

**S. 1197F NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2014  
DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS  
TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT  
SUBTITLE D—CYBERSPACE-RELATED MATTERS**

**SEC. 932. AUTHORITIES, CAPABILITIES, AND OVERSIGHT OF THE UNITED STATES CYBER COMMAND.**

*Authorities, capabilities, and oversight of the United States Cyber Command (sec. 932)*

*The House bill contained a provision (sec. 932) that would require the Defense Science Board to conduct an independent assessment of the organization, missions, and authorities of U.S. Cyber Command (CYBERCOM).*

*The Senate committee-reported bill contained a similar provision (sec. 941) that would require the Secretary of Defense to delegate signals intelligence (SIGINT) collection authorities to CYBERCOM; provide CYBERCOM with the infrastructure and equipment to operate independently of the National Security Agency (NSA) to conduct operations in cyberspace; provide range capabilities to meet CYBERCOM's unique requirements for wartime offensive operations; designate an official within the Office of the Under Secretary of Defense for Policy to serve as the Secretary's principal advisor on offensive military cyber operations and to supervise the organization, manning, and equipping of such forces; and to establish appropriate training facilities for cyber personnel. In addition, the provision would express the sense of Congress that CYBERCOM personnel assigned to support offensive cyber missions should be funded and managed outside of the Military Intelligence Program (MIP) and Information Systems Security Program (ISSP).*

*The agreement includes the Senate committee-reported provision with an amendment. The amendment would assign to the principal advisor responsibility for the overall supervision of cyber activities in the Department, including oversight of policy and operational matters, resources, personnel, acquisition, and technology. In carrying out these responsibilities, the principal advisor shall create a full-time cross-functional team of subject-matter experts from the Office of the Secretary of Defense, the Joint Staff, the military departments, defense agencies, and combatant commands.*

*We stress that this construct of an interdepartmental team under the direction of the principal advisor for cyber is not intended to be merely a coordinating committee, but will provide strong leadership through a joint mechanism to achieve a common purpose and unity of effort in policy, planning, programming, and oversight to support a complex mission that spans the entire Department of Defense. We believe there are good models for effective cross-functional teams, such as the Joint Inter Agency Task Force-South, which successfully brings stakeholders together, including their specific authorities and capabilities, under a single organization. This team concept requires that members operate and think holistically, without regard to home institution loyalties, and receive training in team dynamics and conflict resolution.*

*With regard to cyber acquisitions, we note that there is an existing congressionally-mandated joint entity, the Cyber Investment Management Board, which is chaired by the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Policy, and the Vice Chairman of the Joint Chiefs of Staff. We believe such organizations should be leveraged to the extent possible in organizing this cross functional team.*

*The amendment does not include the requirement for the Secretary of Defense to delegate SIGINT authority to CYBERCOM, because the NSA Director has already made such a delegation. If a decision is made in the future to separate the positions of NSA Director and Commander of CYBERCOM, it would be appropriate for this delegation to come directly from the Secretary of Defense.*

*The amendment also does not include the sense of the Congress that CYBERCOM personnel assigned to support offensive missions should be funded and managed outside of the MIP and ISSP. We expect the Secretary of Defense to devise means to ensure that CYBERCOM personnel include non-career intelligence and cybersecurity officers and enlisted personnel with experience in combat arms.*

*We are aware that there are renewed deliberations about the potential of elevating U.S. Cyber Command from a sub-unified command to a full unified command. As noted by section 940 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112-239), we expect to be briefed and consulted on any such proposal at the time when the Secretary of Defense makes such a decision. As these policy discussions progress, we expect the Department to keep the Committees on Armed Services of the Senate and the House of Representatives informed, upon request, during the quarterly cyber operations briefings, particularly as they relate to the estimated costs and policy implications associated with making the U.S. Cyber Command a unified command.*

---

## **SEC. 932. AUTHORITIES, CAPABILITIES, AND OVERSIGHT OF THE UNITED STATES CYBER COMMAND.**

- (a) **PROVISION OF CERTAIN OPERATIONAL CAPABILITIES.**—The Secretary of Defense shall take such actions as the Secretary considers appropriate to provide the United States Cyber Command operational military units with infrastructure and equipment enabling access to the Internet and other types of networks to permit the United States Cyber Command to conduct the peacetime and wartime missions of the Command.
- (b) **CYBER RANGES.**—
- (1) **IN GENERAL.**—The Secretary shall review existing cyber ranges and adapt one or more such ranges, as necessary, to support training and exercises of cyber units that are assigned to execute offensive military cyber operations.
  - (2) **ELEMENTS.**—Each range adapted under paragraph (1) shall have the capability to support offensive military operations against targets that—
    - (A) have not been previously identified and prepared for attack; and

- (B) must be compromised or neutralized immediately without regard to whether the adversary can detect or attribute the attack.
- (c) **PRINCIPAL ADVISOR ON MILITARY CYBER FORCE MATTERS.**—
- (1) **DESIGNATION.**—The Secretary shall designate, from among the personnel of the Office of the Under Secretary of Defense for Policy, a Principal Cyber Advisor to act as the principal advisor to the Secretary on military cyber forces and activities. The Secretary may only designate an official under this paragraph if such official was appointed to the position in which such official serves by and with the advice and consent of the Senate.
- (2) **RESPONSIBILITIES.**—The Principal Cyber Advisor shall be responsible for the following:
- (A) Overall supervision of cyber activities related to offensive missions, defense of the United States, and defense of Department of Defense networks, including oversight of policy and operational considerations, resources, personnel, and acquisition and technology.
- (B) Such other matters relating to offensive military cyber forces as the Secretary shall specify for purposes of this subsection.
- (3) **CROSS-FUNCTIONAL TEAM.**—The Principal Cyber Advisor shall—
- (A) integrate the cyber expertise and perspectives of appropriate organizations within the Office of the Secretary of Defense, Joint Staff, military departments, Defense Agencies, and combatant commands, by establishing and maintaining a full-time cross-functional team of subject matter experts from those organizations; and
- (B) select team members, and designate a team leader, from among those personnel nominated by the heads of such organizations.
- (d) **TRAINING OF CYBER PERSONNEL.**—The Secretary shall establish and maintain training capabilities and facilities in the Armed Forces and, as the Secretary considers appropriate, at the United States Cyber Command, to support the needs of the Armed Forces and the United States Cyber Command for personnel who are assigned offensive and defensive cyber missions in the Department of Defense.