

Calendar No. 551

118TH CONGRESS
2D SESSION**S. 4715****[Report No. 118–238]**

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, Mr. OSSOFF, and Ms. ROSEN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

NOVEMBER 12, 2024

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italie*]

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

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

4 **SEC. 2. FEDERAL CYBER WORKFORCE DEVELOPMENT IN-**
5 **STITUTE.**

6 (a) **DEFINITIONS.**—In this section:

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

10 (2) **APPROPRIATE CONGRESSIONAL COMMIT-**
11 **TEES.**—The term “appropriate congressional com-
12 mittees” means—

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

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

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

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

21 (E) the Committee on Oversight and Ac-
22 countability of the House of Representatives.

23 (3) **CYBER WORK ROLE.**—The term “cyber
24 work role” means—

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

4 (B) a role relating to work involving de-
 5 signing, building, securing, operating, defend-
 6 ing, and protecting cyberspace resources.

7 (4) DIRECTOR.—The term “Director” means
 8 the National Cyber Director.

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

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

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

21 (b) REQUIREMENT.—

22 (1) IN GENERAL.—Not later than 180 days
 23 after the date of enactment of this Act, the Director,
 24 in consultation with the Secretary of Homeland Se-
 25 curity, the Secretary of Defense, the Director of the

1 Office of Personnel Management, and the head of
2 any other agency the Director determines necessary,
3 shall submit to Congress and make publicly available
4 a plan for the establishment of a Federal institute
5 to provide—

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

11 (B) training for personnel with responsibil-
12 ities for human resource functions relating to
13 cyber personnel.

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

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

23 (B) coordinate with the Secretary of
24 Homeland Security, the Secretary of Defense,
25 and the heads of other agencies determined nec-

1 essary by the Director to develop a cyber work
2 role-specific curriculum for the training pro-
3 vided under subparagraph (A)—

4 (i) in accordance with the NICE
5 framework; and

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

8 (C) prioritize entry-level positions in the
9 provision of curriculum development and train-
10 ing;

11 (D) address the training needs of—

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

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

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

21 (F) consider developing a specific module
22 to familiarize and train appropriate Federal
23 Government hiring managers and human re-
24 sources staff in the unique challenges in recruit-

ing and hiring personnel for Federal cyber work
force roles;

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

(H) develop a badging system to commu-
nicate qualification and proficiency for individ-
uals who successfully complete training through
the Federal institute with consideration of sys-
tems 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 irrespec-
tive of whether an individual has a college de-
gree or a college degree in a cyber-related dis-
cipline.

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

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

(B) to the greatest extent practicable, align
training and tools, including cyber work roles

1 and competencies and the associated tasks,
2 knowledge, and skills from—

3 (i) the Special Publication of the Na-
4 tional Institute of Standards and Tech-
5 nology 800–181, Revision 1, entitled “Na-
6 tional Initiative for Cybersecurity Edu-
7 cation Workforce Framework for Cyberse-
8 curity”, or any successor special publica-
9 tion; or

10 (ii) other applicable publications, stud-
11 ies, or guidance of the Federal Govern-
12 ment;

13 (C) identify—

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

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

23 (D) recommend a course curriculum, deliv-
24 ery method, and length of curriculum for the
25 training provided under paragraph (1)(A) using

1 Federal Government cyber training programs as
2 models, including the Joint Cyber Analysis
3 Course of the Department of Defense and the
4 Federal Cyber Defense Skilling Academy of the
5 Cybersecurity and Infrastructure Security
6 Agency;

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

9 (F) describe a security clearance process to
10 complete some level of security clearance for ap-
11 propriate individuals while individuals are en-
12 rolled in training;

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

19 (H) provide an estimate of the funding and
20 new authorities required to establish and oper-
21 ate the Federal institute;

22 (I) describe any requirements for the Fed-
23 eral institute to conduct work in a classified
24 setting;

1 (J) identify how the Federal institute
2 would—

3 (i) provide some or all of the training
4 required by paragraph (1)(A) through 5
5 academic institutions from among aca-
6 demic institutions that—

