

OFFICE OF THE SECRETARY OF DEFENSE RESERVE FORCES POLICY BOARD

5113 Leesburg Pike, Suite 601 FALLS CHURCH, VA 22041

AUG 19 2014

INFO MEMO

DepSec Action

et). Chairman, Reserve Forces Policy Board

FROM: MajGen Arnold L. Punaro, VSM(IV) (Ret), Chairman SUBJECT: Bar SUBJECT: Report of the Reserve Forces Policy Board on Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force

- The RFPB is a federal advisory committee established to provide you with independent advice and recommendations on strategies, policies and practices designed to improve and enhance the capabilities, efficiency, and effectiveness of the Reserve Components.
- On June 5, 2013, in response to the growing national dependence on computer network technologies and increasing threats to our national security emanating from the cyber domain, the Reserve Forces Policy Board established a Task Group to examine the Department's current path in developing its organizations, policies, doctrine and practices for conducting defensive and offensive cyber operations. The Task Group was further directed to comment on force mix between active, reserve, and civilian personnel and Reserve Component organizations needed to meet the DoD strategy. The RFPB met on June 4, 2014 and voted to make four recommendations.
- The recommendations are listed below with each expanded upon in the attached report:

Recommendation #1 – Include Reserve Components in Cyber Mission Force requirements in order to leverage RC reduced cost, civilian/AC acquired skill/ experience, continuity and longevity.

Recommendation #2 – As part of a Total Force solution, re-evaluate the composition, size and force mix of the planned Cyber Mission Force by FY 2017, and refine as needed based on changing threats, team effectiveness, capability, required capacity and cost.

Recommendation #3 - The Department of Defense should study, and then assign executive responsibility to a single Service for the full range of joint cyber training.

Recommendation #4 - Recruit highly skilled members via a professional accessions and retention program to fill both AC and RC requirements within the Cyber Mission Force.

As required by the Federal Advisory Committee Act, these recommendations were deliberated and approved in an open, public session. The Report, including briefing slides presented to and approved by the Board, is at TAB A and has been posted to the RFPB public website. The basic overview of the RFPB is submitted as TAB B.

COORDINATION: NONE

Attachments(s):

As stated

Prepared by: Maj Gen James N. Stewart, 703-681-0060

APPROVED REPORT

RESERVE FORCES POLICY BOARD

Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force

Report to the Secretary of Defense

The estimated cost of this report or study for the Department of Defense is approximately \$37,000 in Fiscal Years 2013 - 2014. This includes \$9,550 in expenses and \$27,000 in DoD labor.

Generated on 2014Jun18 RefID: 7-A188429

August 18, 2014

RFPB Report FY14-03



...US Cyber Command, with the Services and other partners, are doing something that our military has never done before. We are putting in place foundational systems and processes... for organizing, training, equipping, and operating our military cyber capabilities to meet cyber threats...Our legacy forces lack the training and the readiness to confront advanced threats in cyberspace.¹



- Gen Keith B. Alexander

¹ U.S. Congress. Senate. Committee on Armed Services, Statement of General Keith B. Alexander, Commander United States Cyber Command: Testimony before the Committee on Armed Services. 113th Cong., 2nd sess., February 27, 2014

Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force

TABLE OF CONTENTS

Executive Summary	3
Task	5
Approach	6
Finding and Observations	7
Reserve Component Cyber Organization (Finding 7)	15
Recommendations	16
1. RC Should Be Included in Cyber Mission Force Requirements	16
2. Cyber Mission Force Requirements Should Be Reassessed by FY 2017	21
3. Assign Executive Responsibility for Cyber Schools	23
4. Recruit Skilled Personnel through A Professional Accessions Program	24
Conclusion	25
Bibliography	26
Appendix A – Slides Approved by RFPB on 5 June 2014	29
Appendix B – Slides on CYBER GUARD 13 ANG Participant Civilian Employers	48

EXECUTIVE SUMMARY

At the 5 June 2013 Reserve Forces Policy Board quarterly meeting, a Task Group led by Sergio Pecori was formalized to examine Department of Defense's cyber approach and to provide an objective assessment of the Department's current path in developing its organizations, policies, doctrine and practices for conducting defensive and offensive cyber operations. The Task Group was further directed to comment on force mix between active, reserve, and civilian personnel and Reserve Component organization needed to meet the DoD strategy. The purpose of this report is to provide the Secretary of Defense with analysis and observations, in accordance with the Board's Charter under Title 10, United States Code, Section 10301, to improve and enhance the capabilities, efficiency, and effectiveness of the Reserve Components. The Board's recommendations are made in what we recognize is a dynamic and changing operational and planning environment. It should be noted that the Board concluded in its first finding that USCYBERCOM, Service cyber organizations and the Joint Staff are making exceptional progress in sourcing manpower, developing training programs and enabling employment guidance needed to field a fully operational Cyber Mission Force.

The Reserve Components Should Be Included in Cyber Mission Force Requirements

Initial plans to field the Cyber Mission Force did not embrace Reserve Component integration. Including Reserve Components in Cyber Mission Force requirements would take advantage of reduced cost, civilian acquired skills, experience, continuity and longevity. Several Reserve Components have since proposed allocating manpower and training to create Cyber Mission Force teams; however, most are not allocated to USCYBERCOM, Combatant Commanders, or Service Cyber organizations. The Secretary of Defense should direct a fully integrated Total Force. Optimally, Active Component and Reserve Component cyber units should be co-located whenever possible to leverage reduced cost efficiencies of shared equipment and infrastructure and to provide operational synergies. In addition, USCYBERCOM and the Services should also review the need for cyber expertise outside of the Cyber Mission Force construct that meets niche capabilities that take advantage of the full range of civilian acquired skills within the Reserve Components.

Cyber Mission Force Requirements Should Be Reassessed by FY 2017

As part of a Total Force solution leveraging Reserve Component reduced cost, civilian acquired skills, experience and continuity, the Cyber Mission Force should include the Reserve Components, which is not currently the plan. As the cyber threat changes and more data is collected on team effectiveness, capability and capacity, changes to cyber team composition, number and distribution will be needed. A robust development of performance based metrics

should be developed to quantify these types of future force decisions and provide a sound basis for return on investment and alternative resourcing decisions, including AC/RC force mix.

Executive Responsibility for Cyber Schools Should Be Assigned

In order to achieve long term cost efficiencies, the Department should study and assign executive responsibilities for common cyber schools to a single service. By studying course content and re-aligning their structure, overlap with advanced courses can be reduced and Service redundancy eliminated.

Skilled Personnel Should be Recruited through a Professional Accessions Program

Adopting a professional accessions program, similar to those used for medical profession officers and other highly trained and specialized skills has high potential as a paradigm shifting approach towards acquiring exceptionally qualified recruits. Utilizing USCYBERCOM's Individual Training Evaluation Board process to recognize existing skills would also provide resource savings, reduce training pipeline stress, and enhance growth of the Cyber Mission Force.

TASK

On April 29, 2013 Major General (Ret) Arnold Punaro, the Reserve Forces Policy Board Chairman, in light of the Secretary of Defense prioritizing cyber as a critical capability, directed the establishment of an RFPB Cyber Policy Task Group. The purpose of the Task Group was to address the policy question of to what extent capabilities in the Department's cyber approach should be established in the reserve component. As described in 10 USC 10301, this task group was chartered to examine cyber issues in order to improve and enhance the capabilities, efficiency, and effectiveness of the Reserve Components. Additionally, it complied with the requirements under Title 5, Appendix 2 (Federal Advisory Committee Act); the Code of Federal Regulations, Title 41, Part 102-3 (Federal Advisory Committee Management); and DoD Directive 5104.04 (Department of Defense Federal Advisory Committee Management Program). To address this issue, the Task Group, over a period of nine months, conducted interviews and received briefings from service cyber organizations, Department of Defense policy makers, Cyber subject matter experts, and reviewed existing doctrine, directives and publicly available information. This detailed analysis allowed the group to obtain sufficient evidence to provide a reasonable basis for findings and recommendations needed to answer the following questions:

- 1. What is DoD's current path in developing its organizations, policies, doctrine and practices for the conduct of both defensive and offensive cyber operations?
- 2. Is the Department staffing this new mission with the proper mix of active, reserve, and civilian personnel?
- 3. How should the Reserve Component be organized, manned, equipped, and used to meet the expectations outlined in the July 2011 DoD *Strategy for Operating in Cyberspace*?

Since the tasking letter and terms of reference for this study specifically identify assessing offensive and defensive cyber operations, the Task Group focused on assessing the building of Cyber Mission Forces (CMFs), with only a limited look at established legacy cyber missions, such as Information Assurance, Network Operations, Signal Intelligence, Combat Communications and Electronic Warfare. The Task Group was not able to quantify an optimal mix of active, reserve and civilian personnel or fully address organizational integration of RC Cyber Mission Forces due to its early phase of development. When the recommendations of this group were approved, only 1.5% of Cyber Mission Force teams had reached Full Operational Capability (FOC), with an additional 20% at Initial Operational Capability (IOC). These were all Active component (AC) teams. For the purpose of this report, the Reserve Component (RC) includes both National Guard and Reserve forces. Specifically, the Reserve Component

encompasses the Army National Guard, Army Reserve, Navy Reserve, Marine Corps Reserve, Air National Guard, Air Force Reserve and Coast Guard Reserve.

APPROACH

This report's primary purpose is to provide the Secretary of Defense with thoughtful analysis, observations, and recommendations in response to questions posed by the Chairman of the Reserve Forces Policy Board (RFPB) following the Board's statutory mandate. These responses are intended, in accordance with the RFPB's Charter, to improve and enhance the capabilities, efficiency, and effectiveness of the Reserve Components.

