

114TH CONGRESS
1ST SESSION

S. 2007

To create a consistent framework to expedite the recruitment of highly qualified personnel who perform information technology, cybersecurity, and cyber-related functions to enhance cybersecurity across the Federal Government.

IN THE SENATE OF THE UNITED STATES

AUGUST 6, 2015

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

A BILL

To create a consistent framework to expedite the recruitment of highly qualified personnel who perform information technology, cybersecurity, and cyber-related functions to enhance cybersecurity across the Federal Government.

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 Cybersecurity
5 Workforce Assessment Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) 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 in
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 Gov-
13 ernment Reform of House of Representatives.

14 (2) DIRECTOR.—The term “Director” means
15 the Director of the Office of Personnel Management.

16 (3) ROLES.—The term “roles” has the meaning
17 given the term in the National Initiative for Cyber-
18 security Education’s Cybersecurity Workforce
19 Framework.

20 **SEC. 3. NATIONAL CYBERSECURITY WORKFORCE MEAS-**
21 **UREMENT INITIATIVE.**

22 (a) IN GENERAL.—The head of each Federal agency
23 shall—

1 (1) identify all positions within the agency that
2 require the performance of information technology,
3 cybersecurity, or other cyber-related functions; and

4 (2) assign the corresponding employment code,
5 which shall be added to the National Initiative for
6 Cybersecurity Education's National Cybersecurity
7 Workforce Framework, in accordance with sub-
8 section (b).

9 (b) EMPLOYMENT CODES.—

10 (1) PROCEDURES.—

11 (A) CODING STRUCTURE.—Not later than
12 180 days after the date of the enactment of this
13 Act, the Secretary of Commerce, acting through
14 the National Institute of Standards and Tech-
15 nology, shall update the National Initiative for
16 Cybersecurity Education's Cybersecurity Work-
17 force Framework to include a corresponding
18 coding structure.

19 (B) IDENTIFICATION OF CIVILIAN CYBER
20 PERSONNEL.—Not later than 9 months after
21 the date of enactment of this Act, the Director,
22 in coordination with the Director of National
23 Intelligence, shall establish procedures to imple-
24 ment the National Initiative for Cybersecurity
25 Education's coding structure to identify all

1 Federal civilian positions that require the per-
2 formance of information technology, cybersecu-
3 rity, or other cyber-related functions.

4 (C) IDENTIFICATION OF NON-CIVILIAN
5 CYBER PERSONNEL.—Not later than 18 months
6 after the date of enactment of this Act, the Sec-
7 retary of Defense shall establish procedures to
8 implement the National Initiative for Cyberse-
9 curity Education’s coding structure to identify
10 all Federal non-civilian positions that require
11 the performance of information technology, cy-
12 bersecurity or other cyber-related functions.

13 (D) BASELINE ASSESSMENT OF EXISTING
14 CYBERSECURITY WORKFORCE.—Not later than
15 3 months after the date on which the proce-
16 dures are developed under subparagraphs (B)
17 and (C), respectively, the head of each Federal
18 agency shall submit to the appropriate congres-
19 sional committees of jurisdiction a report that
20 identifies—

21 (i) the percentage of personnel with
22 information technology, cybersecurity, or
23 other cyber-related job functions who cur-
24 rently hold the appropriate industry-recog-
25 nized certifications as identified in the Na-

1 tional Initiative for Cybersecurity Edu-
2 cation's Cybersecurity Workforce Frame-
3 work;

4 (ii) the level of preparedness of other
5 civilian and non-civilian cyber personnel
6 without existing credentials to pass certifi-
7 cation exams; and

8 (iii) a strategy for mitigating any
9 gaps identified in clause (i) or (ii) with the
10 appropriate training and certification for
11 existing personnel.

12 (E) PROCEDURES FOR ASSIGNING
13 CODES.—Not later than 3 months after the
14 date on which the procedures are developed
15 under subparagraphs (B) and (C), respectively,
16 the head of each Federal agency shall establish
17 procedures—

18 (i) to identify all encumbered and va-
19 cant positions with information technology,
20 cybersecurity, or other cyber-related func-
21 tions (as defined in the National Initiative
22 for Cybersecurity Education's coding struc-
23 ture); and

1 (ii) to assign the appropriate employ-
2 ment code to each such position, using
3 agreed standards and definitions.

4 (2) CODE ASSIGNMENTS.—Not later than 1
5 year after the date after the procedures are estab-
6 lished under paragraph (1)(E), the head of each
7 Federal agency shall complete assignment of the ap-
8 propriate employment code to each position within
9 the agency with information technology, cybersecu-
10 rity, or other cyber-related functions.

11 (c) PROGRESS REPORT.—Not later than 180 days
12 after the date of enactment of this Act, the Director shall
13 submit a progress report on the implementation of this
14 section to the appropriate congressional committees.

15 **SEC. 4. IDENTIFICATION OF CYBER-RELATED ROLES OF**
16 **CRITICAL NEED.**

17 (a) IN GENERAL.—Beginning not later than 1 year
18 after the date on which the employment codes are assigned
19 to employees pursuant to section 3(b)(2), and annually
20 through 2022, the head of each Federal agency, in con-
21 sultation with the Director and the Secretary of Homeland
22 Security, shall—

23 (1) identify information technology, cybersecu-
24 rity, or other cyber-related roles of critical need in
25 the agency's workforce; and

1 (2) submit a report to the Director that—

2 (A) describes the information technology,
3 cybersecurity, or other cyber-related roles iden-
4 tified under paragraph (1); and

5 (B) substantiates the critical need designa-
6 tions.

7 (b) GUIDANCE.—The Director shall provide Federal
8 agencies with timely guidance for identifying information
9 technology, cybersecurity, or other cyber-related roles of
10 critical need, including—

11 (1) current information technology, cybersecu-
12 rity, and other cyber-related roles with acute skill
13 shortages; and

14 (2) information technology, cybersecurity, or
15 other cyber-related roles with emerging skill short-
16 ages.

17 (c) CYBERSECURITY NEEDS REPORT.—Not later
18 than 2 years after the date of the enactment of this Act,
19 the Director, in consultation with the Secretary of Home-
20 land Security, shall—

21 (1) identify critical needs for information tech-
22 nology, cybersecurity, or other cyber-related work-
23 force across all Federal agencies; and

1 (2) submit a progress report on the implemen-
2 tation of this section to the appropriate congres-
3 sional committees.

4 **SEC. 5. GOVERNMENT ACCOUNTABILITY OFFICE STATUS**
5 **REPORTS.**

6 The Comptroller General of the United States shall—

7 (1) analyze and monitor the implementation of
8 sections 3 and 4; and

9 (2) not later than 3 years after the date of the
10 enactment of this Act, submit a report to the appro-
11 priate congressional committees that describes the
12 status of such implementation.

○