7 (I) are designated by the Na-
8 tional Security Agency as a National
9 Center of Academic Excellence in cy-
10 bersecurity for cyber defense, cyber
11 research, and cyber operations; and

12 (H) have an operational sensitive
13 compartmented information facility;
14 and

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

17 (K) identify how the instructors of the
18 Federal institute will remain current with re-
19 spect to cybersecurity knowledge, skills and
20 abilities through scholarship or other means;
21 and

22 (L) identify how the Federal institute will
23 maintain the quality and longevity of instruc-
24 tors.

1 (4) CONSULTATION.—In developing a plan for
 2 the Federal institute, the Director shall consult with
 3 the Director of the Office of Personnel Management,
 4 the Chief Human Capital Officers Council, the Chief
 5 Information Officers Council, and the Chief Learn-
 6 ing Officers Council to establish tools for human re-
 7 sources professionals of the Federal Government to
 8 develop the knowledge, skills and abilities required
 9 to manage the career life cycle of cyber professionals
 10 from recruitment to retirement.

11 (e) BRIEFING.—Not later than 270 days after the
 12 date of enactment of this Act, the Director shall provide
 13 to the appropriate congressional committees a briefing on
 14 the plan required under subsection (b)(1), including an es-
 15 timate of the funding and the authorities necessary to im-
 16 plement the plan.

17 (d) NO ADDITIONAL FUNDS.—No additional funds
 18 are authorized to be appropriated for the purpose of ear-
 19 rying out this Act.

20 **SECTION 1. SHORT TITLE.**

21 *This Act may be cited as the “Federal Cyber Workforce*
 22 *Training Act of 2024”.*

23 **SEC. 2. FEDERAL CYBER WORKFORCE DEVELOPMENT INSTI-**
 24 **TUTE.**

25 (a) DEFINITIONS.—*In this section:*

1 (1) *AGENCY.*—*The term “agency” has the mean-*
 2 *ing given the term in section 551 of title 5, United*
 3 *States Code.*

4 (2) *APPROPRIATE CONGRESSIONAL COMMIT-*
 5 *TEES.*—*The term “appropriate congressional commit-*
 6 *tees” means—*

7 *(A) the Committee on Armed Services of the*
 8 *Senate;*

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

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

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

15 *(E) the Committee on Oversight and Ac-*
 16 *countability of the House of Representatives.*

17 (3) *CYBER WORK ROLE.*—*The term “cyber work*
 18 *role” means—*

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

22 *(B) a role relating to work involving de-*
 23 *signing, building, securing, operating, defending,*
 24 *and protecting cyberspace resources.*

1 (4) *DIRECTOR*.—*The term “Director” means the*
 2 *National Cyber Director.*

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

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

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

15 (b) *REQUIREMENT*.—

16 (1) *IN GENERAL*.—*Not later than 180 days after*
 17 *the date of enactment of this Act, the Director, in con-*
 18 *sultation with the Secretary of Homeland Security,*
 19 *the Secretary of Defense, the Director of the Office of*
 20 *Personnel Management, and the head of any other*
 21 *agency the Director determines necessary, shall sub-*
 22 *mit to Congress and make publicly available a plan*
 23 *for the establishment of a Federal institute to pro-*
 24 *vide—*

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

6 (B) training for personnel with responsibil-
7 ities for human resource functions relating to
8 cyber personnel.

