

116TH CONGRESS
2D SESSION

H. R. 7590

To establish in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security a pilot program for the purpose of carrying out a talent exchange program between the private sector and the Cybersecurity and Infrastructure Security Agency, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 13, 2020

Mr. KATKO (for himself, Mr. BRINDISI, and Mr. GALLAGHER) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Oversight and Reform, and Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To establish in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security a pilot program for the purpose of carrying out a talent exchange program between the private sector and the Cybersecurity and Infrastructure Security Agency, and for other purposes.

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. ESTABLISHMENT OF PUBLIC-PRIVATE TALENT**
2 **EXCHANGE FOR CYBERSECURITY SKILLS DE-**
3 **VELOPMENT.**

4 (a) PURPOSE.—There is established, within the Cy-
5 bersecurity and Infrastructure Security Agency of the De-
6 partment of Homeland Security, a pilot program for the
7 purpose of carrying out a talent exchange program be-
8 tween the private sector and the Cybersecurity and Infra-
9 structure Security Agency (in this section referred to as
10 the “program”) in order to—

11 (1) facilitate collaboration with the best and
12 most diverse minds from outside the Federal Gov-
13 ernment to improve national security;

14 (2) incorporate public and private sector talent
15 to challenge thinking, test innovative ideas, and en-
16 able greater understanding on cybersecurity, bring-
17 ing public and private sector expertise together in a
18 way that helps both sectors learn lessons, identify
19 systemic vulnerabilities, and reduce the future im-
20 pact of cyber attacks; and

21 (3) expand existing Cybersecurity and Infra-
22 structure Security Agency programs that integrate
23 private sector and interagency personnel.

24 (b) REQUIREMENTS.—In carrying out the program,
25 the Director of the Cybersecurity and Infrastructure Secu-
26 rity Agency shall—

1 (1) promote public-private cooperation and in-
2 telligence sharing;

3 (2) develop and publicize the knowledge, skills,
4 and abilities, including relevant education, training,
5 apprenticeships, certifications, and other experi-
6 ences, that are required to participate in the pro-
7 gram;

8 (3) provide for participation by cleared and
9 uncleared public and private employees; and

10 (4) develop a plan and application process for
11 the private sector to participate in the program.

12 (c) ASSIGNMENT AUTHORITY.—The Director of the
13 Cybersecurity and Infrastructure Security Agency may,
14 with the agreement of a private sector entity and the con-
15 sent of a employee of the Agency or such entity, as the
16 case may be, arrange for the temporary assignment of—

17 (1) such employee of the Agency to such entity;
18 or

19 (2) such employee of such entity to the Agency.

20 (d) AGREEMENTS.—

21 (1) IN GENERAL.—Before any temporary as-
22 signment may be made under the program, the Di-
23 rector of the Cybersecurity and Infrastructure Secu-
24 rity Agency shall enter into a written agreement
25 with the private sector entity and the employee con-

cerned regarding the terms and conditions of such assignment, which shall—

(A) require that an employee of the Cybersecurity and Infrastructure Security Agency, upon completion of such assignment, serve in the Cybersecurity and Infrastructure Security Agency, or, if appropriate, elsewhere in the civil service, for a period of time equal to at least twice the length of such assignment;

(B) provide that if an employee of the Cybersecurity and Infrastructure Security Agency or of the private sector entity, as the case may be, fails to abide by the terms of such agreement, such employee shall be liable to the United States for payment of all expenses of the assignment of such employee, including the value of the salary and benefits of such employee, unless such failure was for good cause as determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(C) contain language prohibiting an employee of the Cybersecurity and Infrastructure Security Agency from improperly utilizing predecisional or draft deliberative information such employee may be privy to or aware of related to

1 Department of Homeland Security programing,
2 budgeting, resourcing, acquisition, or procure-
3 ment for the benefit or advantage of the private
4 sector entity at which such employee is tempo-
5 rarily assigned.

6 (2) COLLECTION OF COSTS.—

7 (A) IN GENERAL.—An amount for which
8 an employee is liable under paragraph (1)(B)
9 shall be treated as a debt due the United
10 States.

11 (B) WAIVER.—The Director may waive, in
12 whole or in part, collection of a debt described
13 in subparagraph (A) based on a determination
14 that the collection would be against equity and
15 good conscience and not in the best interests of
16 the United States, after taking into account any
17 indication of fraud, misrepresentation, fault, or
18 lack of good faith on the part of the employee
19 concerned.