A temporary five member Task Group, reflecting the balanced representation of the Board, was formalized on 5 June 2013. The Task Group was chaired by Sergio Pecori. The mission of the Task Group was to study the questions raised by the Chairman, gather information, conduct research, analyze relevant facts, and develop for Board consideration a report or reports of advice and recommendations for the Secretary of Defense. A Work Plan was approved by the Board on September 5, 2013. The Task Group conducted eight meetings, met, interviewed or contacted more than 71 officials from the Department of Defense and relevant agencies, Department of Homeland Security and representatives from think tanks and private industry. Updates were presented on observations for deliberation by the full Board in two public sessions on December 12, 2013 and March 5, 2014, with final recommendations approved by the full board June 5, 2014. The completion of the report was aided by the ability to review the Board's public findings and recommendations with appropriate stakeholders.

To address the Task Group's objectives, the Group and staff collected an abundance of research information derived from briefings and papers provided by each of the Services and their Reserve components, interviews with functional area experts within and outside of the Department, reviews from reports and previous studies, as well as organizational documents and Congressional testimony. The Task Group sought inputs from a diverse array of experts and interested parties to inform its analysis. In addition, members attended CYBER GUARD 13 to observe RC members participating in a cyber-exercise along with elements of the AC's Cyber Protection Team #1. The Group was very mindful throughout of the need for cybersecurity. While this report primarily focuses on the Reserve Components, many of the findings, observations, and recommendations apply to Active and Reserve Components as well as the enterprise effort to build cyber capabilities within the Department of Defense.

A parallel effort in reviewing this topic is being accomplished by USCYBERCOM and the Office of the Secretary of Defense (OSD) for Cyber Policy in compliance with requirements levied by Congress through Defense Appropriation language and Section 933 of the 2014

NDAA.² The Cyber Policy Task Group has collaborated with both organizations, sharing information collected from the Services, as well as the Task Group's findings and observations. A key difference between this report and DoD mandated reports is the level of reported detail on RC cyber units, skill sets required to meet cyber mission team requirements and a cost-benefit analysis of meeting cyber manpower requirements with teams sourced from the AC only, compared to a mix of AC/RC or fully filled by the RC. The National Guard has also been tasked to provide an independent assessment.

FINDINGS & OBSERVATIONS

Finding #1: USCYBERCOM, Service cyber organizations and the Joint Staff are making exceptional progress in sourcing manpower, developing training programs and enabling employment guidance needed to field a fully operational Cyber Mission Force.

This assessment of the Department of Defense's current path in developing its cyber organization, policies and doctrine is a snapshot of a moving train. Some of the Board's Findings and Observations as well as our Recommendations are subject to being outdated as fielding the Cyber Mission Force rapidly evolves. Overall, the Department should be commended for its significant efforts in developing an organizational framework, building training capacity and capability, and enabling plans to employ offensive and defensive forces in the cyber domain.

Stepping back to review the history behind these developments begins with the Department recognizing in the 2006 National Military Strategy for Cyberspace Operations that cyber is a domain in which the military operates. This places cyber on par with sea, land, air and space domains.³ Since this recognition, the Department has created the Sub-Unified Command called USCYBERCOM under USSTRATCOM. They achieved IOC on May 21, 2010. This new organization combined the Joint Functional Component Command-Network Warfare and Joint Task Force-Global Network Operations, effectively joining offensive and defensive cyber operations under a single command.⁴ In support of USCYBERCOM, each service has stood up individual service cyber organizations, the last being the 2013 IOC for Coast Guard Cyber. Senior military leadership realized that this force was not sufficient to meet the rising cyber

² National Defense Authorization Act for Fiscal Year 2014, Public Law 113-66, 113th Cong., 1st sess., (December 2013), 163-166.

³ Peter Pace, *The National Military Strategy for Cyberspace Operations* (Washington DC: Chairman of the Joint Chiefs of Staff, 2006), 3.

⁴ Rivers J. Johnson, "About Us," United States Cyber Command, http://www.cybercom.mil/default.aspx# (accessed May 1, 2014).

threat risks or satisfy Department needs. This realization led to the 2012 authorization of a new conceptual framework for adding depth to cyber defense, capability to cyber offense, and enhanced support for our Combatant Commanders, through the fielding of the Cyber Mission Force.⁵ The challenges of bringing disparate service capabilities and divergent cyber solutions into a joint enterprise requires a tremendous amount of effort and collaboration and it appears that the Department of Defense is on a positive vector towards achieving this goal.

Finding #2: The Cyber Mission Force, as authorized in the December 2012 Secretary of Defense Memo, consists of 133 teams.

The Cyber Mission Force is a standardized force presentation construct with three primary mission sets; Defending the nation against cyber-attack with National Mission Forces, Operating and Defending DoD Information Networks (DODIN) with Cyber Protection Forces and Combatant Command Support from Cyber Combat Mission Forces.⁶ The Joint Chiefs of Staff (JCS) "Tank" and Deputy's Management Action Group (DMAG) determined size and composition of 133 teams and approximately 6,000 personnel based on the capabilities needed for a sustained operational requirement.⁷ The CMF is an all Service effort with 30% of the teams resourced each from the Army, Navy, Air Force, and the remaining 10% from the Marine Corps. The force mix initially pursued an 80% Active Component and 20% Civilian manpower composition; although each Service is pursuing a slightly different model. As an example, the Marine Corps is targeting a force mix of approximately 64% Active Component military, with just under 30% civilian and the remainder from contractor sourcing.8

The CMF framework of teams, missions, functional distribution, size and numbers was developed by USCYBERCOM. OSD Capabilities and Program Evaluation (CAPE) were not involved in any analysis on resourcing the force. As of this time, the Task Group is unaware of CAPE conducting a program evaluation of this construct. Anecdotally, there are

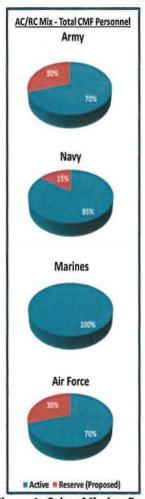


Figure 1: Cyber Mission Force Team Distribution

⁵ DOD, Fiscal Years 2011-2015 Capability Gap Assessment Results and Recommendations for Mitigating Capability Gaps, JROCM 113-09 (Washington DC, June 2009).

⁶ Cheryl Pellerin, "DOD Officials Cite Advances in Cyber Operations, Security," *American Forces Press Service*, March 14, 2013. http://www.defense.gov/news/newsarticle.aspx?id=119532 (accessed June 24, 2014).

⁷ Charles T. Hagel, Quadrennial Defense Review (Washington DC: Department of Defense, 2014), p. 41.

⁸ Mark A. Butler, interview with Marine Forces Cyber Chief of Staff, Columbia, MD, February 25, 2014.

⁹ Lisa A. Dixon, e-mail message from OSD CAPE to author, December 2, 2013.

various levels of analytical rigor applied to determine team numbers and size, with National Mission Teams having the most. ¹⁰ Reserve Component plans and pre-decisional proposals to field an additional 33 Cyber Protection Teams will result in providing a 27% increase in teams and 31% increase in CMF manpower, most of which is above known requirements. This increase in teams and manpower investment, if fully resourced, could cover CMF surge operations, backfill requirements for AC teams or steady state use of an Operational Reserve. However, there is no documentation of RC CMF missions and roles or established requirements. The lack of a defined requirement could result in creating excess Department of Defense force structure. Reserve Component CMF structure would benefit from a mission analysis and formal validation process. There are some indications that this is being accomplished at the Service level, but it lacks consistency. The Air Force, as part of their Total Force integration strategy, has developed a plan that reduces AC manpower in three Cyber Protection Teams and one National Mission Team through RC augmentation.

FIGURE 2: Service Allocation of Cyber Mission Teams/Pre-Decisional and Proposed RC Force Structure						
Cyber Msn Force	National Mission Team	National Support Team	Combat Mission Team	Combat Support Team	Cyber Protection Team	
Army	4	3	8	6	20	
Army Natl Guard			-		11	
Army Reserve	-	-	-	-	10	
Navy	4	3	8	5	20	
Navy Reserve	-	Augment	-	Augment	Augment	
Marine Corps	1	-	3	1	8	
Air Force	4	2	8	5	17	
Air Natl Guard	Augment		-		12	
Air Force Reserve		-	-	-	3	
Coast Guard	Augment	-	Augment		Augment	

AC figures provided by USCYBERCOM/RC figures from Task Group interviews and subject to programmatic action

¹⁰ Interview with Navy, Air Force, Army Reserve, Army National Guard Service Cyber Panel, Pentagon, Washington DC, November 18, 2013.

It also replaces AC manpower from two Cyber Protection Teams with Air National Guard operational support.

Finding #3: Initial direction to establish Cyber Mission Forces from Service Active Components does not take advantage of the skill sets resident in the Reserve Components enhanced by civilian jobs and available at reduced cost.

