AMENDMENT TO RULES COMMITTEE PRINT 116-19
OFFERED BY MR. NORMAN OF SOUTH CAROLINA

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

SEC. 16. CYBERSECURITY DEFENSE ACADEMY PILOT PROGRAM.

(a) PROGRAM REQUIRED.—The Secretary of Defense carry out a pilot program under which the Secretary shall seek to enter into a public-private partnership with eligible cybersecurity organizations to train and place veterans as cybersecurity personnel within the Department of Defense. The public-private partnership entered into under this subsection shall be known as the “Cybersecurity Defense Academy”.

(b) ACTIVITIES.—The Cybersecurity Defense Academy shall provide educational courses in topics relating to cybersecurity, including the following:

(1) Cybersecurity analysis.
(2) Cybersecurity penetration testing.
(3) Cybersecurity threat hunting.
(4) Cybersecurity advanced exploitation.
(5) Linux systems administration.
(6) Robotics process automation analysis.

(e) Placement of Graduates.—

(1) In general.—The Secretary of Defense shall establish a process under which an individual who has completed a course of study at the Cybersecurity Defense Academy may be placed in a cybersecurity-related position within the Department of Defense.

(2) Waiver of Certification.—The Secretary of Defense shall waive the certification requirements set forth in Department of Defense Directives 8570 and 8140 with respect to the initial placement of an individual described in paragraph (1) if the Secretary Determines that the training provided to the individual by the Cybersecurity Defense Academy meets or exceeds the level of training required by such directives.

(d) Eligible Cybersecurity Organization Defined.—In this section, the term “eligible cybersecurity organization” means an nonprofit or for-profit organization that—

(1) has a history of working with state and local governments;

(2) is accredited by the American National Standards Institute;
(3) has experience placing veterans in
cybersecurity positions;

(4) does not charge fees to servicemembers or
veterans for taking a cybersecurity course; and

(5) aligns aptitude and psychometric selection
with cybersecurity career choice.

(e) INITIAL REPORT.—Not later than 90 days after
the date one which the 50th graduate of the Cybersecurity
Defense Academy is placed in the Department of Defense,
the Secretary of Defense shall submit to the congressional
defense committees a report that includes the following:

(1) The number of individuals who graduated
from the Cybersecurity Defense Academy.

(2) The number of such individuals who were
directly placed in cybersecurity positions with em-
ployers.

(3) The efficiency and effectiveness (speed of
entry and candidate selection) based on aptitude and
psychometric tools utilized to allocate veterans to
cybersecurity roles.

(4) The benefits or burdens of permanently es-
tablishing the Cybersecurity Defense Academy.

(5) Recommendations identifying any specific
actions that should be carried out if the program
under this section should become permanent.
(6) Recommendations for any changes to Department of Defense Directives 8570 and 8140.

(f) TERMINATION.—

(1) IN GENERAL.—Except as provided in paragraph (2), the program under this section shall terminate on the date that is five years after the date of the enactment of this Act.

(2) CONTINUATION.—The Secretary of Defense may continue the program after the termination date applicable under paragraph (1) if the Secretary determines that continuation of the program after that date is advisable and appropriate. If the Secretary determines to continue the program after that date, the Secretary shall do the following:

(A) Not later than 180 days after the date on which the report is submitted under subsection (e), the Secretary shall submit to the congressional defense committees a report describing the reasons for the determination to continue the program.

(B) The Secretary shall—

(i) establish the program throughout the Department of Defense and individual service branches;
(ii) make recommendations to the President and all committees of Congress for making the program applicable to all departments and agencies of the Federal Government;

(iii) conduct contract negotiations with companies that provide services under the program to ensure that such services are provided at a cost-effective rate; and

(iv) ensure that cybersecurity courses accredited by the American National Standards Institute are integrated into level III of the IAT, IAM, and IASE baseline certifications described in Department of Defense Directive 8570.