  
25 sources professionals of the Federal Government to

1       develop the knowledge, skills and abilities required  
2       to manage the career life cycle of cyber professionals  
3       from recruitment to retirement.

4       (c) BRIEFING.—Not later than 280 days after the  
5       date of enactment of this Act, the Director shall provide  
6       to the appropriate congressional committees a briefing on  
7       the plan required under subsection (b)(1), including an es-  
8       timate of the funding and the authorities necessary to im-  
9       plement the plan.

10       (d) NO ADDITIONAL FUNDS.—No additional funds  
11       are authorized to be appropriated for the purpose of car-  
12       rying out this Act.