The 2010 Quadrennial Defense Review (QDR) directed the creation of the Comprehensive Review of the Future Role of the Reserve Component report and the 2011 Department of Defense Strategy for Operating in Cyberspace document advocates for additional RC cyber growth as a way to rebalance the Total Force or build greater capacity, expertise and flexibility. 11 There are at least two commission reports that specifically recommend building cyber capabilities in the RC. 12 A third report's findings highlight the cost and value of building RC force structure in areas where civilian acquired skills provide benefit to the Department for domestic and overseas missions. 13 Several think tank reports lend credence to this view. One report went so far as to refer to elements of the cyber mission as "tailor made" for the RC.¹⁴ Despite readily available documents, as brought up in Finding #2, the initial Service force structure decision was to build the Cyber Mission Force primarily in the AC. This path to building cyber capabilities was briefed to the Reserve Forces Policy Board during the June 2013 Quarterly meeting, reinforcing perceptions that barriers remain towards achieving a Total Force culture. A subsequent clarification letter to the RFPB from Lt Gen Davis, the USCYBERCOM Deputy Commander, stated that Service Cyber Component Commanders are actively engaged in integrating Reserve Components, in addition to USCYBERCOM's commitment towards achieving a Total Force solution.¹⁵ However, Army, Navy and Marine Corps Cyber Workforce Strategies and published White Papers on their Workforce models are silent on discussing RC participation in the Cyber Mission Force. USCYBERCOM, as a functional command, OSD, and the Joint Staff may have reservations about advising services how to integrate their reserve components, but they are in the best position to provide advice and to advocate for Total Force solutions that best serve the needs of the Department, as well as interagency, state and private sector partners.

¹¹ James E. Cartwright and Dennis M. McCarthy, *Comprehensive Review of the Future Role of the Reserve Component* (Washington DC: Office of the Vice Chairman of the Joint Chiefs of Staff and Office of Assistant Secretary of Defense for Reserve Affairs, 2011), p. 90-93.

¹² Dennis McCarthy et al., *National Commission on the Structure of the Air Force* (Arlington: NCSAF, 2014), 42. ¹³ Arnold L. Punaro et al., *Commission on the National Guard and Reserves: Transforming the National Guard and Reserves into a 21*st-Century Operational Force (Arlington: CNGR, 2008), 71-72.

¹⁴ Albert A. Robbert et al., *Suitability of Missions for the Air Force Reserve Components* (Washington DC: RAND Corporation, 2014), 56-62.

¹⁵ Jon M. Davis, memorandum to Chairman, Reserve Forces Policy Board, September 11, 2013.

It has been noted that the previous Acting Assistant Secretary of Defense for Readiness and Force Management, before his retirement, directed a study on CMF manpower requirements by the Institute for Defense Analysis which will consider a different mix than 80% active component military and whether a more appropriate mix of contractors, National Guard and Reserve would be more efficient and effective. ¹⁶

Finding #4: Without a continuum of Service mind set, it is impossible to retain valuable Cyber Mission Force skills, experience and capabilities for individuals leaving the Active Component.

Currently, the Marine Corps has a reasonably robust reserve augmentation to the Marine Forces Cyber Headquarters. 17 At the time of the Task Group's review, nearly 35 of 53 Individual Mobility Augmentee Reservists assigned to MARFORCYBER have accomplished "long term" full time support duty, with several reaching the 1,095 active duty day waiver limitations. However, these individuals are not assigned to operational cyber defense or offense operations, despite some having relevant skills in these areas. Creating individual augmentee positions within the Cyber Mission Force would provide an outlet for "a continuum of service" from these highly trained individuals. It would also provide a useful way to capture a greater continuum of service from members leaving the Active Component for private industry within the Service's respective Reserve Components. An existing study by the Institute for Defense Analysis highlights that more than 50 percent of existing legacy cyber organizations' manpower had relevant skills for Cyber Network Defense and Cyber Network Exploitation from civilian occupations. The same survey showed that 88 percent of subject matter experts who observed reserve participation felt they added value to AC units several times or more per year, while none felt there was no value added. In addition, the survey indicates that experienced reserve cyber augmentation can provide operational synergies, when paired and employed in an integrated AC/RC workforce setting.¹⁸

The Coast Guard Cyber organization is extremely small, with only 23 billets assigned to CG Cyber Command and an additional six to the Department of Homeland Security's National Cybersecurity and Communications Integration Center. Size constraints make zero-sum manpower resource decisions even more difficult to achieve as other mission areas are

¹⁶ R.E. Vollrath to Assistant Secretaries of the Military Departments for Manpower and Reserve Affairs, Deputy Chief of Staff Army G1, Chief of Naval Personnel N1, Deputy Chief of Staff, Air Force A1, Deputy Commandant, Manpower & Reserve Affairs, "Requesting Support for Study on Staffing Cyberspace Operations", November 22, 2013, Pentagon, Washington DC.

¹⁷ Andrew (BA) Seay, interview with Marine Forces Cyber, Reserve Detachment OIC, Columbia, MD, March 4, 2014. ¹⁸ Drew Miller, Daniel B Levine and Stanley A Horowitz, *A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber* (Alexandria: Institute for Defense Analysis, 2013), 14-A2.

decremented to make way for new mission growth without increases to authorized endstrength.¹⁹ However, case-by-case consideration for creating augmentee positions for departing members with Cyber Mission Force experience might prove beneficial especially for individuals experienced in their unique mission to protect Maritime Critical Infrastructure and Key Resources (MCIKR) from cyber threats and vulnerabilities or those with interagency expertise from liaison position within the Department of Justice's National Cyber Investigations-Joint Task Force (NCI-JTF).

Finding 5: Existing Reserve Component cyber units are not designed or organized to present 'plug and play' forces under today's Cyber Mission Force construct.

Only a minority of individuals who complete baseline courses resulting in the award of a legacy Military Occupational Specialty (MOS), Rating or Air Force Specialty Code (AFSC) initially considered as qualifying for retraining into the CMF will become cyber warriors under this construct. In short, not all cyber will be part of the Cyber Mission Force. There are well established requirements for individuals in Information Technology, Information Assurance, Cryptologic Technicians, Signals Intelligence, Electronic Warfare, Client Systems, Cyber Transport, and other related specialties. The need to man Network Operations Centers (NOCs) and build and maintain networks remain as validated requirements. Some Services are building new specialties that support the CMF construct, including the Army's newest occupational specialty, 25D, cyber network defender.²⁰ The Air Force significantly restructured their cyber AFSCs in 2010, with 11 new enlisted occupations and consolidation of their communications and information officers into the 17D Cyberspace Operations career field. Consolidating officer career fields has received some criticism, since the majority of these officers still perform functions outside of 'keyboard' network operations in legacy duties, yet are not identified as force support or visibly differentiated from those working directly in the cyber domain.²¹

The existing RC legacy cyber units, such as the Army National Guard's Virginia Data Processing Unit, Army Reserve Information Operations Center, and Air National Guard and Reserve Network Warfare Squadrons/Flights or Information Aggressor Squadrons (IOS) have some complementary skill sets, but do not contain all of the training needed to fill out a full range of capabilities used by Cyber Mission Teams. Some Service RCs augment AC units in lieu of a unit construct. Another compatibility issues is the widely varying size of RC units,

¹⁹ Kyle J. Smith, interview with CG Cyber Command and FY2016-FY2020 Cybersecurity PG Initiative Overview, Alexandria, VA, December 17, 2013.

²⁰ Wilson A. Rivera, "Cyberspace warriors graduate with Army's newest military occupational specialty," WWW.ARMY.MIL: The Official Homepage of the United States Army, December 6, 2013, http://www.army.mil/article/116564/ (accessed December 16, 2013).

²¹ Katrina A. Terry, *Overcoming the Support Focus of the 17D Cyberspace Operations Career Field* (Wright-Patterson Air Force Base: Air Force Institute of Technology, 2011), 58.

typically 65 to 166, which would require some force shaping reductions or additive missions. CMF teams range in size from 24 for support teams to 64 for National Mission Teams, with the Cyber Protection Teams standardized at 39 personnel.

Finding 6: Department of Defense Service Cyber Doctrine is not fully matured and is in various stages of re-write and development.

The Cyber Task Group found doctrine development, especially Service doctrine in its early state of maturity. The overarching core document is Joint Publication (JP) 3-12, Cyberspace Operations; classified SECRET. This JP was published in 2013 and includes Presidential Policy Directive 20 in Appendix A. JP 3-12 mostly fulfills the executive recommendation for a previous doctrine deficiency gap discovered by the Government Accountability Office (GAO) and recorded in report 11-75. However, with the development of the Cyber Mission Force construct, this product will require revisions along with lagging Service Doctrine.²²

The Air Force has the oldest Service Doctrine, with the latest change to Air Force Doctrine Document (AFDD) 3-12 Cyberspace Operations made in 2011. The US Army just released their Field Manual 3-38 Cyber Electromagnetic Activities in February of this year. Neither of these documents discusses the Cyber Mission Force or its organization, roles, missions and responsibilities. The Navy's Warfare Publication (NWP) 3-12, Cyberspace Operations is rescinded pending re-write (draft expected in October 2014). The Marine Corps interim cyber operations doctrine (MCIP) 3-40.02 is currently in edit and should be available in September 2014.²³ The Coast Guard has identified the need to develop Service doctrinal guidance, but currently cyber rates a single paragraph in Coast Guard Publication 3-0.

In the Navy's published strategy guidance, called *Navy Cyber Power 2020*; they bring up a valid point that will steer future doctrine efforts, when they discuss IT infrastructure efficiencies and cybersecurity improvements from the implementation of the Joint Information Environment (JIE). Common JIE architecture and enterprise solutions will eventually drive Services towards common doctrine, tactics, techniques and procedures across the Department of Defense.²⁴ Services are making headway in this effort with the closing of data centers and network gateway consolidations, which effectively reduce the internet facing attack vectors as

²² Davi M. D'Agostino and Gregory C. Wilshusen, *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities* (Washington DC: United States Government Accountability Office, 2011), 43.

