

AMENDMENT TO RULES COMMITTEE PRINT FOR

H.R. 6395

OFFERED BY *Mr. Langevin of Rhode Island*

At the appropriate place in the bill, insert the following:

1 **SEC. ____ . 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

1 systemic vulnerabilities, and reduce the future im-
2 pact of cyber attacks; and

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

6 (b) REQUIREMENTS.—In carrying out the program,
7 the Director of the Cybersecurity and Infrastructure Secu-
8 rity Agency shall—

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

11 (2) develop and publicize the knowledge, skills,
12 and abilities, including relevant education, training,
13 apprenticeships, certifications, and other experi-
14 ences, that are required to participate in the pro-
15 gram;

16 (3) provide for participation by cleared and
17 uncleared public and private employees; and

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

20 (c) ASSIGNMENT AUTHORITY.—The Director of the
21 Cybersecurity and Infrastructure Security Agency may,
22 with the agreement of a private sector entity and the con-
23 sent of a employee of the Agency or such entity, as the
24 case may be, arrange for the temporary assignment of—

1 (1) such employee of the Agency to such entity;

2 or

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

4 (d) AGREEMENTS.—

5 (1) IN GENERAL.—Before any temporary as-
6 signment may be made under the program, the Di-
7 rector of the Cybersecurity and Infrastructure Secu-
8 rity Agency shall enter into a written agreement
9 with the private sector entity and the employee con-
10 cerned regarding the terms and conditions of such
11 assignment, which shall—

12 (A) require that an employee of the Cyber-
13 security and Infrastructure Security Agency,
14 upon completion of such assignment, serve in
15 the Cybersecurity and Infrastructure Security
16 Agency, or, if appropriate, elsewhere in the civil
17 service, for a period of time equal to at least
18 twice the length of such assignment;

19 (B) provide that if an employee of the Cy-
20 bersecurity and Infrastructure Security Agency
21 or of the private sector entity, as the case may
22 be, fails to abide by the terms of such agree-
23 ment, such employee shall be liable to the
24 United States for payment of all expenses of
25 the assignment of such employee, including the

1 value of the salary and benefits of such em-
2 ployee, unless such failure was for good cause
3 as determined by the Director of the Cybersecu-
4 rity and Infrastructure Security Agency; and

5 (C) contain language prohibiting an em-
6 ployee of the Cybersecurity and Infrastructure
7 Security Agency from improperly utilizing pre-
8 decisional or draft deliberative information such
9 employee may be privy to or aware of related to
10 Department of Homeland Security programing,
11 budgeting, resourcing, acquisition, or procure-
12 ment for the benefit or advantage of the private
13 sector entity at which such employee is tempo-
14 rarily assigned.

15 (2) COLLECTION OF COSTS.—

16 (A) IN GENERAL.—An amount for which
17 an employee is liable under paragraph (1)(B)
18 shall be treated as a debt due the United
19 States.

20 (B) WAIVER.—The Director may waive, in
21 whole or in part, collection of a debt described
22 in subparagraph (A) based on a determination
23 that the collection would be against equity and
24 good conscience and not in the best interests of
25 the United States, after taking into account any

1 indication of fraud, misrepresentation, fault, or
2 lack of good faith on the part of the employee
3 concerned.

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

8 (f) DURATION.—

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

12 (2) CISA EMPLOYEES.—No employee of the
13 Cybersecurity and Infrastructure Security Agency
14 may be assigned under the program for more than
15 a total of four years inclusive of all such assign-
16 ments.

17 (g) STATUS OF FEDERAL EMPLOYEES ASSIGNED TO
18 PRIVATE-SECTOR ENTITIES.—An employee of the Cyber-
19 security and Infrastructure Security Agency who is as-
20 signed to a private sector entity under the program shall
21 be considered, during the period of such assignment, to
22 be employed by the Cybersecurity and Infrastructure Se-
23 curity Agency for all purposes.

24 (h) MISSION CONTINUITY.—Before authorizing the
25 temporary assignment of an employee of the Cybersecurity

1 and Infrastructure Security Agency to a private sector en-
2 tity under the program, the Director of the Cybersecurity
3 and Infrastructure Security Agency shall—

4 (1) ensure that the normal duties and functions
5 of such employee can be reasonably performed by
6 other employees of the Cybersecurity and Infrastruc-
7 ture Security Agency without the permanent trans-
8 fer or reassignment of other personnel of the Cyber-
9 security and Infrastructure Security Agency;

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

15 (3) certify that such assignment shall not have
16 an adverse or negative impact on mission attainment
17 or organizational capabilities associated with such
18 assignment.

19 (i) **TERMS AND CONDITIONS FOR PRIVATE-SECTOR**
20 **EMPLOYEES.**—An employee of a private sector entity who
21 is assigned to the Cybersecurity and Infrastructure Secu-
22 rity Agency under the program—

23 (1) shall continue to receive pay and benefits
24 from the private sector entity from which such em-
25 ployee is assigned and may not receive pay or bene-

1 fits from the Cybersecurity and Infrastructure Secu-
2 rity Agency;

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

6 (3) may perform work that is considered inher-
7 ently governmental in nature only when requested in
8 writing by the Director of the Cybersecurity and In-
9 frastructure Security Agency; and

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

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

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

24 (2) the positions such employees held while so
25 assigned;

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

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

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

8 (1) value is derived from the program when
9 participants are meaningfully integrated into their
10 host entities, which will often require a personnel se-
11 curity clearance process for participants from the
12 private sector;

13 (2) the success of the program, and the work-
14 force development efforts critical for the success of
15 key national security priorities more generally, are
16 severely hampered by the current personnel security
17 clearance process; and

18 (3) until such time as the wait times for per-
19 sonnel security clearances meet the stated goals of
20 Federal departments and agencies, in order to im-
21 plement the program, the Director of the Cybersecu-
22 rity and Critical Infrastructure Agency should en-
23 courage—

24 (A) declassification of information as
25 broadly and quickly as possible; and

1 (B) participation of the private sector at
2 the unclassified level to promote open dialogue
3 and information sharing outside the classified
4 space.

