AMENDMENT TO RULES COMMITTEE PRINT 115–23
OFFERED BY MR. AGUILAR OF CALIFORNIA

At the end of subtitle D of title XVI, add the following new section:

SEC. 16. DEPARTMENT OF DEFENSE CYBER WORKFORCE DEVELOPMENT PILOT PROGRAM.

(a) ESTABLISHMENT.—The Secretary of Defense may carry out a pilot program to be known as the “Cyber Workforce Development Pilot Program” (in this section referred to as the “Pilot Program”) under which the Secretary shall provide funds, in addition to other funds that may be available, for the recruitment, training, professionalization, and retention of personnel in the cyber workforce of the Department of Defense.

(b) PURPOSE.—The purpose of the Pilot Program shall be to assess the effectiveness of carrying out a full-scale talent management program to ensure that the cyber workforce of the Department of Defense has the capacity, in both personnel and skills, needed to effectively perform its cyber missions and the kinetic missions impacted by cyber activities.
(c) MANAGEMENT.—The Pilot Program shall be managed by the Chief Information Officer of the Department of Defense, in consultation with the Principal Cyber Advisor to the Secretary of Defense.

(d) GUIDANCE.—The Chief Information Officer of the Department of Defense, in consultation with the Principal Cyber Advisor to the Secretary of Defense, shall issue guidance for the administration of the Pilot Program. Such guidance shall include provisions that—

(1) identify areas of need in the cyber workforce that funds under the Pilot Program may be used to address, including—

(A) changes to the types of skills needed in the cyber workforce;

(B) capabilities to develop the cyber workforce and assist members of the cyber workforce in achieving qualifications and professionalization through activities such as training, education, and exchange programs;

(C) incentives to retain qualified, experienced cyber workforce personnel; and

(D) incentives for attracting new, high-quality personnel to the cyber workforce;
(2) describe the process under which entities may submit an application to receive funds under the Pilot Program;

(3) describe the evaluation criteria to be used for approving or prioritizing applications for funds under the Pilot Program in any fiscal year; and

(4) describe measurable objectives of performance for determining whether funds under the Pilot Program are being used in compliance with this section.

(e) CONSIDERATIONS.—When selecting entities to provide training and education services under the Pilot Program, consideration shall be given to whether the entity providing such services is a Center of Academic Excellence in Information Assurance Education (as that term is defined in section 2200e of title 10, United States Code).

(f) ANNUAL REPORT.—Not later than 120 days after the end of each of fiscal year for which funds are appropriated for the Pilot Program, the Secretary of Defense shall submit to the congressional defense committees a report on the operation of the Pilot Program during such fiscal year. Each report shall include, for the fiscal year covered by such report, the following:
(1) A description of the expenditures made under the Pilot Program (including expenditures following a transfer of funds under the Pilot Program to a military department or Defense Agency) in such fiscal year, including the purpose of such expenditures.

(2) A description and assessment of improvements in the Department of Defense cyber workforce resulting from such expenditures.

(3) Recommendations for additional authorities to fulfill the purpose of the Pilot Program.

(4) A statement of the funds that remain available under the Pilot Program at the end of such fiscal year.

(g) TERMINATION.—The Pilot Program and the annual reporting requirement under subsection (f) shall each terminate on the date that is five years after the date on which funds are first appropriated for the Pilot Program and any funds not obligated or expended under the Pilot Program on that date shall be deposited in the general fund of the Treasury of the United States.

(h) CYBER WORKFORCE DEFINED.—In this Act, the term “cyber workforce” means the following:

(1) Personnel in positions that require the performance of cybersecurity or other cyber-related
functions as so identified pursuant to the Federal Cybersecurity Workforce Assessment Act of 2015 (Public Law 114–113; 5 U.S.C. 301 note).

(2) Military personnel or civilian employees of the Department of Defense who are not described in paragraph (1) but who—

(A) are assigned functions that contribute significantly to cyber operations; and

(B) are designated as temporary members of the cyber workforce by the Chief Information Officer of the Department of Defense, or by the head of a military department or Defense Agency, for the limited purpose of receiving training for the performance of cyber-related functions.