9 (2) INSTITUTE FUNCTIONS.—The plan required
10 under paragraph (1) shall provide for the Federal in-
11 stitute to—

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

18 (B) coordinate with the Secretary of Home-
19 land Security, the Secretary of Defense, and the
20 heads of other agencies determined necessary by
21 the Director to develop a cyber work role-specific
22 curriculum for the training provided under sub-
23 paragraph (A)—

24 (i) in accordance with the NICE
25 framework; and

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

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

6 (D) address the training needs of—

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

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

12 (E) include curriculum development and
13 training for Federal cyber workers seeking tran-
14 sition to mid-career positions, which may in-
15 clude upskilling and reskilling efforts;

16 (F) consider developing a specific module to
17 familiarize and train appropriate Federal Gov-
18 ernment hiring managers and human resources
19 staff in the unique challenges in recruiting and
20 hiring personnel for Federal cyber work force
21 roles;

22 (G) incorporate work-based learning in per-
23 sonnel training;

24 (H) develop a badging system to commu-
25 nicate qualification and proficiency for individ-

1 *uals who successfully complete training through*
 2 *the Federal institute with consideration of sys-*
 3 *tems used by the intelligence community;*

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

7 *(J) provide training to individuals irrespec-*
 8 *tive of whether an individual has a college degree*
 9 *or a college degree in a cyber-related discipline.*

10 *(3) PLAN ELEMENTS.—The plan required under*
 11 *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 NICE framework; or*

21 *(ii) other applicable publications, stud-*
 22 *ies, or guidance of the Federal Government;*

23 *(C) identify—*

24 *(i) elements of the Federal institute*
 25 *and its functions that could use existing fa-*

1 *cilities, resources, and programs of the Fed-*
2 *eral Government; and*

3 *(ii) elements of the Federal institute*
4 *and its functions that would require new fa-*
5 *cilities, resources, and programs of the Fed-*
6 *eral Government in order to implement the*
7 *plan required under paragraph (1);*

8 *(D) recommend a course curriculum, deliv-*
9 *ery method, and length of curriculum for the*
10 *training provided under paragraph (1)(A) using*
11 *Federal Government cyber training programs as*
12 *models, including the Joint Cyber Analysis*
13 *Course of the Department of Defense and the*
14 *Federal Cyber Defense Skilling Academy of the*
15 *Cybersecurity and Infrastructure Security Agen-*
16 *cy;*

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

19 *(F) describe a security clearance process to*
20 *complete some level of security clearance for ap-*
21 *propriate individuals while individuals are en-*
22 *rolled in training;*

23 *(G) recommend a governance structure for*
24 *the Federal institute that would ensure ongoing*
25 *interagency coordination in the development of a*

1 curriculum, the provision of training, and other
2 considerations the Director determines appro-
3 priate;

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

7 (I) describe any requirements for the Fed-
8 eral institute to conduct work in a classified set-
9 ting;

10 (J) identify how the Federal institute
11 would—

12 (i) provide some or all of the training
13 required by paragraph (1)(A) through 5
14 academic institutions from among academic
15 institutions that—

16 (I) are designated by the National
17 Security Agency as a National Center
18 of Academic Excellence in cybersecu-
19 rity for cyber defense, cyber research,
20 and cyber operations; and

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

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

1 (K) identify how the instructors of the Fed-
 2 eral institute will remain current with respect to
 3 cybersecurity knowledge, skills, and abilities
 4 through scholarship or other means; and

5 (L) identify how the Federal institute will
 6 maintain the quality and longevity of instruc-
 7 tors.

8 (4) CONSULTATION.—In developing a plan for
 9 the Federal institute, the Director shall consult with
 10 the Director of the Office of Personnel Management,
 11 the Chief Human Capital Officers Council, the Chief
 12 Information Officers Council, and the Chief Learning
 13 Officers Council to establish tools for human resources
 14 professionals of the Federal Government to develop the
 15 knowledge, skills, and abilities required to manage the
 16 career life cycle of cyber professionals from recruit-
 17 ment to retirement.

18 (c) BRIEFING.—Not later than 280 days after the date
 19 of enactment of this Act, the Director shall provide to the
 20 appropriate congressional committees a briefing on the plan
 21 required under subsection (b)(1), including an estimate of
 22 the funding and the authorities necessary to implement the
 23 plan.

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

Calendar No. 551

118TH CONGRESS
2^D Session

S. 4715

[Report No. 118-238]

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.

NOVEMBER 12, 2024

Reported with an amendment