

113<sup>TH</sup> CONGRESS  
2<sup>D</sup> 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.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

3       **SECTION 1. CYBER AND INFORMATION TECHNOLOGY**  
4                               **RANGES.**

5               (a) MANAGEMENT OF CYBER RANGES AND FACILI-  
6       TIES.—Subsection (b) of section 932 of the National De-  
7       fense Authorization Act for Fiscal Year 2014 (Public Law  
8       113–66) is amended—

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

1           “(3) LIST OF CYBER AND INFORMATION TECH-  
2           NOLOGY RANGES AND FACILITIES.—

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

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

13                  “(i) a ‘cyber range’, as defined by the  
14                  Principal Cyber Advisor pursuant to sub-  
15                  section (c)(2)(C); or

16                  “(ii) an ‘IT range’, as defined by the  
17                  Principal Cyber Advisor pursuant to such  
18                  subsection.

19          “(C) SUBMISSION.—Not later than one  
20          year after the date of the enactment of the Na-  
21          tional Defense Authorization Act for Fiscal  
22          Year 2015, the Principal Cyber Advisor shall  
23          submit to the congressional defense committees  
24          the list established under subparagraph (A).

1           “(4) MANAGEMENT OF SYSTEMS.—The Prin-  
2           cipal Cyber Advisor shall determine, on a case by  
3           case basis, whether a cyber and information tech-  
4           nology range and facility listed under paragraph  
5           (3)(A) should be centrally managed under paragraph  
6           (5) to increase efficiency, provide capability or ca-  
7           pacity to more elements of the Department of De-  
8           fense, or both.

9           “(5) COORDINATING ENTITY.—

10           “(A) ESTABLISHMENT.—Not later than  
11           270 days after the date of the enactment of the  
12           National Defense Authorization Act for Fiscal  
13           Year 2015, the Secretary of Defense shall es-  
14           tablish an entity, or designate an element of the  
15           Department of Defense, to coordinate cyber and  
16           information technology ranges and facilities  
17           that the Principal Cyber Advisor determines  
18           should be centrally managed under paragraph  
19           (4).

20           “(B) DUTIES.—With respect to the cyber  
21           and information technology ranges and facilities  
22           designated under paragraph (4), the head of  
23           the entity established or designated under sub-  
24           paragraph (A) shall be responsible for the fol-  
25           lowing:

1           “(i) Managing the cyber and informa-  
2           tion technology ranges and facilities, in-  
3           cluding coordinating the scheduling of  
4           ranges and facilities.

5           “(ii) Identifying and providing guid-  
6           ance to the Secretary with respect to op-  
7           portunities for integration among the cyber  
8           and information technology ranges and fa-  
9           cilities regarding testing, training, and de-  
10          veloping functions.

11          “(iii) Assisting the military depart-  
12          ments, the National Guard, and the ele-  
13          ments of the Department gain access to  
14          the cyber and information technology  
15          ranges and facilities.

16          “(C) REPORTS.—The head of the entity  
17          established or designated under subparagraph  
18          (A) shall submit to the congressional defense  
19          committees—

20                 “(i) an annual report on the opportu-  
21                 nities for cost reduction and improvements  
22                 to the integration and coordination of the  
23                 cyber and information technology ranges  
24                 and facilities; and

1                   “(ii) by not later than one year after  
2                   the date of the enactment of the National  
3                   Defense Authorization Act for Fiscal Year  
4                   2015, an initial report on the status, inte-  
5                   gration efforts, and usage of cyber and in-  
6                   formation technology ranges and facilities.

7                   “(6) CYBER AND INFORMATION TECHNOLOGY  
8                   RANGES AND FACILITIES DEFINED.—In this sub-  
9                   section, the term ‘cyber and information technology  
10                  ranges and facilities’ means cyber ranges, test facili-  
11                  ties, test beds, and other means of the Department  
12                  of Defense for testing, training, and developing soft-  
13                  ware, personnel, and tools for accommodating the  
14                  mission of the Department.”; and

15                  (2) in the heading, by inserting “AND INFOR-  
16                  MATION TECHNOLOGY” after “CYBER”.

17                  (b) COMMON TERMS.—

18                  (1) IN GENERAL.—Subsection (c)(2) of such  
19                  section is amended by adding at the end the fol-  
20                  lowing new subparagraph:

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

1           ments and agencies of the Federal Govern-  
2           ment.”.

3           (2) ESTABLISHMENT.—In carrying out section  
4           932(c)(2)(C) of the National Defense Authorization  
5           Act for Fiscal Year 2014 (Public Law 113–66), as  
6           added by paragraph (1), the Principal Cyber Advisor  
7           shall—

8                   (A) establish the list of terms and defini-  
9                   tions by not later than 270 days after the date  
10                  of the enactment of this Act; and

11                   (B) use as a basis for such list Joint Pub-  
12                  lication 1–02, Department of Defense Dic-  
13                  tionary of Military and Associated Terms (as  
14                  amended through 31 January 2011).

15           (c) PILOT PROGRAM.—

16                   (1) IN GENERAL.—The head of the entity es-  
17                  tablished or designated under section 932(b)(5)(A)  
18                  of the National Defense Authorization Act for Fiscal  
19                  Year 2014 (Public Law 113–66), as added by sub-  
20                  section (a), shall carry out one or more pilot pro-  
21                  grams to demonstrate commercially available, cloud-  
22                  based cyber training, exercise, and test environments  
23                  (both unclassified and classified) that are available  
24                  to meet the mission of the Department of Defense  
25                  while providing the defense laboratories, the Na-

1 tional Guard, academia, and the private sector ac-  
2 cess to such training, exercise, and test environ-  
3 ments.

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

7 (A) Persistent capability.

8 (B) Remote access.

9 (C) Capability to transfer information  
10 across classification levels.

11 (D) Reuse of environments.

12 (E) Routine integration of new tech-  
13 nologies.

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

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

19 (H) Any other matters the head deter-  
20 mines appropriate.

21 (3) ELIGIBLE ENTITIES.—The head shall select,  
22 using competitive procedures, defense laboratories  
23 and federally funded research and development cen-  
24 ters to carry out pilot programs under paragraph  
25 (1).

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

5                   (A) Transition a pilot program to be car-  
6                   ried out by the Secretary for operations, main-  
7                   tenance, and continued use by cyber organiza-  
8                   tions of the Department.

9                   (B) Provide persistent year-round accessi-  
10                  bility of the environment for continued training  
11                  during non-exercise periods.

12                  (C) Provide a “certification quality” envi-  
13                  ronment for initial and recurring training of all  
14                  cyber teams.

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

20                  (E) Sustain the research and development  
21                  effort under a pilot program to continue updat-  
22                  ing network environments, targets and defended  
23                  assets, and integration of new cyber tools.

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



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

3 (G) Create a library of virtual cyber tem-  
4 plates that are ready to be used on short notice  
5 without the capital expenditures that would oth-  
6 erwise be required.

○