

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. 933. MISSION ANALYSIS FOR CYBER OPERATIONS OF DEPARTMENT OF DEFENSE.

Mission analysis for cyber operations of Department of Defense (sec. 933)

The House bill contained a provision (sec. 933) that would require the Secretary of Defense to conduct a mission analysis of Department of Defense cyber operations and to provide a report on the results of the mission analysis to the congressional defense committees. It would also require the Chief of the National Guard Bureau to provide an assessment of the role of the National Guard in supporting Department of Defense cyber missions.

The Senate committee-reported bill contained a similar provision (sec. 945) that would require the Secretary of Defense to develop a strategy for using the reserve components of the armed forces to support the cyber missions of U.S. Cyber Command, including in support of civil authorities, and to report to the congressional defense committees on this strategy within 180 days of the enactment of this Act.

The agreement merges these provisions with minor modifications to each.

SEC. 933. MISSION ANALYSIS FOR CYBER OPERATIONS OF DEPARTMENT OF DEFENSE.

- (a) **MISSION ANALYSIS REQUIRED.**—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall conduct a mission analysis of the cyber operations of the Department of Defense.
- (b) **ELEMENTS.**—The mission analysis under subsection (a) shall include the following:
- (1) The concept of operations and concept of employment for cyber operations forces.
 - (2) An assessment of the manpower needs for cyber operations forces, including military requirements for both active and reserve components and civilian requirements.
 - (3) An assessment of the mechanisms for improving recruitment, retention, and management of cyber operations forces, including through focused recruiting; educational, training, or certification scholarships; bonuses; or the use of short-term or virtual deployments without the need for permanent relocation.
 - (4) A description of the alignment of the organization and reporting chains of the Department, the military departments, and the combatant commands.
 - (5) An assessment of the current, as of the date of the analysis, and projected equipping needs of cyber operations forces.

- (6) An analysis of how the Secretary, for purposes of cyber operations, depends upon organizations outside of the Department, including industry and international partners.
- (7) Methods for ensuring resilience, mission assurance, and continuity of operations for cyber operations.
- (8) An evaluation of the potential roles of the reserve components in the concept of operations and concept of employment for cyber operations forces required under paragraph (1), including—
 - (A) in consultation with the Secretaries of the military departments and the Commander of the United States Cyber Command, an identification of the Department of Defense cyber mission requirements that could be discharged by members of the reserve components;
 - (B) in consultation with the Secretary of Homeland Security, consideration of ways to ensure that the Governors of the several States, through the Council of Governors, as appropriate, have an opportunity to provide the Secretary of Defense and the Secretary of Homeland Security an independent evaluation of State cyber capabilities, and State cyber needs that cannot be fulfilled through the private sector;
 - (C) an identification of the existing capabilities, facilities, and plans for cyber activities of the reserve components, including—
 - (i) an identification of current positions in the reserve components serving Department cyber missions;
 - (ii) an inventory of the existing cyber skills of reserve component personnel, including the skills of units and elements of the reserve components that are transitioning to cyber missions;
 - (iii) an inventory of the existing infrastructure of the reserve components that contributes to the cyber missions of the United States Cyber Command, including the infrastructure available to units and elements of the reserve components that are transitioning to such missions; and
 - (iv) an assessment of the manner in which the military departments plan to use the reserve components to meet total force resource requirements, and the effect of such plans on the potential ability of members of the reserve components to support the cyber missions of the United States Cyber Command;
 - (D) an assessment of whether the National Guard, when activated in a State status (either State Active Duty or in a duty status under title 32, United States Code) can operate under unique and useful authorities to support domestic cyber missions and requirements of the Department or the United States Cyber Command;
 - (E) an assessment of the appropriateness of hiring on a part-time basis non-dual status technicians who possess appropriate cyber security expertise for purposes of assisting the National Guard in protecting critical infrastructure and carrying out cyber missions;
 - (F) an assessment of the current and potential ability of the reserve components to—

- (i) attract and retain personnel with substantial, relevant cyber technical expertise who use those skills in the private sector;
 - (ii) organize such personnel into units at the State, regional, or national level under appropriate command and control arrangements for Department cyber missions;
 - (iii) meet and sustain the training standards of the United States Cyber Command; and
 - (iv) establish and manage career paths for such personnel;
- (G) a determination of how the reserve components could contribute to total force solutions to cyber operations requirements of the United States Cyber Command; and
- (H) development of an estimate of the personnel, infrastructure, and training required, and the costs that would be incurred, in connection with implementing a strategy for integrating the reserve components into the total force for support of the cyber missions of the Department and United States Cyber Command, including by taking into account the potential savings under the strategy through use of personnel referred to in subparagraph (C)(i), provided that for specific cyber units that exist or are transitioning to a cyber mission, the estimate shall examine whether there are misalignments in existing plans between unit missions and facility readiness to support such missions.
- (c) **LIMITATIONS ON CERTAIN ACTIONS.—**
- (1) **REDUCTION IN PERSONNEL OF AIR NATIONAL GUARD CYBER UNITS.—** No reduction in personnel of a cyber unit of the Air National Guard of the United States may be implemented or carried out in fiscal year 2014 before the submittal of the report required by subsection (d).
 - (2) **REDUCTION IN PERSONNEL AND CAPACITY OF AIR NATIONAL GUARD RED TEAMS.—** No reduction in the personnel or capacity of a Red Team of the Air National Guard of the United States may be implemented or carried out unless the report required by subsection (d) includes a certification that the personnel or capacity to be reduced is directly related to Red Team capabilities that are no longer required.
- (d) **REPORT REQUIRED.—** Not later than 30 days after the completion of the mission analysis under subsection (a), the Secretary shall submit to the congressional defense committees a report containing—
- (1) the results of the mission analysis;
 - (2) recommendations for improving or changing the roles, organization, missions, concept of operations, or authorities related to the cyber operations of the Department; and
 - (3) any other matters concerning the mission analysis that the Secretary considers appropriate.
- (e) **NATIONAL GUARD ASSESSMENT.—** Not later than 30 days after the date on which the Secretary submits the report required under subsection (d), the Chief of the National Guard Bureau shall submit to the congressional defense committees an assessment of the role of the National Guard in supporting the cyber operations mission of the Department of Defense as such mission is described in such report.

(f) FORM.—The report under subsection (d) shall be submitted in unclassified form, but may include a classified annex.