I

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. ESTABLISHMENT OF PUBLIC-PRIVATE TALENT EXCHANGE FOR CYBERSECURITY SKILLS DEVELOPMENT.

(a) PURPOSE.—There is established, within 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 (in this section referred to as the ''program'') in order to—

(1) facilitate collaboration with the best and most diverse minds from outside the Federal Government to improve national security;

(2) incorporate public and private sector talent to challenge thinking, test innovative ideas, and enable greater understanding on cybersecurity, bringing public and private sector expertise together in a way that helps both sectors learn lessons, identify systemic vulnerabilities, and reduce the future impact of cyber attacks; and

(3) expand existing Cybersecurity and Infrastructure Security Agency programs that integrate private sector and interagency personnel.

(b) REQUIREMENTS.—In carrying out the program, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) promote public-private cooperation and intelligence sharing;

(2) develop and publicize the knowledge, skills, and abilities, including relevant education, training, apprenticeships, certifications, and other experiences, that are required to participate in the program;

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

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

(c) ASSIGNMENT AUTHORITY.—The Director of the Cybersecurity and Infrastructure Security Agency may, with the agreement of a private sector entity and the consent of a employee of the Agency or such entity, as the case may be, arrange for the temporary assignment of—

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

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

(d) AGREEMENTS.—

(1) IN GENERAL.—Before any temporary assignment may be made under the program, the Director of the Cybersecurity and Infrastructure Security Agency shall enter into a written agreement 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

Department of Homeland Security programing, budgeting, resourcing, acquisition, or procurement for the benefit or advantage of the private sector entity at which such employee is temporarily assigned.

(2) COLLECTION OF COSTS.—

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

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

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

(f) DURATION.—

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

(2) CISA EMPLOYEES.—No employee of the Cybersecurity and Infrastructure Security Agency may be assigned under the program for more than a total of four years inclusive of all such assignments.

(g) STATUS OF FEDERAL EMPLOYEES ASSIGNED TO PRIVATE-SECTOR ENTITIES.—An employee of the Cybersecurity and Infrastructure Security Agency who is assigned to a private sector entity under the program shall be considered, during the period of such assignment, to be employed by the Cybersecurity and Infrastructure Security Agency for all purposes.

(h) MISSION CONTINUITY.—Before authorizing the temporary assignment of an employee of the Cybersecurity and Infrastructure Security Agency to a private sector entity under the program, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) ensure that the normal duties and functions of such employee can be reasonably performed by other employees of the Cybersecurity and Infrastructure Security Agency without the permanent trans-

fer or reassignment of other personnel of the Cybersecurity and Infrastructure Security Agency;

(2) ensure that the normal duties and functions of such employee are not, as a result of and during the course of such assignment, performed or augmented by contractor personnel in violation of section 1710 of title 41, United States Code; and

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

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

(1) shall continue to receive pay and benefits from the private sector entity from which such employee is assigned and may not receive pay or benefits from the Cybersecurity and Infrastructure Security Agency;

(2) may not have access to any trade secrets or to any other nonpublic information which is of commercial value to such private sector entity;

(3) may perform work that is considered inherently governmental in nature only when requested in

writing by the Director of the Cybersecurity and Infrastructure Security Agency; and

(4) may not be used to circumvent the provisions of section 1710 of title 41, United States Code.

(j) REPORTING REQUIREMENT.—The Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives, not later than 1 month after the end of the fiscal year involved, a report on any activities carried out utilizing the authorities provided by this section during that fiscal year, including information concerning—

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

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

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

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

(k) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) value is derived from the program when participants are meaningfully integrated into their host entities, which will often require a personnel security clearance process for participants from the private sector;

(2) the success of the program, and the workforce development efforts critical for the success of key national security priorities more generally, are severely hampered by the current personnel security clearance process; and

(3) until such time as the wait times for personnel security clearances meet the stated goals of Federal departments and agencies, in order to implement the program, the Director of the Cybersecurity and Critical Infrastructure Agency should encourage—

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

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

○