National Guard Bureau

Cyber Mission Analysis Assessment

Chief of the National Guard Bureau Assessment of the Department of Defense's Mission Analysis for Cyber Operations

Submitted in compliance with Section 933(e) of Public Law 113-66,

the National Defense Authorization Act for Fiscal Year 2014

Generated on 29 September 2014

Table of Contents

I. Executive Summary

This report fulfills the requirement contained in the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2014, Section 933(e) "National Guard Assessment." The results of the National Guard's assessment reflect the Chief of the National Guard Bureau's (CNGB) view for successfully integrating the National Guard into the Department of Defense's (DoD) Cyber Mission Force (CMF) and across all Cyber missions to create a Whole of Government and Whole of Nation approach to securing U.S. cyberspace.

The CNGB appreciates the opportunity to provide the "National Guard Assessment" required by Section 933(e) of the NDAA. The CNGB commends the Office of the Deputy Assistant Secretary of Defense for Cyber Policy for its openness, transparency, and inclusiveness in developing the report. Its collaborative approach resulted in the most comprehensive study to date of Reserve Component integration into the Cyber mission. To complete this independent assessment of the Secretary of Defense's *Mission Analysis for Cyber Operations of the Department of Defense* report, the National Guard Bureau (NGB) consulted with key stakeholders to ensure an equally transparent review. The NGB solicited input from the Director of the Army National Guard (DARNG), Army Cyber Command (ARCYBER), the Director of the Air National Guard (DANG), Air Force Cyber Command (AFCYBER), United States Cyber Command (USCYBERCOM), the National Guard Cyber General Officer Advisory Council, The Adjutants General (TAG) of the States and Territories, the Council of Governors, and the Office of the Secretary of Defense. The input received in these engagements is reflected throughout this report.

Based on the National Guard's assessment of the Secretary of Defense's *Mission Analysis for Cyber Operations of the Department of Defense* report, the CNGB highlighted six specific areas of the report:

1. The CNGB supports the Army's proposed plan to field one full-time Army National Guard (ARNG) CPT and ten part-time ARNG CPTs.

2. The CNGB supports the Services' plans to develop and integrate cyberspace forces into their respective Reserve Components as part of the DoD's Total Force approach to cyberspace. Specifically, the CNGB supports the U.S. Air Force's plan to staff two CMF Cyber Protection Teams (CPT) and the Cyber Operations portion of one National Mission Team (NMT) as part of the Air Force's allocation of the CMF.

3. The CNGB supports training National Guard cyberspace personnel to DoD joint training standards as prescribed by the Secretary of Defense's approved guidance.

4. The CNGB supports the Governors' ability to employ National Guard cyberspace-trained personnel in State Active Duty (SAD) and Title 32 status, as described in the Council of Governors letter dated August 15, 2014, in compliance with Federal and State law, to provide State-initiated and State-directed cyberspace support to civil authorities. This

would be in roles of expertise, such as to coordinate, train, advise, and assist (C/TAA).

5. The CNGB acknowledges the need for reorganization and realignment of the current Red Team capabilities in the Air National Guard (ANG) to create a sound program and enduring construct.

6. The Services require additional resources to execute their plans to build and train cyberspace forces in the Reserve Component to support the DoD's Total Force approach to cyberspace.

II. National Guard Assessment

The National Guard is a natural fit for developing DoD cyberspace capabilities that best leverage Federal and State authorities in defending our Nation against evolving cyberspace threats. The National Guard stands ready to support the DoD's Total Force approach to addressing CMF and emerging cyberspace requirements with talented, professional, highly trained National Guard Soldiers and Airmen. The National Guard recommends developing National Guard cyberspace capabilities through planned efforts and highlights the challenges in programmed funding, training, and formalizing National Guard cyberspace requirements.

Programmed Funding: The Army plan is to establish 10 part-time ARNG CPTs starting in FY 2017. The CNGB welcomes the ability to work with the Army to develop this mission. The Army's proposal must be completed in the FY 2017 Program and Budget Review cycle, which is not projected to start until October 2014.

Alternatively, the Air Force plans to include the ANG CPTs as part of its delegated CMF requirement for FY 2016. The Air Force submitted a funding request for CPTs in the FY 2016 Program and Budget Review cycle that has not yet been approved. To mitigate future funding issues, the CNGB requests assistance in programming support.

The CNGB has directed the ANG and ARNG to continue to engage with their Service counterparts to build a Future Years Defense Program that includes resources essential to organizing, training, equipping, and staffing National Guard cyberspace forces. The National Guard continues to work with the Army and Air Force to secure resources for these critical capabilities during the FY 2017-2021 POM development cycle.

