I

113TH CONGRESS
2D SESSION

H. R. 4500

To improve the management of cyber and information technology ranges and facilities of the Department of Defense, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 28, 2014

Mr. KILMER (for himself, Ms. TSONGAS, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on Armed Services

---

A BILL

To improve the management of cyber and information technology ranges and facilities of the Department of Defense, 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. CYBER AND INFORMATION TECHNOLOGY RANGES.

(a) MANAGEMENT OF CYBER RANGES AND FACILITIES.—Subsection (b) of section 932 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66) is amended—

(1) by adding at the end the following new paragraphs:

''(3) LIST OF CYBER AND INFORMATION TECHNOLOGY RANGES AND FACILITIES.—

''(A) IN GENERAL.—The Principal Cyber Advisor designated under subsection (c)(1) shall establish a comprehensive list of the cyber and information technology ranges and facilities of the Department of Defense.

''(B) TERMINOLOGY.—In establishing the list under subparagraph (A), the Principal Cyber Advisor shall denote whether each cyber and information technology range and facility is—

''(i) a 'cyber range', as defined by the Principal Cyber Advisor pursuant to subsection (c)(2)(C); or

''(ii) an 'IT range', as defined by the Principal Cyber Advisor pursuant to such subsection.

''(C) SUBMISSION.—Not later than one year after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2015, the Principal Cyber Advisor shall submit to the congressional defense committees the list established under subparagraph (A).

''(4) MANAGEMENT OF SYSTEMS.—The Principal Cyber Advisor shall determine, on a case by case basis, whether a cyber and information technology range and facility listed under paragraph (3)(A) should be centrally managed under paragraph (5) to increase efficiency, provide capability or capacity to more elements of the Department of Defense, or both.

''(5) COORDINATING ENTITY.—

''(A) ESTABLISHMENT.—Not later than 270 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2015, the Secretary of Defense shall establish an entity, or designate an element of the Department of Defense, to coordinate cyber and information technology ranges and facilities that the Principal Cyber Advisor determines should be centrally managed under paragraph (4).

''(B) DUTIES.—With respect to the cyber and information technology ranges and facilities designated under paragraph (4), the head of the entity established or designated under subparagraph (A) shall be responsible for the following:

''(i) Managing the cyber and information technology ranges and facilities, including coordinating the scheduling of ranges and facilities.

''(ii) Identifying and providing guidance to the Secretary with respect to opportunities for integration among the cyber and information technology ranges and facilities regarding testing, training, and developing functions.

''(iii) Assisting the military departments, the National Guard, and the elements of the Department gain access to the cyber and information technology ranges and facilities.

''(C) REPORTS.—The head of the entity established or designated under subparagraph (A) shall submit to the congressional defense committees—

''(i) an annual report on the opportunities for cost reduction and improvements to the integration and coordination of the cyber and information technology ranges and facilities; and

''(ii) by not later than one year after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2015, an initial report on the status, integration efforts, and usage of cyber and information technology ranges and facilities.

''(6) CYBER AND INFORMATION TECHNOLOGY RANGES AND FACILITIES DEFINED.—In this subsection, the term 'cyber and information technology ranges and facilities' means cyber ranges, test facilities, test beds, and other means of the Department of Defense for testing, training, and developing software, personnel, and tools for accommodating the mission of the Department.''; and

(2) in the heading, by inserting ''AND INFORMATION TECHNOLOGY'' after ''CYBER''.

(b) COMMON TERMS.—

(1) IN GENERAL.—Subsection (c)(2) of such section is amended by adding at the end the following new subparagraph:

''(C) Establishing and maintaining a list of terms and definitions with respect to commonly used terms relating to cyber matters to improve the coordination and cooperation among the military departments and among other depart-

ments and agencies of the Federal Government.''.

(2) ESTABLISHMENT.—In carrying out section 932(c)(2)(C) of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66), as added by paragraph (1), the Principal Cyber Advisor shall—

(A) establish the list of terms and definitions by not later than 270 days after the date of the enactment of this Act; and

(B) use as a basis for such list Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms (as amended through 31 January 2011).

(c) PILOT PROGRAM.—

(1) IN GENERAL.—The head of the entity established or designated under section 932(b)(5)(A) of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66), as added by subsection (a), shall carry out one or more pilot programs to demonstrate commercially available, cloud-based cyber training, exercise, and test environments (both unclassified and classified) that are available to meet the mission of the Department of Defense while providing the defense laboratories, the Na-

tional Guard, academia, and the private sector access to such training, exercise, and test environments.

(2) EVALUATION.—The pilot programs under paragraph (1) shall evaluate the costs and benefits with respect to the following matters:

(A) Persistent capability.

(B) Remote access.

(C) Capability to transfer information across classification levels.

(D) Reuse of environments.

(E) Routine integration of new technologies.

(F) Use of commercially available cloud-based solutions that are compliant with the Federal Risk and Authorization Management Program.

(G) Pay-per-use utility pricing model.

(H) Any other matters the head determines appropriate.

(3) ELIGIBLE ENTITIES.—The head shall select, using competitive procedures, defense laboratories and federally funded research and development centers to carry out pilot programs under paragraph (1).

(4) FOLLOW-ON ACTIVITIES.—Based on the information learned under the pilot programs under paragraph (1), the Secretary of Defense may carry out any of the following activities:

(A) Transition a pilot program to be carried out by the Secretary for operations, maintenance, and continued use by cyber organizations of the Department.

(B) Provide persistent year-round accessibility of the environment for continued training during non-exercise periods.

(C) Provide a ''certification quality'' environment for initial and recurring training of all cyber teams.

(D) Replicate the capability of a pilot program to provide similar high-end training and exercise opportunities for non-Department cyber professionals, including in coordination with the Secretary of Homeland Security.

(E) Sustain the research and development effort under a pilot program to continue updating network environments, targets and defended assets, and integration of new cyber tools.

(F) Sustain technology infusion under a pilot program to apply and evaluate advanced

concepts and solutions to problems that affect multiple mission spaces of the Department.

(G) Create a library of virtual cyber templates that are ready to be used on short notice without the capital expenditures that would otherwise be required.

○