HR 4500

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

Congress: 113 (2013–2015, Ended)
Chamber: House
Policy Area: Armed Forces and National Security
Introduced: Apr 28, 2014
Current Status: Referred to the Subcommittee on Intelligence, Emerging Threats & Capabilities.
Latest Action: Referred to the Subcommittee on Intelligence, Emerging Threats & Capabilities. (Jul 1, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/house-bill/4500

Sponsor

Name: Rep. Kilmer, Derek [D-WA-6]
Party: Democratic • **State:** WA • **Chamber:** House

Cosponsors (2 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Connolly, Gerald E. [D-VA-11]	D · VA		Apr 28, 2014
Rep. Tsongas, Niki [D-MA-3]	D · MA		Apr 28, 2014

Committee Activity

Committee	Chamber	Activity	Date
Armed Services Committee	House	Referred to	Jul 1, 2014

Subjects & Policy Tags

Policy Area:

Armed Forces and National Security

Related Bills

Bill	Relationship	Last Action
113 HR 3304	Related bill	**Dec 26, 2013:** Became Public Law No: 113-66.

Summary (as of Apr 28, 2014)

Amends the National Defense Authorization Act for Fiscal Year 2014 to require the Principal Cyber Advisor (PCA) (the principal advisor to the Secretary of Defense on military cyber forces) to establish and submit to Congress a comprehensive list of cyber and information technology ranges and facilities of the Department of Defense (DOD).

Defines "cyber and information technology ranges and facilities" as cyber ranges, test facilities, test beds, and other DOD means for testing, training, and developing software, personnel, and tools for accommodating DOD's mission.

Requires the PCA to determine, on a case-by-case basis, whether listed ranges and facilities should be managed centrally to increase efficiency, should provide capability or capacity to more DOD elements, or both.

Directs the Secretary to establish or designate an entity to coordinate such ranges and facilities that the PCA determines should be centrally managed. Requires the head of such entity to: (1) manage and identify opportunities for integration of such ranges and facilities; and (2) assist the military departments, the National Guard, and elements of DOD to gain access to such ranges and facilities.

Requires the PCA to establish and maintain a list of commonly used terms relating to cyber matters to improve the coordination and cooperation among the military departments and other federal agencies.
Directs the head of the coordination entity to carry out one or more pilot programs to demonstrate commercially available, cloud-based cyber training, exercise, and test environments that are accessible to defense laboratories, the National Guard, academia, and the private sector.

Actions Timeline

- **Jul 1, 2014:** Referred to the Subcommittee on Intelligence, Emerging Threats & Capabilities.
- **Apr 28, 2014:** Introduced in House
- **Apr 28, 2014:** Referred to the House Committee on Armed Services.