²³ Tony Mattaliano, email from Marine Corps HQ C2/Cyber EW Integration Division, Quantico, VA, July 3, 2014.
²⁴ Kendall L. Card and Michael S. Rogers, *Navy Cyber Power 2020* (Washington DC: Department of the Navy, 2012), 2-3.

the Defense Information Systems Agency (DISA) refines plans for a single security architecture.²⁵

Finding 6a: Strategic Cyber guidance is spread across multiple documents without established links.

Current Strategic Guidance is spread across multiple documents; consisting of Presidential Policy Directives, Initiatives, Policy Reviews, and Executive Orders, as well as Department of Defense Strategy, International Strategy, and National Military Strategy. A comprehensive overarching document that provides linkages to these documents is needed. This core strategy should include roles and responsibilities, milestones, costs, resources, and performance measures beneficial to holding the DoD and other Agencies and Departments accountable. This is a continuing problem that has been noted by the GAO in testimony and reports to Congress as recently as 2013.²⁶

The Department of Defense could also benefit from strategy improvements similar to those needed in National Plans, as identified in GAO report 13-187. The 2006 National Military Strategy for Cyberspace Operations was replaced or complemented by the 2011 Department of Defense Strategy for Operating in Cyberspace even though DOD goals are not as clear and content in some ways is less complete and relevant to the Services.²⁷ As an example, vulnerabilities that are discussed mention theft of intellectual property as the most pervasive threat. However, there is no discussion or guidance on DoD's responsibilities in this regard. Future iterations should include a foreword or preface that highlights a summary of revisions and changes as well as linkages to other relevant documents. It should also include goals, implying a definitive end state instead of initiatives or steps to achieve, as well as an expanded description of a plan of action. Although it may not be palatable to the Intelligence Community to which USCYBERCOM is attached, delving into different strategies for different actors, an attribution strategy and a goal for cybersecurity metrics would also be useful.²⁸ The current lack of transparency on issues like this and the classified Standing Rules of Engagement (SROE) reduce the deterrence value of this document. In fact, the DoD strategy makes no mention of deterrence or what would spark an offensive cyber response, leaving this to the *International Strategy for*

²⁵ Brian T. Dravis, interview with DISA Director JIE Synchronization Office, Fort Meade, MD, May 20, 2014.

²⁶ Gregory C. Wilshusen, *Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges* (Washington DC: United States Government Accountability Office, 2013), 18-23.

²⁷ Sean Lawson, "DOD's "First" Cyber Strategy is Neither First, Nor a Strategy," *Forbes*, August 1, 2011. http://www.forbes.com/sites/seanlawson/2011/08/01/DoDs-first-cyber-strategy-is-neither-first-nor-a-strategy/
²⁸ Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace* (Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2013), 35-37.

Cyberspace, which alludes to implications that a cyber-attack against the U.S. could be met with a kinetic response.²⁹

The Cyber Policy Task Group did not make any of these a recommendation since the majority of these documents fall under the purview of the Cybersecurity Coordinator Special Assistant to the President and the Executive Office of the President. Most of these deficiencies have also been brought to light in other reports and assessments, similar to the Letort Papers.

Finding 7: Reserve Component Cyber Organization Some Reserve Components are planning or propose to build Cyber capable Mission Forces without Department or Service identified requirements.

The terms of reference for this study required the Task Group to examine how RC cyber organizations are manned, equipped and used to meet DOD cyber strategies. Many of these existing RC cyber organizations will continue to meet valuable needs in Cyber Command and Control, Internet Control, Combat Communications, Analysis and Communications Security and other missions. A few will restructure into defensive and offensive cyber functions performed by the CMF. In addition to RC cyber units, USCYBERCOM currently has 90 Reserve Component personnel authorizations directly assigned, which are 78% filled. The Service distribution is 41% AF Reserve, 32% Army Reserve, 24% Navy Reserve, and 3% Marine Reserve. This type of Reserve individual augmentation will continue to grow. The Joint Manpower Validation Board (JMVD) has validated an additional 132 positions that are currently listed as an unfunded requirement and have yet to be Service sourced through the Planning, Programming, and Budgeting Process. These Reservists perform duties as CYBERCOM Headquarters staff support, exercise support, crisis surge support, and plan to extend capability into Geographic Centers of Excellence. They perform duties in intelligence analysis and production, strategy, doctrine and policy, exercise and training, and cyber support. The areas of defensive cyber operations and combat targeting are under development, with cyber analytics and cyber law currently unsupported.³⁰

Even though Active Components are all striving to achieve a standardized Cyber Mission Force team construct, Reserve Component organization and fielding is following a diverse range of concepts based on perceived needs and planned operations. While training is expected to produce the same standardized individual output, the ability to employ as a team or an operational reserve will be significantly different. At this stage of development, it is difficult to assess which is the preferred solution, or whether these constructs will meet the overall needs of

²⁹ Barack Obama, *International Strategy for Cyberspace* (Washington DC: Executive Office of the President, 2011), 14.

³⁰ Sheila Zuehlke, email of briefing provided to Joint Reserve Component Council, Fort Meade, MD, January 15, 2014.

their respective Services or the Department. It would be expected to see cyber teams performing at a higher level that those drawn from a pool, similar to aircrew or surgical teams; however, theoretically, individuals with standardized training should meet requirements in a satisfactory manner. The planning information presented in the following bullets are meant to highlight the component differences, but the Task Group cautions that most of these are "pre-decisional" and either lack approved Concepts for Operation or Program Objective Memorandum (POM) action as well as requirements validation. The planning is so dynamic that the Navy Reserve changed their plans during the writing of this report from a team organization towards an augmentation pool concept.

- Army National Guard proposes 10 regional and possibly FEMA aligned Cyber
 Protection Teams, and one Title 10 full time operational Cyber Protection Team
- Army Reserve proposes 10 Cyber Protection Teams with no full time manpower at team level, managed from staff above team level
- Navy Reserve proposes Cyber Mission Force Active Component team augmentation
- Air National Guard proposes 12 Cyber Operations Squadrons manned with 30% full time and yielding two quickly deployable teams in addition to National Mission Team rotational augmentation
- Air Force Reserve proposes one unit with manning for a full time CPT (39),
 employed as RC integrated augmentation to three AC teams and surge capacity with two additional traditional reserve CPTs
- Marine Corps Reserve and Coast Guard Reserve are not planning to participate in the CMF

Each Service Reserve Component is seeking unique organizational solutions.

Recommendation 1: Include Reserve Components in Cyber Mission Force requirements in order to leverage RC reduced cost, civilian/AC acquired skill/experience, continuity and longevity.

Recommendation 1a: Ensure RC surge and Operational Reserve requirements are identified and filled before considering force structure reductions.

The Secretary should direct USCYBERCOM and the Service Secretaries to validate the requirement for RC inclusion in the Cyber Mission Force prior to Fiscal Year (FY) 2017 POM deliberation activities. The Defense Advisory Council recommended that cyber offense and

defense resources in mostly personnel should be increased by an additional 25% above FY 2014 levels.³¹ Although CMF AC manpower was partially sourced as early as 2013 with plans to complete by 2016, the Task Group contends that increased RC participation at that percentage above the planned CMF size could be reasonably validated. DOD leadership was able to determine an estimated steady state requirement for the AC. This would be complete if they were to determine operational reserve, surge or backfill requirements and document as a validated need. While this requirement may eventually be refined as employment experience is gained and further analysis completed, delaying implementation of a true Total Force Solution causes unnecessary thrash as each RC struggles to come up with their own plan amidst sequestration driven reductions. The USCYBERCOM Commander and Director of NSA made a good step in the right direction to begin this process by the hosting the RC Mission Alignment Conference in July of 2014. The purpose of this conference was to quantify the RC's potential roles, responsibilities, and authorities for support of the CMF so the Services can build a more holistic approach to leveraging RC strengths and providing a unified joint approach, as well as inform an appropriate answer to Congressional Defense Committees.³² This recognizes that there should only be one Cyber Mission Force, an all-encompassing view, not several independent RC solutions to complementing this Force.

We hope this conference forum considered funding and participation of an Operational Reserve. One potential discussion topic could be the UK RC participation model. The UK Ministry of Defense set a policy that a minimum of 10% of Army expeditionary requirements would be met by the Reserves.³³ While this goal is clearly unrealistically high for National Mission Teams, it may turn out to be a reasonable model for Cyber Protection Teams.

Recommendation 1b: Create AC/RC cyber associate units that share infrastructure and equipment to the maximum extent possible.

Sharing cyber equipment, infrastructure and mission focus between collocated Active and Reserve Component units could best be served by associations. In addition to reduced cost, leveraging shared equipment and facilities improves AC/RC integration, with the benefit of increased RC efficiency. One study indicates that Cyber Network Defense (CND) and Cyber Network Attack (CNA) integrated units spend between 60-65% of their duty time on operational mission tasks instead of the majority of time normally spent on education, training, and

³¹ Barry M. Blechman et al., *Strategic Agility: Strong National Defense for Today's Global and Fiscal Realities* (Washington DC: Stimson, 2013), 26.

³² Andrew J. Adams, email from Combined Action Group (CAG) staff to author, June 18, 2014.

³³ Ranald Munro, "Army 2020 and beyond" (presentation by the Deputy Commander Land Forces Reserve, British Army presented to the Reserve Forces Policy Board quarterly meeting, Washington DC, March 5, 2014).

administration.³⁴ The 2014 *National Commission on the Structure of the Air Force* believes the next step to improving integration should include integrating the leadership chain of AC/RC associated units and reducing redundant overhead by alternating leadership positions between components.³⁵ A previous RFPB report on RC Use, Balance, Cost and Savings also recommended that the Secretary of Defense should direct Secretaries of the Military Departments to review options and explore creative opportunities to co-locate and share Active and Reserve Component equipment for training and operational use with a view toward improving Active and Reserve Component integration and reducing overall equipment procurement requirements.³⁶ We believe this concept builds on that recommendation.

