AMENDMENT TO RULES COMM. PRINT 119–33
OFFERED BY MR. PATRONIS OF FLORIDA

In title XV, subtitle A, add at the end the following new section:

SEC. 15___. PILOT PROGRAM ON DEPARTMENT OF DEFENSE PARTNERSHIPS WITH INSTITUTIONS OF HIGHER EDUCATION RECOGNIZED IN THE NATIONAL CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY PROGRAM.

(a) ESTABLISHMENT.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall establish a pilot program under the Defense Cyber Workforce Framework to assess the feasibility of partnering advanced cyberspace operations and information aggressor units of the Department of Defense with institutions of higher education recognized by the National Security Agency in the National Centers of Academic Excellence in Cybersecurity program for Cyber Research, Cyber Defense, or Cyber Operations—

(1) to improve the cyber workforce pipeline of the United States;

(2) to enhance military cyber training through academic collaboration, research, and cyber range

exercises, and to create direct pathways for students into Federal cybersecurity careers;

(3) to leverage existing scholarship and fellowship opportunities, such as the Cyber Service Academy, the Science, Mathematics and Research for Transformation program, and other cyber scholarship-for-service programs; and

(4) to improve coordination, guidance, and counseling for participating students seeking to pursue careers in cybersecurity or cyber operations in the Department of Defense or elsewhere in the Federal Government.

(b) ELEMENTS.—The pilot program required by subsection (a) shall include the following:

(1) Establishment of a research cell supporting aggressor operations through open-source intelligence, emerging threat analysis, and development of adversary emulation playbooks.

(2) An assessment framework for determining the impact of the program, including a cost-benefit analysis for partnering students with operational units, that—

(A) determines the time to clear students for participation in the program; and

(B) determines the time and cost necessary to get students access to networks required to provide operational support to military cyber operators.

(3) Assessment of the curricula for participating students to determine if such coursework is relevant and impactful in preparing such students to directly support operational military cyber operators.

(4) Tracking students participating in the program to determine how the pilot impacts potential future employment with the Department of Defense or the Federal Government.

(5) Development of a cyber threat intelligence engineering capability supporting participating institutions and Department of Defense cyber operators through—

(A) ingestion, normalization, validation, and standardization of cyber threat intelligence from operational and intelligence community sources;

(B) development of high-fidelity adversary emulation playbooks, threat models, and digital threat representations for use across Department of Defense cyber training, testing, and experimentation environments;

(C) support for live, virtual, and constructive cyber range environments used for workforce development, operational training, and cyber test and evaluation activities; and

(D) development of student internship, fellowship, and scholarship opportunities focused on cyber threat intelligence, adversary emulation, and cyber range engineering disciplines.

(c) DURATION.—The pilot program established under subsection (a) shall terminate on September 30, 2031.