Training: When the USCYBERCOM CMF construct was established, DoD designed training requirements and training slots to support approximately 6,200 cyberspace personnel. However, USCYBERCOM's CMF initial plan did not account for training approximately 2,000 Reserve Component personnel now included in the Services' proposed Reserve Component integration plan. Therefore, the CNGB request funding to train National Guard cyberspace forces to DoD's joint training standards. The Services must identify training slots concurrently and proportionally for the National Guard cyberspace forces.

Capabilities Based Assessment (CBA). To capture requirements appropriate for the National Guard formally, NGB will conduct a CBA of National Guard cyberspace forces as directed by Joint Requirements Oversight Memorandum (JROCM) 073-14. This JROCM captured the Council's near-term priorities for development of requirements documents and supporting analyses. This National Guard Cyber CBA will leverage the work done to complete this report, as well as the Cyber CBAs already completed by the Army and Air Force. It will also build upon the ANG and ARNG's work to develop National Guard Cyber courses of action. Although these efforts are meant to examine issues that are unique to the National Guard, NGB does not intend to duplicate the Services' efforts.

National Guard Assessment of DoD Findings

The CNGB understands that DoD considered many factors to determine how to best integrate National Guard cyberspace forces into in the DoD's Total Force approach to address CMF and emerging cyberspace requirements. Those factors included whether the position is military essential, peacetime and wartime demands, deployment frequency and duration, speed of response, unit readiness for specific mission sets, and costs. The examination of these factors and discussions with key stakeholders led to six DoD findings and five key recommended ways forward. This section assesses the DoD's findings and key recommended ways forward independently because its report lists them separately.

DoD Finding: The Reserve and Guard can offer load-sharing and surge capacity for the CMF

National Guard Assessment: The CNGB concurs with the DoD's finding that Reserve and National Guard cyberspace forces can offer load-sharing and surge capacity for the CMF. As the ARNG and ANG stand up their cyberspace forces with their respective Service, the CNGB has directed a build-assess-build approach to ensure the National Guard is strengthening critical cyberspace capabilities and capacity with an emphasis on meeting the requirements of a Whole of Government response. As stated in the DoD's report, it is essential that DoD ensures that all cyberspace personnel, both Active and Reserve Components, are trained to the same joint standards.

ARNG: The NGB understands the 11 ARNG CPTs are above the Army's current CMF requirement. The NGB agrees that leveraging ARNG cyber personnel to expand the Army's cyberspace capabilities is a starting point to using ARNG Cyber Forces.

ANG: The CNGB concurs with the Air Force's plan to staff two full-time CPTs by leveraging 12 ANG squadrons rotating between activation and dwell status, with a 1:5 dwell posture. Additionally, the CNGB agrees with the Air Force plan to staff the Cyber Operations portion of one CMF NMT by leveraging three ANG squadrons on a rotational basis. The ANG fills the CMF CPT and NMT requirement with approximately 600 trained cyberspace professionals, which is a mix of full-time and traditional drill status Airmen.

Additionally, the ANG has established five Cyber Intelligence, Surveillance, and Reconnaissance (ISR) units with a total of 435 personnel in five States that perform Digital Network Intelligence (DNI) support to 25th Air Force, formally known as the Air Force Intelligence and Surveillance and Reconnaissance Agency. DNI is a long-term analysis to evaluate attempts to penetrate, exploit, or disrupt military networks, as well as assess adversary and enemy cyberspace capabilities and activity patterns. These units are aligned under Air Combat Command's 25th Air Force, which is responsible for all Air Force ISR forces. The ANG Cyber Operations and ISR squadrons are listed in Annex 1.

DoD Finding: The National Guard can offer support to "Whole of Government" and "Whole of Nation" cyber requirements.

National Guard Assessment: CNGB concurs with the DoD's finding that in addition to providing capability and capacity for the CMF, National Guard cyberspace forces are uniquely postured to support critical Whole of Government and Whole of Nation cyberspace requirements.

The CNGB remains committed to the *2013 State-Federal Consultative Process of Programming and Budgetary Proposals Affecting the National Guard,* commonly known as "the Consultative Process." The Consultative Process provides ways for the Governors, through the Council of Governors and the CNGB, to provide States' requirements for consideration in DoD's planning, programming, budgeting, and execution process.

DoD Finding: National Guard personnel, under State command and control, can support State missions.