Recommendation 1c: Validate proficiency and ongoing certification requirements that would justify additional Reserve Inactive Duty Training Periods.

USCYBERCOM asked the RFPB for assistance in addressing funding for an additional 72 Inactive Duty Training periods, similar to those used by the aviation community. Expertise for validating additional training period requirements resides within the Services. CYBERCOM will need to assist the Services in validating proficiency and currency training needed by Cyber Mission Team operators or continuation training requirements needed for recurring certifications. A robust justification will ensure that operational requirements are not being "off-ramped" towards shrinking Reserve Component budgets, when it would be more appropriate to fund through Military Personnel Appropriations (MPA) orders. Performing operational missions in a reserve status is not by itself restricted by U.S. Code if the primary purpose is to provide required training. Certain operational activities that may require Title 10 or Title 50 could potentially restrict a limited number of National Guard training missions. Defensive cyber missions should not be an issue.

Recommendation 1d: Identify cyber specialties needed in the Guard and Reserve outside of the Cyber Mission Force construct.

The Cyber Mission Force is well thought out in providing enhanced defensive and offensive cyber operations. However, to capture a wider range of civilian acquired skills,

³⁴ Drew Miller, Daniel B. Levine and Stanley A. Horowitz, A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber Missions (Alexandria: Institute for Defense Analysis), 23.

³⁵ Dennis McCarthy et al., National Commission on the Structure of the Air Force (Arlington: NCSAF, 2014), 61. ³⁶ Arnold L. Punaro, *Reserve Component Use, Balance, Cost and Savings: A Response to Questions from the Secretary of Defense* (Falls Church: RFPB, 2013), 34.

additional missions outside of these teams should be explored. As an example, the Air National Guard has proposed utilizing Industrial Control System (ICS) expertise from their Washington Air National Guard units to form a capability to train CMF teams on these types of systems. They could also perform ICS and Supervisory Control and Data Acquisition (SCADA) vulnerability assessments on national critical infrastructure as well as DOD owned systems. Another example of small team or individual expertise could include reservists from computer or software manufacturers familiar with vendor sourcing and certification that could assist in addressing supply chain vulnerability assessments and enterprise acquisitions.

USCYBERCOM Guard and Reserve Directorate leadership have taken an innovative approach to seeking RC cyber talent with their proposal to enhance some existing Joint Reserve Intelligence Centers with a Joint Cyber Reserve Element near U.S. geographic cyber and technology centers of gravity in the Silicon Valley, Los Angeles, Seattle, New York City, Austin and the Research Triangle Park in North Carolina among others. Creating distributed operations near major cyber research, industry, and academic centers is an attractive way to leverage an exceptional RC cyber workforce on the leading edge of cyber innovations.³⁸



Figure 3 Source: WANTED Analytics Cybersecurity professional hiring

Robert Burris, interview with Air National Guard Advisor to 24th Air Force, San Antonio, TX, May 15, 2014.
 Sheila Zuehlke, email of briefing provided to Joint Reserve Component Council, Fort Meade, MD, January 15, 2014.



Although federal missions dictate requirements for building force capability, the Council of Governors has met with the Secretary of Defense and expressed support for increasing National Guard cyber capabilities as one of their top priorities.³⁹ The Task Group recommends that the Kansas Intelligence Fusion Center (KIFC) should be considered as a model for maximizing access and information sharing cyber expertise and intelligence between federal, state, and private sector partners. Nearly 80% of critical infrastructure resides in the private sector. Industry and privacy advocates have

expressed reservations with militarized cyber responses and have opposed additional regulations. which have contributed to the lack of any major cybersecurity legislation passing since 2002.⁴⁰ To illustrate this point, in a recent round table hosted by the Center for Strategic & International Studies on the use of the National Guard in cyber security response, one major financial service provider estimated that a uniformed presence responding to an incident within his company would cause the value of his firm's stock to drop 5%. 41 Despite whether this is true or not, privacy and confidentiality concerns exist. The state or regional fusion center provides a means to put a civilian face on military cybersecurity assistance. The KIFC is directed by the Kansas Attorney General, with oversight over privacy rights and civil liberties. The Kansas National Guard Adjutant General as the designated state Homeland Security Advisor is a key member of this mutually beneficial partnership that provides foreign threat analysis and receives force protection assistance in return. Intelligence members from the National Guard are assigned to a compartmentalized collocated fusion center that separates homeland security intelligence analysis from their Military Analysis Center. They focus on national level Standing Intelligence Needs (SINS), but work collaborative issues with DHS analysts and private security representatives. This brings greater resources to the issues of several different functional Information Sharing and Analysis Center sectors representing; energy, financial services, telecommunications and other critical infrastructure. They are also assisted by the 177th Information Aggressor Squadron from the Kansas Air National Guard on cyber intrusion pattern analysis and threats to critical infrastructure components and networks. 42 The National Guard brings security clearances and access to classified federal capabilities to the state and local level, similar to the information sharing environment established at the national level by the DHS National Cybersecurity and Communications Integration Center or NCCIC. The distributed

³⁹ Ashton B. Carter and Jane Holl Lute, letter from DoD/DHS to Governors' Branstead and O'Malley Washington DC, May 3, 3013.

⁴⁰ Rita Tehan, *Cybersecurity: Authoritative Reports and Resources, by Topic* (Washington DC: Congressional Research Service, 2013), 1.

⁴¹ Stephanie Sanok Kostro, "The Future of the Army National Guard in Cybersecurity" (roundtable discussion hosted by CSIS, Washington DC, December 19, 2013).

⁴² Jeremy Jackson, interview by author, Topeka, KS, February 2014.

network approach ties them into critical infrastructure and analysis subject matter experts making this model an effective information sharing environment within an existing legal framework.

Not all states have resident National Guard unit cyber capabilities, but they do have Army National Guard authorizations for eight cybersecurity professionals and an additional cyber intelligence 35F/N position to assist with National Guard and state network security. These individuals could liaise with joint partners in respective fusion centers on cyber issues. One limitation is the current capability of the fusion centers, of which only 50% of the existing 77 nationwide have a cyber-sector team. The other limitation is that not all states have filled their nine authorizations. Some of the states have been blocked on filling their authorizations due to funding shortfalls. The Task Group's last update indicated that only 64% of computer network defense positions have been filled. Seven states have two or less, and only fifteen states have six or more positions filled.

Recommendation 2: As part of a Total Force solution, re-evaluate the composition, size and force mix of the planned Cyber Mission Force by FY 2017, and refine as needed based on changing threats, team effectiveness, capability, required capacity and cost.

The full sourcing of Cyber Mission Force manpower should be complete in FY 2016, with up to two years of training needed for some teams to reach FOC certification. By the end of 2017 enough teams should be in place to re-evaluate effectiveness and capacity based on the performance and operations tempo of existing FOC teams. Considering the dynamic nature of the cyber threat and complexity of the CMF construct, an ongoing reassessment should be accomplished. As more countries gain offensive cyber capabilities, it is likely that the number of National Mission Teams may need to increase. Concurrently, JIE architecture improvements might drive down the requirements for Cyber Protection teams. These types of decisions, as well as RC integration, will require analytic data from well-developed metrics.

There has been debate on quantifying what type and amount of RC cyber capabilities that are applicable to the CMF from civilian acquired skills. Some AC Service planners are skeptical and without a formal tracking mechanism for certified skills, there will continue to be doubts. CYBER GUARD 13 participant interviews with the Task Group left an impression that RC teams were up to the task and brought civilian acquired capabilities to the exercise that were not yet available from the AC team in training. Air National Guard participants supplied the RFPB with a list of civilian companies that employ their members. The list of companies was

⁴³ DHS, *2012 National Network of Fusion Centers Final Report* (Washington DC: Department of Homeland Security, 2013), 4.

⁴⁴ Stephanie S. Kostro et al., *Citizen-Soldiers in a Time of Transition: The Future of the U.S. Army National Guard* (Washington DC: Center for Strategic & International Studies, 2014), 58-59.

well represented by major cyber and technology industries as well as government agencies and is included in Appendix B. The DOD *Cyberspace Workforce Strategy* has two relevant focus area elements that address this topic. The first is identifying and tracking personnel and qualifications within the cyberspace workforce and the second is analyzing RC support for cyberspace missions that offer DOD access to private sector cyber expertise in addition to requirement analysis for crisis and surge capabilities necessary to conduct cyberspace missions.⁴⁵ The Task Group believes that following through with the implementation plan for this strategy should be a priority for the Department of Defense.

Recommendation 2a: Direct the development of performance based metrics to evaluate Cyber Mission Force teams.

The Task Group, like the Defense Science Board, found a similar lack of success in discovering cyber metrics useful for the Department to make investment decisions or shape its cyber structure. GAO's 12-275 report addresses outcome-based measures assisting DHS in assessing cybersecurity effectiveness. This is equally applicable to the Department of Defense. USCYBERCOM and Service cyber organizations' current priorities, with a minority of the Cyber Mission Force teams now reaching IOC, are training and fielding teams. However, they have assigned a project within USCYBERCOM towards developing metrics. This effort needs to be elevated in importance. This could be aided by reinvigorating the OSD Chief Information Office cyber metrics working group. The Task Group believes that this project will require a significantly larger collaborative effort and should include DHS, academic/private sector partners, Defense Labs and key DOD Service and Agency stakeholders. Cyber metrics are "difficult to identify, delimit and quantify," yet they are vitally important in risk determinations and return on investment and alternative decisions. Currently the Department is unable to either rate their own cybersecurity effectiveness in personnel performance or fully quantify effectiveness of cyber tools and IT architecture.

