

119TH CONGRESS
1ST SESSION

H. R. 3435

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 HOUSE OF REPRESENTATIVES

MAY 15, 2025

Mr. FALLON (for himself and Ms. KAPTUR) introduced the following bill;
which was referred to the Committee on Oversight and Government Reform

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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Federal Cyber Work-
5 force Training Act of 2025”.

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

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

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

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

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

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

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

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

15 (E) the Committee on Oversight and Gov-
16 ernment Reform of the House of Representa-
17 tives.

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

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

23 (B) a role relating to work involving de-
24 signing, building, securing, operating, defend-
25 ing, and protecting cyberspace resources.

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

3 (5) FEDERAL INSTITUTE.—The term “Federal
4 institute” means the Federal institute described in
5 the 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 Tech-
14 nical Education Act of 2006 (20 U.S.C. 2302).

15 (b) REQUIREMENT.—

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

1 (A) training for personnel hired for cyber
2 work roles in the Federal Government, includ-
3 ing new hires and personnel seeking transition
4 to 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
11 institute 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
19 Homeland Security, the Secretary of Defense,
20 and the heads of other agencies determined nec-
21 essary by the Director to develop a cyber work
22 role-specific curriculum for the training pro-
23 vided under subparagraph (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
8 mid-career positions; and

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

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

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

22 (G) incorporate work-based learning in
23 personnel 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 de-
9 gree or a college degree in a cyber-related dis-
10 cipline.

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

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

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

21 (i) Special Publication 800–181, Revi-
22 sion 1, of the National Institute of Stand-
23 ards and Technology entitled “National
24 Initiative for Cybersecurity Education

1 Workforce Framework for Cybersecurity”,
2 or any successor special publication; 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 270 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.

○