National Guard Assessment: The CNGB concurs with the DoD's finding that the National Guard is well-positioned to offer its expertise and support to State missions under State command and control. The DoD correctly asserts that U.S. Code provisions permit National Guard forces to support domestic missions related to supporting law enforcement, homeland operations, and Defense Support of Civil Authorities -related cyberspace activities. National Guard personnel could be used to perform cyberspace missions in Title 10 or Title 32 status.

Additionally, State National Guard personnel could be used in SAD status to perform related State cyberspace missions in support of civil authorities if authorized by State and Federal law. The CNGB recognizes and strongly supports the Governors' authority to employ National Guard personnel independently in SAD status possibly to support C/TAA functions in compliance with Federal and State law. While under State command and control, National Guard personnel operate at the direction, and under the command, of the Governor concerned. It is important to note that use of National Guard personnel in a Title 32 status requires approval of the Secretary of Defense to perform purely

operational missions. These unique dual-constitutional authorities allow the National Guard to serve as a bridge across State and Federal government boundaries.

DoD Finding: Greater clarity is needed regarding Command and Control versus Coordination and Communication.

National Guard Assessment: The CNGB concurs with the DoD's finding that additional work is required to define command and control clearly, along with chains of communication and coordination for National Guard cyberspace forces when not operating in Title 10 status.

The inclusion of approximately 2,000 Reserve Component cyberspace forces in the CMF will force key stakeholders to define command and control clearly, along with communication and coordination policies for National Guard cyberspace forces not operating in Title 10 status respectful of the inherent authorities of the Governors.

The role of the CNGB as a channel of communication between the States and the DoD in domestic operations is well documented. The CNGB recommends examining the role of the Dual-Status Commander (DSC) to determine applicability to both cyberspace operations and domestic operations with a cyberspace component. Federal law—Title 10 U.S.C., Section 12304—and DoD policy—Joint Action Plan for Developing Unity of Effort—prescribe the DSC as the usual and customary means of ensuring unity of effort between Title 10 and Title 32 or SAD forces when responding to a domestic incident.

In addition, greater clarity is required regarding coordination and communication versus command and control within domestic cyberspace operations. As mentioned in DoD's report, the DoD selected its Information Networks' (DoDIN) Direct-Support C2 model as the framework to achieve unified action across the full scope of its cyberspace operations.

To ensure unity of effort and unified action down to the National Guard Joint Force Headquarters-State (JFHQ-State) and among the Federal, State, and local mission partners, NGB supports further evaluation of the Direct-Support C2 model. This evaluation would define the lines of communication and coordination for the cyberspace operational domain between the National Guard, the supporting emergency operations center, the National Guard JFHQs-State, and the JFHQ-DoDIN.

DoD Finding: Additional flexibility in hiring highly-technical civilian cyber professionals likely is required.

National Guard Assessment: The CNGB concurs with the DoD's finding that additional flexibility and authorities are likely required to entice individuals from outside of Government to provide subject-matter expert support to USCYBERCOM and other military components.

The CNGB recommends the DoD consider different Service commitments in critical need cyberspace positions. For example, instead of a four or six-year active duty commitment, consideration should be given to ten-year commitments (two for active duty and eight for National Guard) or other options to season on active duty and then serve the National Guard.

DoD Finding: Training and equipping the cyberspace Total Force may require additional capability.

National Guard Assessment: The CNGB concurs with the Department's finding that training and equipping the cyberspace Total Force likely will require additional capabilities. As discussed in the DoD's report, USCYBERCOM has heavily relied upon Intelligence Community (IC) training and platforms to conduct operations. The DoD made a number of strategic decisions to invest in training and infrastructure to support the CMF.

For example, the USCYBERCOM CMF training requirements, training slots, and support infrastructure discussed earlier were envisioned to support approximately 6,200 cyberspace personnel. However, USCYBERCOM's CMF initial plan did not account for training approximately 2,000 Reserve Component personnel now included in the Services' proposed Reserve Component integration plan. Therefore, the CNGB asserts that Reserve Component forces should receive a concurrent and proportional allocation of training dollars and student slots to integrate these personnel into the DoD's mission-appropriate, cyberspace-related training programs.

The CNGB affirms training received from other sources, such as the ARNG Professional Education Center (PEC) and the ANG Regional Training Institute, must be considered when building the appropriate equivalency training packages to conform to the DoD joint training standard.

National Guard Assessment of DoD's Five Key Recommended Ways Forward

DoD Recommended Way Forward: National Guard personnel may provide a C/TAA support roles when directed by their Governor or The Adjutant General if in SAD status or, if authorized by DoD, in Title 32 status.