Re-validating the initial framework is essential to determining the most efficient and effective force size and mix investment given declining budget resources. As an example, current plans allow for Cyber Protection Teams to be assigned to Combatant Commanders,

(Washington DC: Defense Science Board, 2013), 12.

⁴⁷ Gregory C. Wilshusen, *Communications Networks: Outcomes-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts* (Washington DC: Government Accountability Office, 2013), 21.

⁴⁹ Mark Mateski et al., *Cyber Threat Metrics* (Albuquerque: Sandia National Laboratories, 2012), 31.

⁴⁵ Ashton Carter, *Department of Defense Cyberspace Workforce Strategy* (Washington DC: DOD, 2013), 5-15. ⁴⁶ Paul Kaminski, James R. Gosler, and Lewis Von Thaer, *Resilient Military Systems and the Advanced Cyber Threat*

⁴⁸ Stuart H. Starr, "The Challenges Associated with Assessing Cyber Issues," in *Cyber Infrastructure Protection*, (Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2013), 2:238-242.

Service cyber organizations, and USCYBERCOM. Understanding both the capability and capacity of these teams as well as the workload and operational tempo will be pivotal to determining whether this initial allocation is correct or needs rebalancing. Internal CMF team refinement may also need to be made, within numbers of tool developers, color teams and HUNT functions. As of now, the Services metric tends to focus on implementation progress. Tied to recommendation #1 is the need to close a feedback loop back to the service Programming, Planning and Budgeting guidance for future fiscal years to address this reassessment.

Recommendation 3: The Department of Defense should study, and then assign executive responsibility to a single Service for the full range of joint cyber training.

Each of the services, with the exception of the Coast Guard, maintains at least some of their own baseline cyber technician/information technology schools. However, with the implementation of the Joint Information Enterprise standardized network architecture and desire for joint "plug and play" of different service cyber teams, it may be prudent to examine whether resource consolidation efficiencies could be found within the Department of Defense by appointing a single service as the cyber school executive agent.

The Task Group recognizes that this is not as simple as it appears, since each service retains the majority of their cyber trained personnel in legacy missions that fill unique requirements. However, the Task Group believes that re-aligning these types of courses could potentially reduce overlapping coverage in joint advanced courses through a common syllabus and assist in USCYBERCOM's end objective to produce a standardized Cyber Mission Team member. This recommendation is a long range goal. For the short term, further disrupting training pipelines could adversely impact capacity and delay cyber mission teams reaching Full Operational Capability. Any additional delays would be undesirable, despite fiscal savings that might result from consolidations.

The Cyberspace Training Advisory Council is chaired by USCYBERCOM J7, OSD Personnel and Readiness and OSD CIO representatives. This group is suitably positioned to pursue this recommendation, since it is included in their draft charter that is expected to be approved in the summer of 2014. The Council is preparing a catalog of service cyber schools and evaluating content for equivalency between courses. The assessment of graduated students and equivalency evaluation should combine to identify gaps in training capabilities and determine ways to reduce duplication by aligning existing training solutions.⁵⁰

⁵⁰ Stephanie Keith, email attachment of draft Department of Defense Cyberspace Training Advisory Council Charter, June 13, 2014.

Recommendation 4: Recruit highly skilled members via a professional accessions and retention program to fill both AC and RC requirements within the Cyber Mission Force.

To meet Strategic Initiative #5 of the 2011, Strategy for Operating in Cyberspace, consideration should be given towards recruiting highly skilled members via a professional accessions program, similar to the UK Land Information Assurance Group (LIAG) Army Reserve model. Paradigm-shifting approaches, mentioned as a strategy initiative, require out-ofthe-box proposals to tap into exceptionally talented industry pools. A 2014 RAND report also mentioned a similar proposal based on the UK select reserve, as a way to attract higher paid individuals that might otherwise not be interested in Active Component service or the lower pay provided by the GS civilian pay schedule.⁵¹ The specific cyber model the Task Group advocates differs in that it proposes targeted recruitment into the officer grades of Captain and Major for exceptionally qualified individuals through professional accessions, similar to how existing JAG or medical officers are brought into uniformed service. Services could leverage USCYBERCOM's Individual Training and Evaluation Board process to grant credit for existing skills, and reduce both the training bill (Class billets/Human Capital costs) for the Services, as well as the amount of time spent in Officer Training/Candidate Schools, compared to Commissioned Officer Orientation Programs (12-14 weeks versus 5 weeks). For the RC, this serves the additional benefit of limiting the candidates' time away from work and their potential personal financial cost from the lower military pay they would receive.

The Services' ability to recruit civilians using the standard General Service Pay tables and also retain individuals through traditional bonus programs may not be sufficient to compete with high industry demands. The UK Army Reserve notes that their organization has been successful in enticing higher paid individuals to participate in lower paying military operations through flexible scheduling and an overall modest tax rebate bonus based on the amount of service given in that year.⁵² The UK model also contains more flexibility in meeting physical standards. The more flexible standards could be adopted to help retain Wounded Warriors in uniformed service. The need to foster non-traditional hiring for niche mission needs is also a focus element from the DOD's Cyberspace Workforce Strategy.

⁵¹ Albert A. Robbert et al., *Suitability of Missions for the Air Force Reserve Components* (Washington DC: RAND Corporation, 2014), 42-46.

⁵² Christopher Barrington Brown, interview with Commander LIAG, 2 Signals Corps, Royal Corps of Signals, UK Army Reserve, Washington DC, November 17, 2013.

CONCLUSION

The cyber domain is increasing in its criticality and importance to the Department's network centric warfight. Threats and attempted intrusions into government networks are rapidly increasing as more of the world's population goes online. Cybersecurity incidents increased 680% between 2006 and 2011 alone. Despite the extensive training lead times needed to bring CMF teams to full certification, it is evident to the Task Group that significant progress is being made in as short of time as possible to improve the Department's cybersecurity posture and provide a wider range of capabilities to Combatant Commanders. Once fully fielded, the Department of Defense will dwarf the Department of Homeland Security's cyber incident response capabilities. Their Industrial Control System Cyber Emergency Response Team (ICS-CERT) and US-CERT resources used to respond to .gov and critical infrastructure incidents will equate to approximately 13% of the personnel the Department is committing to Cyber Protection Teams for defense of .mil networks. S4

There are areas in which the Department should improve and issues that still need further effort. The Department has put together integration/implementation teams, working groups and convened councils to address several of the issues the Task Group mentions in this report. There are a few items which remain unclear as to whether they will be addressed in a timely and collaborative manner. These include updating and maturing Service Cyberspace Operations Doctrine and developing Tactics, Techniques and Procedures (TTPs) across the Services. Another significant issue is the determination of an appropriate AC/RC mix in cyber missions. Other than AF component integration into six of their 39 CMF teams, there appears to be no Service appetite for operational reserve forces performing steady state operations, nor validated surge requirements for proposed and planned RC cyber growth. This is the impetus behind the Task Group's Human Capital Management intensive four recommendations and five sub-recommendations.

The Reserve Forces Policy Board makes these recommendations to the Secretary of Defense under our statutory charter. The RFPB stands ready to make its members and staff available for further consultation or discussion on these matters as the Department shall require.

Respectfully submitted.

Major General (Ret) Arnold L. Punaro Chairman, Reserve Forces Policy Board

⁵⁴ Eric Schneider, interview with DHS NCCIC Operations Chief, Arlington VA, April 15, 2014.

⁵³ Gregory C. Wilshusen, *Cybersecurity: Threats Impacting the Nation* (Washington DC: GAO, 2012), 9.

BIBLIOGRAPHY

- Alexander, Keith B, interview by Senate Committee on Armed Services. Statement of General Keith B. Alexander: Commander United States Cyber Command (February 27, 2014).
- Blechman, Barry M, et al. *Strategic Agility: Strong National Defense for Today's Global and Fiscal Realities.* Summary of Findings from the Defense Advisory Committee, Washington DC: Stimson, 2013.
- Card, Kendall L, and Michael S Rogers. *Navy Cyber Power 2020*. Strategy, Washington DC: Department of the Navy, 2012.
- Carter, Ashton. "Department of Defense Cyberspace Workforce Strategy." *U.S. Department of Defense Chief Information Officer*. December 4, 2013. http://DoDcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy signed(final).pdf (accessed June 16, 2014).
- Cartwright, James E, and Dennis M McCarthy. Comprehensive Review of the Future Role of the Reserve Component Volume 1. Deputy Secretary of Defense directed report, Washington DC: Office of the Chairman of the Joint Chiefs of Staff and Office of Assistant Secretary of Defense for Reserve Affairs, 2011.
- Chen, Thomas M. An Assessment of the Department of Defense Strategy for Operating in Cyberspace.

 The Letort Papers. Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2013.
- D'Agostino, Davi M, and Greagory C Wilshusen. *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities.* Report to Congressional Requesters, Washington DC: Government Accountability Office, 2011.
- Davis, Jon M. "United States Cyber Command (USCYBERCOM) Reserve Component (RC) Initiatives." *Memorandum for Chairman, Reserve Forces Policy Board.* Fort George G. Meade, September 11, 2013.
- Department of Defense. "Department of Defense Strategy For Operating In Cyberspace." *Department of Defense Chief Information Officer*. July 2011. http://DoDcio.defense.gov/Portals/0/Documents/Cyber/DoD%20Strategy%20for%20Operating% 20in%20Cyberspace%20July%202011.pdf (accessed September 12, 2013).
- DHS. "2012 National Network of Fusion Centers Final Report." *Department of Homeland Security*. June 2013. http://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fus ion%20Centers%20Final%20Report.pdf (accessed April 1, 2014).
- Hagel, Charles T. *Quadrennial Defense Review 2014.* NDAA Congressionally Mandated Report, Washington DC: Department of Defense, 2014.