20 (e) TERMINATION.—An assignment under the pro-
21 gram may, at any time and for any reason, be terminated
22 by the Director of the Cybersecurity and Infrastructure
23 Security Agency or the private sector entity concerned.

24 (f) DURATION.—

1 (1) IN GENERAL.—An assignment under the
2 program shall be for a period of not less than one
3 year and not more than three years.

4 (2) CISA EMPLOYEES.—No employee of the
5 Cybersecurity and Infrastructure Security Agency
6 may be assigned under the program for more than
7 a total of four years inclusive of all such assign-
8 ments.

9 (g) STATUS OF FEDERAL EMPLOYEES ASSIGNED TO
10 PRIVATE-SECTOR ENTITIES.—An employee of the Cyber-
11 security and Infrastructure Security Agency who is as-
12 signed to a private sector entity under the program shall
13 be considered, during the period of such assignment, to
14 be employed by the Cybersecurity and Infrastructure Se-
15 curity Agency for all purposes.

16 (h) MISSION CONTINUITY.—Before authorizing the
17 temporary assignment of an employee of the Cybersecurity
18 and Infrastructure Security Agency to a private sector en-
19 tity under the program, the Director of the Cybersecurity
20 and Infrastructure Security Agency shall—

21 (1) ensure that the normal duties and functions
22 of such employee can be reasonably performed by
23 other employees of the Cybersecurity and Infrastruc-
24 ture Security Agency without the permanent trans-

1 fer or reassignment of other personnel of the Cyber-
2 security and Infrastructure Security Agency;

3 (2) ensure that the normal duties and functions
4 of such employee are not, as a result of and during
5 the course of such assignment, performed or aug-
6 mented by contractor personnel in violation of sec-
7 tion 1710 of title 41, United States Code; and

8 (3) certify that such assignment shall not have
9 an adverse or negative impact on mission attainment
10 or organizational capabilities associated with such
11 assignment.

12 (i) TERMS AND CONDITIONS FOR PRIVATE-SECTOR
13 EMPLOYEES.—An employee of a private sector entity who
14 is assigned to the Cybersecurity and Infrastructure Secu-
15 rity Agency under the program—

16 (1) shall continue to receive pay and benefits
17 from the private sector entity from which such em-
18 ployee is assigned and may not receive pay or bene-
19 fits from the Cybersecurity and Infrastructure Secu-
20 rity Agency;

21 (2) may not have access to any trade secrets or
22 to any other nonpublic information which is of com-
23 mercial value to such private sector entity;

24 (3) may perform work that is considered inher-
25 ently governmental in nature only when requested in

1 writing by the Director of the Cybersecurity and In-
2 frastructure Security Agency; and

3 (4) may not be used to circumvent the provi-
4 sions of section 1710 of title 41, United States
5 Code.

6 (j) REPORTING REQUIREMENT.—The Director of the
7 Cybersecurity and Infrastructure Security Agency shall
8 submit to the Committee on Homeland Security and Gov-
9 ernmental Affairs of the Senate and the Committee on
10 Homeland Security of the House of Representatives, not
11 later than 1 month after the end of the fiscal year in-
12 volved, a report on any activities carried out utilizing the
13 authorities provided by this section during that fiscal year,
14 including information concerning—

15 (1) the private sector entities to and from which
16 employees were assigned under the program;

17 (2) the positions such employees held while so
18 assigned;

19 (3) a description of the tasks such employees
20 performed while so assigned; and

21 (4) a discussion of any actions that might be
22 taken to improve the effectiveness of the program,
23 including any proposed changes in law.

24 (k) SENSE OF CONGRESS.—It is the sense of Con-
25 gress that—

1 (1) value is derived from the program when
2 participants are meaningfully integrated into their
3 host entities, which will often require a personnel se-
4 curity clearance process for participants from the
5 private sector;

6 (2) the success of the program, and the work-
7 force development efforts critical for the success of
8 key national security priorities more generally, are
9 severely hampered by the current personnel security
10 clearance process; and

11 (3) until such time as the wait times for per-
12 sonnel security clearances meet the stated goals of
13 Federal departments and agencies, in order to im-
14 plement the program, the Director of the Cybersecu-
15 rity and Critical Infrastructure Agency should en-
16 courage—

17 (A) declassification of information as
18 broadly and quickly as possible; and

19 (B) participation of the private sector at
20 the unclassified level to promote open dialogue
21 and information sharing outside the classified
22 space.

○