National Guard Assessment: The NGB supports the Governors' ability to employ National Guard personnel in SAD status possibly to perform C/TAA functions in compliance with Federal and State law. The NGB agrees that while under State command and control—in SAD or Title 32 status— National Guard personnel operate at the direction, and under the command, of the Governor; however, the use of National Guard personnel in a Title 32 status to perform purely operational missions requires the Secretary of Defense's approval.

DoD Recommended Way Forward: The Services' proposed plan to integrate approximately 2,000 Reserve Component personnel into the cyberspace force structure adequately addresses the opportunity for surge support and additional Service CPT support in the near-term.

National Guard Assessment: As stated earlier, the CNGB supports the Air Force's plan to staff two CMF CPTs with personnel from twelve ANG squadrons. Additionally, the CNGB supports the Air Force's plan to fill a portion of one CMF NMT with personnel from three ANG squadrons.

Additionally, the CNGB supports the Army's plan to field one-full-time ARNG CPT and ten part-time ARNG CPTs. The NGB understands the 11 ARNG CPTs are not included in the Army's current CMF requirement, but it has a long-term plan to align these forces properly to DoD cyberspace requirements.

DoD Recommended Way Forward: Cyberspace forces require consideration of a persistent training environment.

National Guard Assessment: NGB strongly agrees the need for a persistent training environment to provide adequate support for all Service and Reserve Component training activities. This capability is long overdue and essential to building the Total Force in Cyber.

DoD Recommended Way Forward: Because there is no command and control over National Guard cyberspace forces in a Title 32 or SAD status, policies, and processes must be clarified to ensure unity of effort by DoD forces and State National Guard forces.

National Guard Assessment: The DoD assertion that "...there is no command and control over National Guard cyberspace forces..." is incorrect. While there is no Federal command and control of National Guard forces under SAD and Title 32 status, these forces are under the command and control of the Governor and his or her assigned officers. In addition, the DSC is designed specifically to provide unity of effort between the Active Component and the NG forces when both are employed. Use of the DSC for Cyber Operations should be examined. We understand there are concerns regarding current legislation and policies covering cyberspace operations. Any modifications to legislation or policy must improve the National Guard's ability to team with the Federal, State, local, tribal, and territorial (SLTT) capabilities and private-sector partners in all areas of domestic and cyberspace operations. The CNGB assesses that the authorities used to perform domestic operations are sufficient to include cyberspace operations.

DoD Recommended Way Forward: The Military Departments/Services may require additional flexibility in civilian hiring authorities.

> **National Guard Assessment:** The CNGB concurs that the military may require additional flexibility in civilian hiring authorities.

National Guard Assessment of Red Teams

With respect to Section 933(c)(2) of the NDAA, the Secretary of Defense's report did not specifically address Red Team capabilities beyond their integral part in all 68 CPTs within the CMF structure. The existing Red Team capability in the ANG has been a valuable addition to the DoD's cyberspace defense. To this end, USCYBERCOM's CMF established the requirement for Red Team capability in the CPT. This requirement results in a more than a five-fold increase in Red Team capacity across the DoD.

Specifically, the USCYBERCOM CMF 68 CPTs with embedded Red Team elements acknowledges the requirement for Red Teams. The 68 CPTs include 2 ANG CPTs supported by 12 ANG squadrons. As a result, Red Team personnel and the ANG's capacity will increase significantly in size and scope across the Nation. ANG squadrons supporting CPTs are available to support additional activities, including the Red Team, when not activated on CPT missions. Red Team capability and capacity will no longer reside in only one ANG squadron, but in a total of 13, which would more than double ANG Red Team capability.

To meet future mission tasking and stringent fiscal constraints, the ANG requests the ability to align the existing ANG Red Team force structure to a template that is regular and customary, to the principles of the Air Force and ANG. The CNGB recognizes the talents, skills, and training required to develop Red Team capabilities and capacity. Concurrently, the ANG is evaluating additional options to use and retain the skills of current Red Team personnel affected by changes in unit alignment. These options are intended to leverage the Red Team capability and the investment in these valuable Airmen.

The ANG is also considering the future defensive cyberspace capabilities distributed across as many Federal Emergency Management Area regions as much as practical. This optimizes the application of this limited resource and use of developed relationships in defense of Federal, State, and local networks, and critical infrastructure. The ANG has addressed this holistically because it plans to expand the cyberspace capability aggressively.