- Johnson, Rivers J. "About Us." *United States Cyber Command.* n.d. https://www.cybercom.mil/default.aspx# (accessed May 1, 2014).
- Kaminski, Paul, James R Gosler, and Lewis Von Thaer. Resilient Military Systems and the Advanced Cyber Threat. Task Force Report, Washington DC: Defense Science Board, 2013.
- Kostro, Stephanie S. Citizen-Soldiers in a Time of Transition: The Future of the U.S Army National Guard. CSIS Homeland Security and Counterterrorism Program Report, Washington DC: Center for Strategic & International Studies, 2014.
- Lawson, Sean. "DOD's "First" Cyber Strategy is Neither First, Nor a Strategy." *Forbes*. August 1, 2011. http://www.forbes.com/sites/seanlawson/2011/08/01/DoDs-first-cyber-strategy-is-neither-first-nor-a-strategy/ (accessed November 1, 2013).
- Mateski, Mark, et al. *Cyber Threat Metrics*. Sandia Report, Albuquerque: Sandia National Laboratories, 2012.
- McCarthy, Dennis, et al. *National Commission on the Structure of the Air Force*. Report to the President and Congress of the United States, Arlington: NCSAF, 2014.
- Miller, Drew, Daniel B Levine, and Stanley A Horowitz. A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber Missions. Force-mix research report, Alexandria: Institute for Defense Analysis, 2013.
- Myers, Richard B. *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*. Washington DC: Chairman of the Joint Chiefs of Staff, 2004.
- Nagl, John, and Travis Sharp. An Indispensable Force: Investing in America's National Guard and Reserves. Commission review, Washington DC: Center for a New American Security, 2010.
- Obama, Barack. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." *whitehouse.gov*. May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.p df (accessed September 20, 2013).
- Pace, Peter. *The National Military Strategy For Cyberspace Operations*. Washington DC: Chairman of the Joint Chiefs of Staff, 2006.
- Pellerin, Cheryl. "DOD Officials Cite Advances in Cyber Operations, Security." *American Forces Press Service*. March 14, 2013. http://www.defense.gov/news/newsarticle.aspx?id=119532 (accessed June 24, 2014).
- Punaro, Arnold L. Reserve Component Use, Balance, Cost and Savings: A Response to Questions from the Secretary of Defense. Solicited Report, Falls Church: Reserve Forces Policy Board, 2014.
- Punaro, Arnold L, et al. Commission on the National Guard and Reserves: Transoforming the National Guard and Reserves into a 21st-Century Operational Force. Report to Congress and the Secretary of Defense, Arlington: CNGR, 2008.

- Rivera, Wilson A. "Cyberspace warriors graduate with Army's newest military occupational specialty." WWW.ARMY.MIL: The Official Homepage of the United States Army, December 6, 2013.
- Robbert, Albert A, et al. Suitability of Missions for the Air Force Reserve Components. Research Report, Washington DC: RAND Corporation, 2014.
- Starr, Stewart H. The Challenges Associated with Assessing Cyber Issues. Vol. II, chap. 9 in Cyber Infrastructure Protection, edited by Tarek Saadawi, Louis H Jordan Jr., & Vincent Boudreau, 235-258. Carlisle: Strategic Studies Institute & U.S. Army War College Press, 2013.
- Tehan, Rita. *Cybersecurity: Authoritative Reports and Resources, by Topic.* Report for Congress, Washington DC: Congressional Research Service, 2013.
- Terry, Katrina A. Overcoming the Support Focus of the 17D Cyberspace Operations Career Field.

 Graduate Research Project, Wright-Patterson Air Force Base: Air Force Institute of Technology, 2011.
- U.S. Congress. Senate. *National Defense Authorization Act for Fiscal Year 2014*. HR 3304. 113th Cong., 1st Sess. Public Law 113-66. Washington DC, July 8, 2013.
- Wilshusen, Gregory C. Communications Networks: Outcomes-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersercurity Efforts. Report to Congressional Requesters, Washington DC: United States Government Accountability Office, 2013.

APPENDIX A SLIDES APPROVED BY RFPB ON 4 JUNE 2014



Cyber Policy Task Group

RFPB Recommendation Brief 4 June 2014

Mr. Sergio "Satch" Pecori Task Group Chair



Overview



- Cyber Policy Task Group Charter
- Individuals/Offices
 Contacted for Data
- Findings and Observations
- Reserve Component Cyber Mission Force Organization Finding
- Recommendations
- Questions





Cyber Policy Task Group Members





- Mr. Sergio "Satch" Pecori
 - At-Large Member & Task Group Chair
- Gen (Ret) John Handy
 - At-Large Member



- Navy Reserve Member
- Hon. Gene Taylor
 - At-Large Member
- MajGen (Ret) Leo Williams
 - At-Large Member
- Col Jay Jensen
 - Staff Policy Advisor













Chairman Charge to Task Group



On 29 April 2013, the RFPB Chairman directed the establishment of a task group to:

- Assess DoD's current path in developing its cyber organization, policies, doctrine
- Examine adequacy of staffing mix of active, reserve and civilian personnel
- Consider how RC components should be organized, manned and equipped in order to meet stated DoD strategy
- Consult with Senior Defense officials and other persons and organizations
- Develop a preliminary work plan to submit to RFPB at September 5th meeting



OFFICE OF THE SECRETARY OF DEFENSE RESERVE FORCES POLICY BOARD

8783 Leesings Pilie, Substitit FALCS GHIRRON, VA 22041

APR 20

Mr Sergie A. Pecoci 4517 Tortle Bay Springfield, H. 62711-7401

Dear Such

In resource to the goeba grows of commuter acrossly technologies and the related time as no our national security, the Department of Defense (DeD) is clearly on a course to increase an expandituse to operate within the cyber domain. The Secretary of Defense receivily stated. "Cyber attacks - which barely registered as a threat a decade age - have grown state a defining receiving platential adversaries seeking the ability to strike at America's security, energy, economic and entired infrastructure with the benefit of anonymity and distance." Consequently, the recently delivered budget request for Fiscal Y our 2014 has presented cyber as one of the Department's critical explodations.

A central policy question that the Board meet consider as the extens to which mencapabilities be established within reserve component force structures.

In an affect to help asswer this question. I am establishing a Cyber Poincy Task Group that I would like for you to lead. This Task Group will gather information, conduct research, analyse relevant facts, and develop, for Board consideration, a report or reports of advoce and recommendations for the Secretary of Defense concerning current and future policies, practices and strategies of the Department related to the cyber gornam.

The Tash Group should consult with nazion Defense efficials, and other persons and organizations that you down appropriate. You will need to compily with the requirements in Tale 5. Appendix 2 (Foderal Advance) Committee Acts; the Code of Foderal Regulations, Tale 4: Part 160-3 (Fuderal Advance) Committee Management, and DoD Discusses 5104.04 (Department of Defense Foderal Advisory Committee Management Programs. A qualified Designated Foderal Officer will be appointed from the RFPB staff to assist you with morning three requirements.

The Task Group should began with an independent, recurral and unvarianted assessment of DeD's current path in developing its impostantions, politices, doctrine and processes for the conduct of both definitive and officialities explore agreement. Then the Group should unsariate whether the Department is currently uniffing this new mission with the proper rate of active, reserve, and evolute personnel. Finally, consider how Reneve Component organizations chould be organized, manned, organized and used is more the capacitations outlined in the Ledy, 2013. DoD Synogy for Operating in Cyberspace that states, "pandigm-shifting approaches such as the development of Reneve and National Guara cyber capabilities can build groupe capacity, and flushfilling across NOS, holerst, state, and provide store active are



Cyber Policy Task Group Contacts



- DASD OSD Cyber Policy
- Dep Commander USCYBERCOM
- Chief of Staff, USCYBERCOM
- Military Advisor, USD Policy
- Mobility Asst to DIRNSA
- Asst to Chairman, JCS Natl Guard
- Natl Guard Assistant to DIRNSA/Commander USCYBERCOM
- AG Wisconsin/ New Hampshire
- Asst Commandant for C4IT/CIO USCG
- Dep Dir Trans Regional Policy
- Director of Operations ARCyber, G-3
- Director, DISA Joint Information Environment Technical Synchronization
- Dep Director of Operations, USCYBERCOM, J-3
- Director Strategic Initiatives Group, ARCyber
- CMF Lead, ARCyber
- Director, Strategic initiative, USCYBERCOM
- Director Plans, Policy, Exercises, Training, Readiness 2nd Army, G-5/7
- Institute for Defense Analysis
- Senior Fellow, International Security Program, Center for Strategic & International Studies

- Visiting Fellow, Brookings Institution
- Director National Cyber and Communications Integration Center (NCCIC)
- Professional Staff, House Armed Services Com
- Senior Advisor to Dep Asst Sec of Cybersecurity, DHS
- OSD Cyber Policy staff
- NGUAS Legislative Affairs Manager, Air Programs & Cyber Security
- NGB Director C4I/CIO, J-6
- Chief, Force Development AF Information Dominance/ SAF/CIO, A6
- Director of Communications/CIO AFRC A6
 - Chief USAR Cyber and Information Operations Division, G39
- Marine Corps Combat Development Command
- Branch Head Information Operations, USMC
- Chief of USCG Reserve Forces
- Deputy Commander CG Cyber
- Chief of Strategic Planning, CG Cyber Command
- MarForCyber, Chief of Staff
- MarForCyber, Reserve Det OIC
- Commander, UK LIAG, Royal Signals
- AFSPACE Cyber Programs Integrator



Cyber Policy Task Group Contacts



- Chairman, National Commission on the Structure of the Air Force
- Dep Dir for Intel, IO, Cyber & Space, OSD-RA
- Branch Head for Cyber and EW Strategy, Plans & Policy CNO OPNAV Staff
- N2N6 C12 Information Dominance Corp, Reserve Manpower, Training & Education Advisor
- FORCM (AW), USN
- Director Deloitte Consulting LLP Cyber Guard 13 RC Participant
- Senior Cyber Vulnerability Analyst, ManTech Group Cyber Guard 13 RC Participant
- OSD CAPE C4I and Cyber Programs
- OSD P-R, Dep Director Cyber Readiness
- OSD AT&L Dep Director C3 & Cyber
- DHS NCCIC Director of Operations



Findings/Observations Summary (



- #1: DoD is making exceptional progress towards fielding a fully operational Cyber Mission Force (CMF)
- #2: The DoD stated requirement for the CMF consists of 133 teams sourced from Active Components
- #3: Initial direction to establish Cyber Mission Forces does not take advantage of Total Force solutions
- #4: Marine Corps and Coast Guard have no plans for RC participation in Cyber Mission Force teams
- #5: Existing RC cyber units are not designed/organized to "plug and play" under the Cyber Mission Force construct
- #6: DoD Service Cyber Doctrine is not fully updated
 - Strategic cyber guidance is spread across multiple documents without established links



Findings and Observations



 Finding #1: USCYBERCOM, service cyber organizations and the Joint Staff are making exceptional progress in sourcing manpower, developing training programs and enabling employment guidance needed to field a fully operational Cyber Mission Force





Findings and Observations Cont.



- Finding #2: The Cyber Mission Force, as authorized in the 2012 Secretary of Defense Memo, consists of 133 teams
 - Three primary cyber missions and force of approx 6,000 people
 - Service split of 30% each for Army, Navy, Air Force; 10% Marine Corps
 - Force mix of 80% Active Component, 20% Civilian; however, each service is pursuing a slightly different force mix; some include contractor personnel
 - No Reserve Components were included
- Finding #3: Initial direction to establish Cyber Mission Forces from Service Active Components does not take advantage of the skill sets resident in the Reserve Components enhanced by civilian jobs and available at reduced cost



Findings and Observations Cont.



- Finding #4: Without a continuum of Service mind set, it is impossible to retain valuable Cyber Mission Force skills, experience and capabilities for individuals leaving the Active Component
 - Coast Guard and Marine Corps have no plans in place
- Finding #5: Existing Reserve Component cyber units are not designed/organized to present "plug and play" forces under today's Cyber Mission Force construct
 - The majority of cyber trained forces will remain in legacy missions that have established enduring requirements



Findings and Observations Cont.



- Finding #6: DoD Service Component Cyber Doctrine is not fully matured and is in various stages of re-write and development
 - Strategic Cyber guidance is spread across multiple documents, without established links



RC CMF Organization Finding



- Some Reserve Components are building Cyber capable Mission Forces without DoD or Service identified requirements
 - Army National Guard proposes 10 FEMA region aligned Cyber Protection Teams, and 1 Title 10 Full Time Cyber Protection Team
 - Army Reserve proposes 10 Cyber Protection Teams with no full time manpower at team level
 - Navy Reserve proposes Cyber Mission Force Active Component team augmentation
 - Air National Guard proposes 12 Cyber Operations Squadrons manned with 30% full time yielding two quickly deployable teams
 - Air Force Reserve proposes one unit with manning for a full time
 CPT (39) and surge with 2 additional traditional reserve CPTs
 - USMCR and USCGR are not planning to participate in the CMF41



Recommendations Summary



- #1: Due to their reduced cost, civilian/AC acquired skill/experience, continuity and longevity, the RC should be included in Cyber Mission Force requirements
- #2: As part of a Total Force solution, re-evaluate the size, composition and force mix of the planned Cyber Mission Force by FY17, and refine as needed based on changing threats, team effectiveness, capability, capacity and cost
- #3: Assign executive responsibility to a single Service for common cyber schools to reduce duplicative courses
- #4: Recruit highly skilled members via a professional accessions and retention program to fill requirements for the CMF



Recommendations



 Recommendation #1: Include Reserve Components in Cyber Mission Force requirements in order to leverage RC reduced cost, civilian/AC acquired skill/experience, continuity and longevity

(OSD CIO/Policy, USCYBERCOM, Joint Staff, Services)

- Ensure RC surge and Operational Reserve requirements are identified and filled before considering force structure reductions
- Create AC/RC cyber associate units that share infrastructure/equipment to the maximum extent possible
- Validate proficiency and ongoing certification requirements that would justify additional reserve Inactive Duty Training periods
- Identify cyber specialties needed in the Guard and Reserve outside of the Cyber Mission Force construct



Recommendations Cont.



 Recommendation #2: As part of a Total Force solution, re-evaluate the composition, size and force mix of the planned Cyber Mission Force by FY17, and refine as needed based on changing threats, team effectiveness, capability, required capacity and cost

(OSD CIO/P-R/CAPE/Policy, USCYBERCOM, Joint Staff, Services)

 Direct the development of performance based metrics to evaluate Cyber Mission Force teams



Recommendations Cont.



(OSD CIO, OSD P-R, USCYBERCOM)

- Align and consolidate content; similar courses gain efficiencies and feed advanced joint schools
- Supports Joint Information Enterprise standard service network architecture and enterprise services
- Assist USCYBERCOM in producing interchangeable and fully joint Cyber Mission Force capability



Recommendations Cont.



 Recommendation #4: Recruit highly skilled members via a professional accessions and retention program to fill both AC and RC requirements within the CMF

(OSD P-R, OSD Cyber Policy, OSD RA, USCYBERCOM)

- Paradigm-shifting approach to expanding the aperture on accessions for both AC/RC in growing CMF, similar to UK Reserve model
- Training efficiencies gained through USCYBERCOM Individual Training Evaluation Board recognition of civilian acquired education and skills
- Excellent opportunity to retain Wounded Warriors (skilled or qualified for cyber training)
- Cost savings from Officer Orientation courses versus Line
 Officer Training Schools



Questions?



Mr. Sergio "Satch" Pecori Task Group Chair

APPENDIX B CYBERGUARD 13 PARTICIPANT CIVILIAN EMPLOYEES



175th Network Warfare Squadron Maryland ANG























INSIGHT APPLIED





















Booz | Allen | Hamilton











National Institute of Standards and Technology Technology Administration, U.S. Department of Commerce



262nd Network Warfare Squadron, Washington ANG

















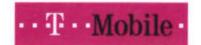














































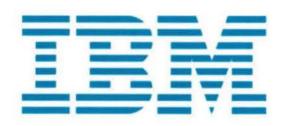






229th Information Operations Squadron, Vermont ANG





















Rhode Island ANG

















BAE SYSTEMS

































Federal Aviation







177th Information Aggressor Squadron, Kansas ANG



































223rd Intelligence Flight, Kentucky ANG























BAE SYSTEMS



273rd Information Operations Flight, Texas ANG





The Reserve Forces Policy Board – Basic Overview

The Reserve Forces Policy Board (RFPB) is a federal advisory committee mandated by law in the Office of the Secretary of Defense to "serve as an independent adviser to the Secretary of Defense to provide advice and recommendations to the Secretary on strategies, policies, and practices designed to improve and enhance the capabilities, efficiency, and effectiveness of the reserve components." As required by statute, the board also produces an annual report which the Secretary of Defense transmits to the President and Congress on reserve component matters the board considers appropriate to include in the report.

The board consists of 20 members; a civilian chairman, a general/flag officer from each of the seven reserve components, a two-star military executive, a senior enlisted advisor, plus ten other U.S. citizens, who may or may not be government employees, with significant knowledge of and experience in policy matters relevant to national security and reserve component matters.

The board is supported by a staff consisting of a Colonel or Navy Captain from each of the six DoD reserve components. There is also a Coast Guard staff officer. These officers also serve as liaisons between their respective components and the board. The law requires them "to perform their staff and liaison duties under the supervision of the military executive officer of the board in an independent manner reflecting the independent nature of the board."

Established in 1951, the board is one of the oldest advisory committees in the Department of Defense.

In the National Defense Authorization Act of 2011, Congress significantly revised the operating framework and membership of the RFPB. Previously, other than the chairman, the board included only DoD officials and made recommendations through the Assistant Secretary of Defense for Reserve Affairs. In 2008, the Commission on the National Guard and Reserves recommended that the RFPB's governing statute (10 USC 10301) be amended because the board was not structured to obtain and provide directly to the Secretary of Defense a wide range of independent advice on National Guard and Reserve matters due to the nature of its membership and its subordination to other offices within DoD. The revised law was effective 1 July 2011.

On 12 September 2011, retired Marine Corps Major General Arnold Punaro was sworn in as the first chairman of the board under the revised structure. Other new members were sworn in at an organizational meeting on 13 October.

The board is organized into three subcommittees: Ensuring a Ready, Capable, Available and Sustainable Operational Reserve; Enhancing DoD's Role in the Homeland; and Supporting and Sustaining Reserve Component Personnel. Subcommittees meet as required. The full board meets quarterly. The RFPB website is at http://rfpb.defense.gov/.