III. Conclusion

Current and emerging cyber threats require a Whole of Government and Whole of Nation approach, which integrates the responses of SLTT governments and private industry. The National Guard has unique constitutional and statutory authorities for directly supporting SLTT governments and defense-critical infrastructure. This allows the National Guard to build relationships that span organizations and sectors, such as the States, State law enforcement, the DoD, the Department of Homeland Security, and the Federal Bureau of Investigation.

The NGB stands ready to support the DoD's CMF with talented, professional, highly trained National Guard Soldiers and Airmen. The National Guard recognizes and strongly supports the Governors' authority to employ National Guard personnel independently in SAD status possibly to perform C/TAA functions in compliance with Federal and State law. In addition, CNGB strongly supports the need for a persistent training environment that allows the Services and Reserve components to develop, refine, exercises, and validate critical cyberspace skills and abilities essential to building the DoD's Cyber Total Force.

The CNGB appreciates the teamwork, transparency, and leadership all stakeholders exhibited during the mission analysis and preparation of this report. The National Guard understands that while each organization has its unique equities, the entire team is working for the good of the Nation. The National Guard stands ready as a full partner in the Total Force. The CNGB will continue to support this process to ensure that the Nation has a capable, flexible, balanced, and cost-effective cyberspace force.

In conclusion, this report reflects the CNGB's view for successfully integrating the National Guard into the DoD's CMF and across all cyberspace missions to provide freedom of action in cyberspace.

Annex 1: National Guard Cyber Force

Air National Guard Cyber Forces

ANG Cyber Operations Squadrons:

- *102nd Network Warfare Squadron (Rhode Island).* Mission: Air Force Computer Emergency Response Team support and forensics.
- *229th Information Operations Squadron (Vermont).* Mission: Cyber training for the Air Force and Army.
- *166th Network Warfare Squadron (Delaware)* and *175th Network Warfare Squadron (Maryland).* Mission: Force Application.
- *273rd Information Operation Squadron (Texas).* Mission: 24th Air Force support.
- *262nd Network Warfare Squadron (Washington).* Mission: Interceptor/hunter, Industrial Control System/Supervisory Control and Data Acquisition missions and AFCYBER support.
- *143rd Information Operations Squadron (Washington)* and *261st Network Warfare Squadron (California).* Mission: Interceptor/hunter missions.
- *177th Information Aggressor Squadron (Kansas).* Mission: Red teaming assessments.

ANG Cyber ISR Squadrons:

- *124th Intelligence Squadron (Ohio). Mission: DNI*
- *218th Intelligence Group (Tennessee). Mission: DNI*
- *223rd Intelligence Flight (Kentucky). Mission: DNI*
- *256th Intelligence Squadron (Washington). Mission: DNI*
- *TBD Intelligence Squadron (Maryland). Mission: DNI*

Army National Guard Cyber Forces

Current ARNG Cyber Forces:

- Virginia DPU Manassas, Virginia
- One active duty ARNG CPT
- Computer Network Defense-Teams

Future ARNG Cyber Force:

- 10 part-time ARNG CPTs

Annex 2: Acronym list

AFCYBER – Air Force Cyber Command
AOS – Area of Support
ARCYBER – Army Cyber Command
ARNG – Army National Guard
ANG – Air National Guard
C2 – Command and Control
C/TAA – Coordinate, Train, Advise, and Assist
CBA – Capabilities Based Assessment
CMF – Cyber Mission Force
CND-T – Computer Network Defense Teams
CPT – Cyber Protection Team
CS – Civil Support
DANG – Director of the Air National Guard
DARNG – Director of the Army National Guard
DNI – Digital Network Intelligence
DoD – Department of Defense
DoDIN – Department of Defense Information Networks
DSC – Dual-Status Commander
DSCA – Defense Support of Civil Authorities
FY – Fiscal Year
HLD – Homeland Defense
ISR – Intelligence, Surveillance, and Reconnaissance
JFHQ-DOIM – Joint Force Headquarters–Directorates of Information Management
JFHQ-State – Joint Force Headquarters–State
JIE – Joint Information Environment
JROCM – Joint Requirements Oversight Memorandum
NDAA – National Defense Authorization Act
NGB – National Guard Bureau
NGB-JCC – National Guard Bureau Joint Cyber Cell
NMT – National Mission Team
PEC – Professional Education Center
SAD – State Active Duty
SLTT – Federal, State, Local, Tribal, and Territorial
TAG – The Adjutant General
USCYBERCOM – United States Cyber Command

Annex 3: Section 933 Reporting Requirement

Reporting Requirement
Section 933 of H.R. 3304, the National Defense Authorization Act for Fiscal Year 2014
(Public Law 113-66)

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.